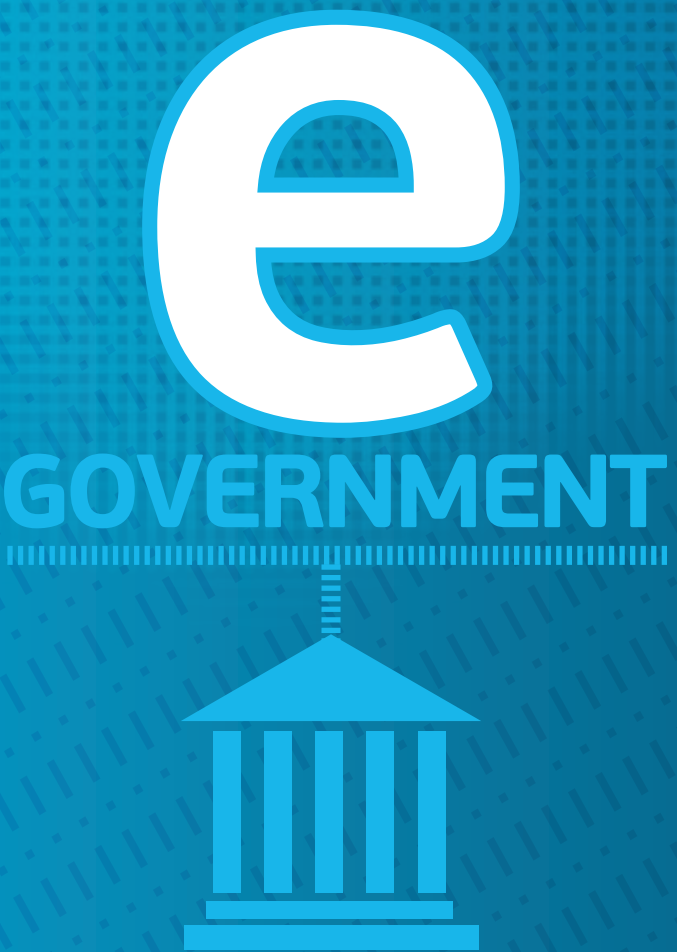
RAPPORT FINAL

UIT-D COMMISSION D'ÉTUDES 2

QUESTION 17-3/2

ETAT D'AVANCEMENT DES ACTIVITÉS RELATIVES AU CYBERGOUVERNEMENT ET IDENTIFICATION DES DOMAINES D'APPLICATION DU CYBERGOUVERNEMENT PRÉSENTANT UN INTÉRÊT POUR LES PAYS EN DÉVELOPPEMENT



5e PÉRIODE D'ÉTUDES 2010-2014

Secteur du développement des télécommunications

POUR NOUS CONTACTER

Site web: www.itu.int/ITU-D/study_groups
La Librairie électronique de l'UIT: www.itu.int/pub/D-STG/
Courriel: devsg@itu.int
Téléphone: +41 22 730 5999

QUESTION 17-3/2:

Etat d'avancement des activités relatives au cybergouvernement et identification des domaines d'application du cybergouvernement présentant un intérêt pour les pays en développement

LES COMMISSIONS D'ÉTUDES DE L'UIT-D

Pour appuyer les activités menées par le Bureau de développement des télécommunications dans les domaines du partage des connaissances et du renforcement des capacités, les Commissions d'études de l'UIT-D aident les pays à atteindre leurs objectifs de développement. Parce qu'elles ont un rôle de catalyseur en créant, en partageant et en mettant en pratique des connaissances dans le domaine des TIC au service de la réduction de la pauvreté et du développement socio-économique, les Commissions d'études de l'UIT-D contribuent à instaurer des conditions permettant aux pays d'utiliser les connaissances pour être mieux à même d'atteindre leurs objectifs de développement.

PLATE-FORME DE CONNAISSANCES

Les résultats des travaux des Commissions d'études de l'UIT-D et les documents de référence connexes sont utilisés pour faciliter la mise en oeuvre de politiques, stratégies, projets et initiatives spéciales dans les 193 Etats Membres de l'UIT. Ces activités permettent en outre d'étoffer la base des connaissances partagées par les membres.

AU COEUR DE L'ÉCHANGE D'INFORMATION ET DU PARTAGE DES CONNAISSANCES

Des réunions présentielles, le Forum électronique et des réunions offrant la possibilité de participer à distance permettent de faire part de sujets présentant un intérêt commun, dans une atmosphère propice à un débat ouvert et à l'échange d'informations.

BASE D'INFORMATIONS

Des rapports, lignes directrices, bonnes pratiques et recommandations sont élaborés sur la base des contributions reçues et examinées par les membres des Commissions. Des données sont recueillies grâce à des enquêtes, contributions et études de cas, et mises à la disposition des membres, qui peuvent les consulter facilement en utilisant les outils de gestion de contenus et de publication web.

COMMISSION D'ÉTUDES 2

La CMDT-10 a confié à la Commission d'études 2 l'étude de neuf Questions relatives au développement de l'infrastructure et des technologies de l'information et de la communication, aux télécommunications d'urgence et à l'adaptation aux changements climatiques. Les activités ont porté essentiellement sur l'étude des méthodes et approches les plus adaptées et efficaces pour la fourniture de services dans les activités de planification, de développement, de mise en oeuvre, d'exploitation, de maintenance et de suivi des services de télécommunication, afin d'en accroître l'utilité pour les utilisateurs. Dans le cadre de ces activités, l'accent a été mis en particulier sur les réseaux large bande, les radiocommunications mobiles et les télécommunications/TIC pour les zones rurales et isolées, les besoins des pays en développement dans le domaine de la gestion du spectre, l'utilisation des TIC pour atténuer les effets des changements climatiques dans les pays en développement, l'utilisation des télécommunications/TIC pour atténuer les effets des catastrophes naturelles et pour les opérations de secours, les tests de conformité et d'interopérabilité et les cyberapplications et, au premier chef, les applications se fondant sur les télécommunications/TIC. Les travaux ont également porté sur la mise en oeuvre des technologies de l'information et de la communication, compte tenu des résultats des études menées par l'UIT-T et l'UIT-R et des priorités des pays en développement.

La Commission d'études 2, conjointement avec la Commission d'études 1 de l'UIT-R, s'occupe également de la Résolution 9 (Rév.Hyderabad, 2010) de la CMDT-10 intitulée "Participation des pays, en particulier des pays en développement, à la gestion du spectre radioélectrique".

Le présent rapport a été établi par un grand nombre de volontaires provenant d'administrations et opérateurs différents. La mention de telle ou telle entreprise ou de tel ou tel produit n'implique en aucune manière une approbation ou une recommandation de la part de l'UIT.

Table des matières

Page

Page

Figures and Tables

QUESTION 17-3/2

Etat d'avancement des activités relatives au cybergouvernement et identification des domaines d'application du cybergouvernement présentant un intérêt pour les pays en développement

1 Introduction

1.1 Révolution des TIC et développement des applications Internet

"L'Internet change tout". Cette expression résume plus ou moins les changements fondamentaux dus aux TIC et, en particulier, à la technologie Internet. Le développement des TIC, leur diffusion et leur application à grande échelle, ont influencé tous les aspects de la société. On parle de révolution des TIC. Une société modifiée à l'issue de la révolution des TIC reçoit le nom de société de l'information. Concrètement, la révolution des TIC consiste dans le processus de transformation, l'apparition de la société de l'information, et les incidences qui en résultent sur divers secteurs, notamment l'entreprise et les services publics. L'Internet a complétement transformé la manière dont les administrations publiques fournissent des services au public et aux entreprises dans leur globalité. L'intérêt accordé aux applications TIC à l'échelle nationale dans de nombreux pays reflète la conviction chez les pouvoirs publics et les citoyens que les technologies servant de base au cybergouvernement constitueraient des leviers puissants pour améliorer l'efficacité de l'administration et rendre plus pratique la fourniture de services au public, ce qui se traduirait par un avantage sur le plan concurrentiel dans le contexte de la société de l'information.

1.2 Cybergouvernement et CE 2 à l'UIT

Dans le cadre du Programme 3 de l'UIT-D, on a entrepris l'étude d'applications de cybergouvernement, notamment de systèmes modernes permettant d'accéder à des services et de les payer, en collaboration et en partenariat avec le secteur privé et avec d'autres organisations du système des Nations Unies. Pour tirer parti des avantages potentiels qu'offrent les applications de cybergouvernement, les pays en développement ont besoin d'informations sur les stratégies, les bonnes pratiques, les sources de compétences spécialisées et l'appui financier, ainsi que sur le type d'applications et de plates-formes technologiques de cybergouvernement qui seraient les plus utiles à leurs habitants, en fonction des besoins et des possibilités actuelles de chaque pays.

L'UIT a décidé de créer une nouvelle commission d'études pour les questions relatives au cybergouvernement, qui concernent principalement l'évaluation de l'état d'avancement des activités relatives au cybergouvernement dans le monde et l'identification des domaines les plus utiles aux pays en développement, par exemple l'utilisation des plates-formes mobiles et hertziennes pour la fourniture et le paiement de services dans les zones rurales et isolées.

L'origine des contributions à l'étude de la Question se décompose comme suit: état d'avancement de l'examen des Questions des Commissions d'études de l'UIT-T (13 et 17, par exemple) ayant trait à ce sujet (authentification, confidentialité, etc.); état d'avancement des projets lancés par le BDT en collaboration avec d'autres organisations du système des Nations Unies et avec le secteur privé au sujet des services et applications de cybergouvernement, l'accent étant mis sur la participation des pays en développement; état d'avancement des autres activités pertinentes entreprises par le Secrétariat général de l'UIT ou par le BDT; rapports d'activité et études de cas présentés par des Etats Membres et des Membres du Secteur et

portant sur les initiatives, applications ou technologies susceptibles d'être utiles à la mise en place d'applications de cybergouvernement.

L'UIT a publié un kit pratique de mise en oeuvre du cybergouvernement, à savoir le cadre d'évaluation de l'état de préparation en matière de cybergouvernement (e-Government Readiness Assessment Framework, 2009). Ce kit pratique examine les dimensions clés de l'environnement de cybergouvernement, afin d'aider les décideurs à identifier les domaines d'action prioritaires, sur la base de l'état de préparation de leur pays et des stratégies nationales de développement. L'UIT a également mené une étude sur les technologies mobiles, en collaboration avec l'OCDE et le Département des affaires économiques et sociales des Nations Unies, étude qui a donné lieu en 2011 à la publication d'un rapport: "L'administration publique sur mobile: technologies mobiles pour des gouvernements réactifs et des sociétés connectées". Ce Rapport, dans lequel l'accent est mis sur le potentiel considérable des technologies mobiles pour l'amélioration de l'administration publique, dresse une analyse approfondie des prérequis de l'administration publique sur mobile, de ses principaux avantages et des principales difficultés qu'elle pose, décrit la chaîne de valeur et les principales parties prenantes, et fait l'inventaire des mesures concrètes à appliquer pour aider les décideurs à évaluer et à mettre à jour leurs connaissances dans le domaine de l'administration publique sur mobile.

1.3 Etudes comparatives sur le cybergouvernement dans les organisations internationales

La plupart des organisations internationales, notamment l'ONU, l'OCDE, l'UIT, la Banque mondiale, et les banques de développement régionales, telles que la BAD et la BAfD, considèrent les questions relatives au cybergouvernement comme un thème de travail important en ce qui concerne le développement durable dans les pays en développement. Depuis 2002, le Département des affaires économiques et sociales des Nations Unies mène régulièrement une enquête sur le cybergouvernement, qui vise à évaluer globalement le niveau de développement du cybergouvernement à l'échelle nationale, et permet de classer les pays membres selon leur état de préparation en matière de cybergouvernement. A cette fin, l'ONU a élaboré un modèle de développement du cybergouvernement comportant cinq phases distinctes, chaque phase étant caractérisée à l'aide d'indicateurs pertinents.

L'OCDE a créé au début des années 2000 un Groupe de travail sur le cybergouvernement, dont les travaux ont donné lieu à la publication de deux livres traitant de nombreuses questions fondamentales en matière de cybergouvernement: "L'administration électronique: un impératif" en 2003, et "E-Governement for better governement" en 2004. Ces ouvrages ont été suivis d'études nationales sur le cybergouvernement concernant, entre autres, la Finlande (2003), le Mexique (2004), la Norvège (2005), la Hongrie (2007), les Pays-Bas (2007), la Turquie (2007). Le niveau de développement du cybergouvernement et les efforts fournis en ce domaine dans chaque pays ont été examinés afin de formuler des recommandations en matière de politiques. L'OCDE a continué à étudier la question du cybergouvernement en menant des recherches thématiques, qui ont donné lieu à des publications telles que: "Benefits Realisation Management" et "E-Government as atool for transformation" en 2007, et "An Economic Framework to Assess the Costs and Benefits of Digital Identity Management Systems for E-Government Service" en 2009.

Les travaux de la Banque mondiale en matière de cybergouvernement visent à aider les pays clients à se doter des capacités institutionnelles nécessaires à la mise au point d'applications de cybergouvernement qui permettront d'améliorer la qualité de fonctionnement et la responsabilisation de l'administration publique, notamment en ce qui concerne la fourniture de services au public. Le Département global des TIC de la Banque mondiale fournit des avis techniques ainsi qu'une aide à l'investissement pour la conception et le déploiement de solutions et d'applications de cybergouvernement. Celles-ci englobent les stratégies, les politiques, les aspects réglementaires et juridiques, les cadres institutionnels, l'architecture d'entreprise et les normes d'interopérabilité, les infrastructures et les services partagés, la gestion de la formation et du changement, les applications de cybergouvernement et les systèmes de

financement innovants, tels que les partenariats public-privé. La Banque mondiale soutient notamment la Tunisie, la Mongolie, le Ghana et le Rwanda.

2 Principes du cybergouvernement

2.1 Qu'est-ce que le cybergouvernement?

Créé au début des années 90, le concept de cybergouvernement associe deux mots fortement hétérogènes. Alors que l'un est un terme très technique, l'autre s'emploie depuis longtemps de manière courante pour parler du système de gouvernance. Si ce mot nouveau n'a pas été facilement accepté dans les tous premiers temps qui ont suivi son introduction, il est rapidement devenu l'objectif incontournable de la plupart des pays cherchant à transformer l'administration publique pour en faire une structure moderne et innovante. Selon les futurologues, la transformation de l'administration publique devrait donner naissance à un système de gouvernance révolutionnaire.

Des organisations internationales, telles que l'OCDE et l'ONU, donnent une définition du cybergouvernement. L'OCDE définit le cybergouvernement comme "l'usage des technologies de l'information et de la communication (TIC), et en particulier de l'Internet, en tant qu'outil visant à mettre en place une administration de meilleure qualité" (OCDE, 2003). L'ONU le décrit comme un mode d'administration publique qui met en application les TIC pour transformer les relations internes et externes. La finalité du cybergouvernement est d'établir une "bonne gouvernance", c'est-à-dire de rendre l'administration publique aussi efficace et pratique que possible du point de vue du public. Il vise à façonner le cadre des TIC de telle sorte que celles-ci deviennent un facteur clé pour assurer le passage à une administration publique claire, transparente et efficace.

Le cybergouvernement consiste essentiellement à transformer l'administration publique afin d'instaurer de nouvelles relations internes et externes à l'aide des technologies électroniques. Dès lors, comme l'indique l'OCDE (2003), l'accent en matière de cybergouvernement devrait être mis davantage sur "gouvernement" que sur "cyber-". En vertu de ce principe, les questions relatives au cybergouvernement s'inscrivent dans le contexte de la réforme de la gestion publique nationale et des initiatives en faveur d'une bonne gouvernance. Autrement dit, loin de se limiter à une affaire d'innovation technique, le cybergouvernement a pour objet la réforme de l'administration publique. Visant à répondre d'une part aux besoins du secteur public, et, d'autre part, à ceux des citoyens et des entreprises, il permet de garantir la mise à profit des TIC pour transformer les opérations internes au sein des organismes gouvernementaux ainsi que les modalités d'interaction entre le secteur public et le secteur privé.

Etant donné que le cybergouvernement correspond à une recherche de transformation des processus opérationnels internes et des relations externes avec les citoyens, il convient de le considérer en tant que processus, c'est-à-dire continuellement soumis à des modifications tandis que les fonctions de l'administration publique évoluent sous l'influence des changements sociaux.

2.2 Tendance de l'évolution des TIC au service du cybergouvernement

2.2.1 Caractéristiques des TIC utilisées pour le cybergouvernement

Dans le monde actuel, placé sous le signe de la technologie, les TIC sont déjà la clef de voûte du processus de transformation de l'administration publique. L'usage des TIC dans les administrations publiques est désormais bien établi, celui-ci faisant partie intégrante de la conduite de leurs activités. L'infrastructure de l'information et, en particulier, la technologie Internet, se caractérisent par un certain nombre d'avantages liés à leur nature, tels que l'ouverture, les connexions, l'accessibilité, etc. Par conséquent, les TIC ont fait l'objet d'une attention nationale en tant que vecteur déterminant de transformation. Les questions relatives au cybergouvernement s'inscrivent dans le cadre de la transformation de l'administration publique et des modalités d'interaction entre les organismes gouvernementaux et les

citoyens. Par ailleurs, les TIC sont un outil efficace pour améliorer l'engagement des citoyens dans l'élaboration des politiques publiques. L'application des TIC permet de supprimer les cloisons entre les organismes, ce qui est essentiel pour transformer les structures de gouvernance, de manière à rationaliser et simplifier les administrations publiques et, dans certains cas, à supprimer les doubles emplois. En outre, les TIC améliorent l'accessibilité des organismes gouvernementaux au public, ce qui se traduit par la participation des citoyens au processus décisionnel.

2.2.2 Comparaison fixe/mobile

Dans les premiers temps de l'application des TIC à la transformation de l'administration publique, la plupart des initiatives en matière de cybergouvernement reposait sur l'utilisation des technologies de l'Internet fixe. Les transactions en ligne s'effectuaient sur les réseaux de communication fixes, qui avaient été installés sous terre pour servir d'infrastructure nationale de l'information. L'accès à des services de cybergouvernement n'était possible que depuis un nombre d'endroits restreint, habitations ou bureaux, par l'intermédiaire des lignes de télécommunication filaires. Toutefois, alors que la diffusion des technologies mobiles atteint un niveau élevé[1], l'Internet mobile et l'accès hertzien aux administrations publiques commencent à avoir une incidence considérable sur l'environnement du cybergouvernement. Les technologies mobiles renforcent les capacités du secteur public à tirer parti de l'usage des TIC pour améliorer ses opérations internes ainsi que ses interactions avec les citoyens et les entreprises. Il en résulte que le cybergouvernement s'étend à l'administration publique sur mobile, ou qu'il évolue vers ce nouveau mode de gouvernance, lequel marque l'émergence des applications TIC de prochaine génération dans le secteur public.

Dans les pays en développement, le niveau d'accès au large bande fixe est plus bas que le niveau d'accès aux technologies mobiles. Cette situation est due au coût élevé des technologies filaires et de l'infrastructure nécessaire au déploiement de l'Internet large bande fixe. Parce qu'elles créent de nouvelles voies de communication assurant une desserte plus large, les technologies mobiles permettent de fournir un accès dans des zones où l'Internet fixe et la téléphonie filaire ne constituent pas une option viable en raison de l'infrastructure nécessaire à leur déploiement (OCDE et UIT, 2011). Les dispositifs mobiles bon marché et prêts à l'emploi suppriment les obstacles à l'accès des citoyens dans des zones où les services Internet fixes étaient très limités.

Si, à leurs débuts, où seuls les réseaux 2G étaient disponibles, les technologies mobiles passaient pour un piètre moyen d'accéder à un large éventail d'informations et de services, les smartphones, qui coïncident avec l'arrivée des réseaux 3G et 4G, offrent des possibilités sans précédent en matière de fourniture de services publics aux citoyens et aux entreprises. Par ailleurs, les technologies mobiles améliorent les possibilités de communication en temps réel entre les administrations publiques et les citoyens, ce qui permet aux fonctionnaires de comprendre les besoins des citoyens et de leur proposer des solutions pertinentes avec une grande réactivité. Réciproquement, la communication en temps réel permet aux citoyens de mieux comprendre les administrations publiques, ce qui augmente leurs possibilités de participation au processus décisionnel.

2.2.3 Pour un cybergouvernement mobile et social

Du point de vue du lien entre l'évolution des TIC et les initiatives de cybergouvernement, il convient de prendre en considération les technologies sociales, qui permettent aux administrations publiques de solliciter en amont les citoyens pour des retours d'information sur les politiques publiques en vue de les perfectionner. En utilisant des médias en ligne tels que Facebook, Twitter, etc., sur lesquels les citoyens se

[1] Les réseaux mobiles sont accessibles à 90% de la population mondiale, et à 80% de la population des zones rurales. Dans les pays de l'OCDE, le nombre d'abonnements au large bande mobile a augmenté à un taux de croissance équivalent annuel de 20% entre 2007 et 2009 (OCDE et UIT, 2011).

rendent régulièrement, les administrations publiques entrent en rapport direct avec eux et suivent ce qu'ils disent au sujet des opérations publiques et des services fournis. Lorsque les technologies sociales sont associées aux dispositifs mobiles, cela augmente leurs retombées pour les administrations publiques.

Au lieu de répondre de manière passive aux demandes des citoyens, les administrations ont la possibilité de participer aux conversations qui ont lieu sur de nombreux sites de médias sociaux, de manière à apprendre ce que les gens pensent de la qualité des programmes d'administration publique. Si, à ces débuts, le cybergouvernement consistait simplement à fournir des informations aux citoyens et à répondre à leurs demandes concernant les services publics sur les sites web des administrations publiques, il ne peut plus se limiter aujourd'hui à attendre de manière passive les demandes de renseignements et les plaintes du public. La nouvelle voie ouverte par l'importance grandissante des technologies sociales dans les TIC débouche sur de nouvelles perspectives pour les initiatives de cybergouvernement.

2.2.4 Les données publiques en libre accès comme tendance en faveur d'une administration publique placée sous le signe de la transparence, de la responsabilisation, de la participation et de la collaboration[2]

Ces dernières années, on observe dans un certain nombre de pays une tendance aux données publiques en libre accès, qui vise à la cocréation de valeur publique entre le secteur privé, la société civile et les citoyens. Ce paradigme politique est basé sur les principes de transparence, de participation et de collaboration. Il s'agit d'un changement culturel, qui fait des administrations publiques, des citoyens et des autres parties prenantes de la société des partenaires. Les valeurs fondamentales des données publiques en libre accès peuvent se résumer comme suit: i) Transparence: Les administrations publiques devraient fournir aux citoyens des renseignements sur leurs activités, de façon à garantir une gouvernance responsable; ii) Participation: Les administrations publiques devraient solliciter activement des avis d'expert et consulter tous les secteurs de la société, de manière à élaborer des politiques en disposant des informations les plus pertinentes; iii) Collaboration: Les fonctionnaires devraient collaborer avec les citoyens et le secteur privé dans le cadre de leur travail de résolution de problèmes aux niveaux local et national.

La société de l'information entraîne une évolution des points de vue sur les institutions sociales et leurs domaines de responsabilisation. Dans le monde entier, les administrations publiques s'ouvrent de plus en plus et partagent une quantité croissante d'informations avec les citoyens, les médias et autres parties prenantes, à la suite de la large adhésion aux principes de bonne gouvernance, qui sont les fondements des politiques visant à instaurer la paix et à atteindre les objectifs de développement.

Les données publiques en libre accès jouent le rôle de pilier dans l'élaboration d'une stratégie de gouvernance axée sur la transparence. Ce terme signifie que les organismes gouvernementaux mettent leurs données en ligne, de sorte que celles-ci puissent être lues par les humains et traitées par les machines (de préférence sous forme de données brutes ou structurées dans des formats ouverts qui puissent être pris en charge par les machines, et sous licence libre de sorte que les données soient réutilisables par des tiers). Le public peut examiner et télécharger les données, et même s'en servir comme base pour créer de nouvelles analyses et applications.

Les données publiques en ligne permettent d'atteindre des niveaux inédits d'engagement civique et de responsabilisation et de transparence des pouvoirs publics, et, partant, d'améliorer la fourniture des services publics et l'utilisation des ressources publiques. En dépit des nombreuses difficultés liées à la fracture numérique qui existe entre "les pays se situant à des stades différents de développement et qui a des incidences sur de nombreuses applications utiles d'un point de vue économique et social dans des

[2] D'après un document du BDT.

domaines comme la gouvernance, la santé et l'éducation", les administrations publiques partout dans le monde utilisent de plus en plus l'Internet afin de partager des données aux niveaux national, régional et local.

La valeur intrinsèque et les avantages potentiels des données publiques en libre accès semblent relativement clairs, bien qu'il soit possible d'élargir notre imagination collective par des échanges actifs d'idées et d'expériences. Les pouvoirs publics rencontrent des difficultés à tous les niveaux (national, régional et local) pour lancer et maintenir des initiatives en matière de données en libre accès, en raison du manque de compréhension des avantages qu'elles représentent de la part des décideurs et des parties prenantes, ainsi que de connaissances techniques insuffisantes.

Par conséquent, il est nécessaire de renforcer les capacités des fonctionnaires, ainsi que celles des parties prenantes issues du secteur privé, des milieux scientifiques et de la société civile, à concevoir, mettre en oeuvre et évaluer des formes d'initiatives présentant un caractère durable en matière de publication des données. Si l'on reconnaît largement les avantages généraux que peut avoir pour la société et la démocratie le fait d'améliorer la transparence, la responsabilisation, la dimension participative et l'efficacité de l'administration publique, des études récentes montrent que les données publiques en libre accès ont également des effets positifs sur l'économie, en ce sens qu'elles permettent de créer de nouveaux produits et de nouveaux services basés sur leur réutilisation.

Un large éventail d'indicateurs sont actuellement utilisés afin d'évaluer la qualité de fonctionnement de l'administration publique, en particulier dans le domaine du cybergouvernement. L'un des défis de l'administration publique de demain consiste à concevoir et à mettre en oeuvre de nouveaux systèmes de mesure visant à établir des critères de référence relatifs à la qualité de fonctionnement des administrations publiques, afin de garantir les possibilités de suivi et d'amélioration de l'engagement des citoyens et des données publiques en libre accès. Il est nécessaire d'établir des critères de référence en ce qui concerne l'état de "préparation à la transformation" des administrations publiques, ainsi que les améliorations de la "valeur publique" du point de vue des citoyens. Les initiatives qui ont vu le jour dans le monde ces dernières années en matière de données publiques en libre accès, tendent à prouver que les parties prenantes n'ont pas encore bien compris les avantages potentiels de cet outil, que ce soit en matière de transparence et de responsabilisation des administrations publiques, ou en termes de retombées sur le plan économique et social.

2.3 Composants du cybergouvernement

2.3.1 Portail, échange d'informations, sécurité

Les portails de l'administration publique sont un composant essentiel du cybergouvernement, qui permet aux citoyens et aux entreprises d'accéder facilement aux renseignements et aux services publics. L'idée fondamentale qui sous-tend la création d'un portail de l'administration publique est de regrouper les renseignements et les services fournis par les divers organismes et de créer un point d'accès unique à l'ensemble de ces renseignements et de ces services. Les citoyens et les entreprises sont mieux informés lorsqu'ils souhaitent connaître l'identité, le département et le niveau du responsable de certains renseignements ou d'un certain programme concernant l'administration publique. S'ils ont la possibilité d'interagir facilement avec les pouvoirs publics et d'accéder à des documents officiels et à des actes administratifs, les citoyens feront preuve d'une plus grande volonté de participer au processus d'administration publique, ce qui se traduira par un renforcement de la dimension participative des modèles de gouvernance, d'où un élargissement du rôle joué par les citoyens dans les processus décisionnels associés à ces modèles. Le portail constitue un outil puissant pour classer et intégrer la grande quantité d'informations relevant de l'administration publique.

En raison de l'évolution des technologies de cybergouvernement vers les technologies mobiles et sociales, le portail fait l'objet d'une restructuration qui vise à en faire un lieu où les pouvoirs publics vont au-devant des citoyens pour solliciter leurs réactions, et consultent l'ensemble des secteurs de la société de manière à prendre des décisions qui servent au mieux l'intérêt général. Les fonctionnaires sont en mesure

d'obtenir des informations concernant l'opinion des personnes sur les politiques d'administration publique. Plutôt que de répondre de manière passive à des demandes provenant de l'extérieur, les organismes gouvernementaux s'attachent à comprendre les besoins des personnes afin de satisfaire leurs exigences.

Le partage de l'information, qui permet de refondre et d'intégrer les processus opérationnels de l'administration publique, constitue un élément essentiel de la mise en oeuvre du cybergouvernement. L'idée de base du partage de l'information est de stocker les informations une seule fois, plutôt que de répéter l'opération à plusieurs reprises, de sorte que les citoyens et les entreprises n'ont pas à fournir les mêmes informations à différentes administrations publiques. Les citoyens n'ont pas à se rendre autant de fois dans les bureaux des administrations publiques et ont moins de pièces justificatives à soumettre lorsqu'ils demandent à bénéficier d'un certain service.

Le partage de l'information vise à englober le concept selon lequel les pouvoirs publics recueillent des informations une fois auprès des citoyens et des entreprises, de sorte que toutes les administrations publiques puissent ensuite les utiliser. Les informations sont une ressource essentielle à la conduite efficace de l'administration publique. Il arrive fréquemment que différents organismes demandent des informations concernant l'identification des citoyens, par exemple, pour leur imposition ou le renouvellement de leur permis de conduire. La situation serait moins pesante pour les citoyens et les entreprises si, lorsqu'ils entrent pour la première fois en rapport avec une administration publique en vue de bénéficier d'un service particulier, ils devaient uniquement fournir des informations supplémentaires. Les points à prendre en considération dans le domaine du partage de l'information sont les technologies habilitantes, les aspects juridiques, les dispositions institutionnelles et la culture organisationnelle. Cette dernière fait l'objet de beaucoup d'attention, car l'échec du partage de l'information est mis sur le compte d'un égoïsme organisationnel favorisant une vision de l'information comme source de pouvoir, vision à l'origine des réticences vis-à-vis du partage de l'information.

L'une des questions les plus sensibles en matière de partage de l'information concerne les risques d'intrusion dans les données personnelles et la faiblesse de la sécurité des réseaux. On ne saurait trop souligner l'importance de la protection de la confidentialité et de la sécurité dans le cadre de la promotion du cybergouvernement. Aussi pratique et efficace que soit le système, à défaut d'une protection sûre de la confidentialité, son adoption se heurtera à la résistance des utilisateurs, et la confiance de ces derniers sera difficile à rétablir. Il est possible d'assurer la protection des données personnelles à l'aide de mesures techniques, mais aussi juridiques, organisationnelles et culturelles. Si le partage de l'information est un élément essentiel du cybergouvernement et un prérequis de la promotion des applications TIC, la protection des informations est une mesure de prévention contre les incidents de fuite de données personnelles susceptibles de survenir dans le cadre du partage de l'information.

2.3.2 Réseaux, capacités humaines

Les réseaux haut débit sont une infrastructure fondamentale pour permettre aux fonctionnaires d'accéder à des bases de données et à des applications diverses. Des prérequis existent non seulement en ce qui concerne les interconnexions entre les organismes gouvernementaux, c'est-à-dire entre les administrations publiques centrales et locales, ainsi qu'entre les ministères, mais aussi pour que les citoyens et les entreprises puissent interagir avec les administrations publiques lors de leurs demandes de renseignements et de services. Le cybergouvernement peut assurer la fourniture de services publics, tels que la santé et l'éducation, par l'intermédiaire des réseaux large bande. Les systèmes de cybersanté sont utilisés pour fournir des services à distance aux habitants des zones rurales, tandis que les systèmes de cyberapprentissage offrent aux élèves la possibilité de recevoir, en dehors du cadre de leur scolarité, des ressources d'apprentissage dont ils ne pourraient pas disposer dans leur établissement.

La capacité des utilisateurs à se servir des systèmes mis en oeuvre est primordiale en vue de tirer pleinement avantage du cybergouvernement. Lors de la phase initiale de mise en oeuvre du cybergouvernement, il est souvent arrivé que le niveau d'utilisation du système soit si bas que les investissements dans le cybergouvernement ont été qualifiés de gâchis. Parmi les diverses raisons à

l'origine de ces critiques, l'incapacité des utilisateurs à se servir du système a souvent été mise en avant. Lors de la phase initiale de mise en oeuvre du cybergouvernement, il est primordial d'organiser des formations aux compétences Internet de base, à l'intention, notamment, des personnes vivant dans des zones isolées. Cette question a été abordée dans le cadre des discussions relatives à la fracture numérique. Si les disparités dans l'utilisation des services de cybergouvernement ont parfois à voir avec les installations techniques, notamment en cas de manque d'équipements ou de connexions Internet large bande à un prix abordable, c'est principalement en raison de l'insuffisance des capacités humaines qu'il n'est pas possible de tirer pleinement avantage des systèmes mis en oeuvre. Il est fortement recommandé, lors de l'élaboration d'un plan national pour les TIC englobant les services de cybergouvernement, de prévoir des programmes de formation aux TIC à l'intention des fonctionnaires et des citoyens, en particulier dans les zones rurales.

2.4 Catégories d'activités relatives au cybergouvernement

2.4.1 Applications: services G2G, G2C et G2B

Les sigles G2G et G2C s'emploient respectivement pour désigner les services fournis à l'intérieur des pouvoirs publics ("Government to Government") et par les administrations publiques aux citoyens ("Government to Citizens"). Le sigle G2B désigne les services fournis par les administrations publiques aux entreprises ("Government to Business"), catégorie de services qui, du point de vue des caractéristiques des applications de cybergouvernement, est très proche de la catégorie G2C. Les services G2G relèvent des initiatives de cybergouvernement portant sur les activités d'arrière-guichet (back office), tandis que les services G2C et G2B ont trait aux interactions entre les pouvoirs publics d'un côté, et les citoyens et les entreprises de l'autre, c'est-à-dire aux activités de guichet (front office).

La catégorie G2G se compose des initiatives dont la principale finalité est l'innovation en matière de méthodes de travail, c'est-à-dire, par exemple, la mise en place de méthodes de travail électroniques, le développement du partage de l'information administrative et la restructuration des méthodes opérationnelles axées sur les services. Par exemple, les systèmes de gestion électronique des documents, les systèmes de financement des administrations publiques locales et centrales, les systèmes d'audit électronique, etc. appartiennent à la catégorie G2G.

Les catégories G2C et G2B regroupent les applications ayant pour objet l'innovation en matière de services aux citoyens et aux entreprises. En République de Corée, les services G4C (Government for Citizens) représentent la catégorie d'applications G2C. Par ailleurs, le système national de protection sociale, le système d'information sur les produits alimentaires et les médicaments, et le système d'information sur l'emploi et la recherche d'emploi, sont des exemples d'applications G2C. Dans la catégorie G2B, celle de l'innovation en matière de services aux entreprises, figurent le service du portail des entreprises concernant les tâches administratives des sociétés, l'information industrielle, ainsi que d'autres services supplémentaires liés à des activités diverses à tous les stades du cycle de vie de l'entreprise, depuis son lancement jusqu'à sa cessation d'activité. Les systèmes d'information sur les flux logistiques, les entreprises étrangères, etc. font également partie de cette catégorie. Dans la catégorie des applications G2C figure également un système visant à encourager la participation des citoyens au processus de prise de décision dans le secteur public, ce qui revêt une grande importance dans l'optique de la cyberdémocratie. Ce système vise à renforcer les moyens dont disposent les citoyens pour exprimer leurs opinions sur des politiques particulières et interagir avec les pouvoirs publics à tous les niveaux.

2.4.2 Financement

La taille du fonds requis par les initiatives de cybergouvernement est telle qu'il convient d'élaborer avec soin un plan fixant les modalités de leur financement. Afin de faciliter la mobilisation des ressources nécessaires à la mise en oeuvre des projets de cybergouvernement, de nombreux pays en développement s'appuient sur leurs dirigeants politiques, qui reconnaissent l'importance cruciale du cybergouvernement. Cette stratégie est celle qu'utilise la République de Corée lors de la phase de lancement de projets nationaux de technologies de l'information. Etant donné qu'il était très difficile, de par la nature des technologies de l'information, de mettre en évidence les avantages liés à l'investissement dans ce secteur, le Gouvernement coréen a décidé de mettre de côté une certaine quantité de fonds exclusivement réservée aux projets de technologies de l'information, sur la base de décrets pris par le Président de la République.

Le problème du financement des projets de technologies de l'information donne lieu à un débat sur l'équilibre entre l'offre et la demande. Dans les milieux universitaires, il est communément admis que si l'on souhaite stimuler l'innovation technologique et le lancement de nouvelles applications, il est politiquement plus efficace d'intervenir du côté de la demande que du côté de l'offre. Le risque de mauvaise affectation de fonds publics est élevé en cas d'incompréhension du côté de la demande. La question fondamentale lorsqu'on s'intéresse au côté de la demande d'un projet est la suivante: quels types de service justifient l'énorme investissement requis par les projets de cybergouvernement? Cette question se pose en raison du risque de créer une solution coûteuse à laquelle ne correspond aucun problème.

A ce stade, nous nous retrouvons malheureusement face à un dilemme. En effet, il semble qu'un certain nombre de projets liés aux technologies de l'information aient créé un type de demande qu'il est pratiquement impossible de prévoir avant que l'offre ne soit disponible. En raison de ce dilemme, les premiers projets de cybergouvernement sont menés conformément à la théorie de l'offre. C'est à la stratégie prônée par les tenants de cette théorie que répond le mécanisme de financement utilisé lors de la phase de lancement du cybergouvernement dans des pays comme la République de Corée. Toutefois, le fait de mettre l'accent sur l'offre ne doit pas nous faire perdre de vue qu'il est important de tenir compte de la demande potentielle d'un service de cybergouvernement. Par exemple, lorsqu'il est question de décider sur quels services faire porter les initiatives de cybergouvernement, nous pourrions traiter les aspects relatifs à la demande en examinant les transactions hors ligne entre les administrations publiques et les citoyens.

2.4.3 Dispositions juridiques et institutionnelles

Lors du processus d'élaboration des activités de cybergouvernement, la mise en place des dispositions juridiques et règlementaires correspondantes est une condition nécessaire du succès, car la mise en oeuvre des méthodes de travail de l'administration publique a lieu dans la stricte application de la législation. Par exemple, si les documents papier avaient dans le passé valeur de preuve juridique en matière de gestion de la gouvernance, l'instauration de systèmes de cybergouvernement a donné lieu à l'introduction des documents électroniques pour conduire l'administration publique, d'où la nécessité d'établir des dispositions juridiques pour ce type de document. La mise en place de dispositions concernant la valeur de preuve juridique s'effectue en regroupant et en coordonnant des fonctions de gouvernance analogues qui, auparavant, relevaient de plusieurs organismes gouvernementaux différents.

Afin d'établir une base institutionnelle pour le cybergouvernement, il convient d'amender les lois et décrets concernant les affaires civiles ayant été élaborés dans le cadre de l'environnement hors ligne, de sorte qu'il y soit traité de la conduite des affaires civiles à l'aide des technologies numériques. Même après la mise en oeuvre technique des systèmes de cybergouvernement, la façon de travailler et de penser des fonctionnaires et des citoyens n'évoluera que si la législation et la réglementation relatives au fonctionnement du cybergouvernement sont mises en place à leur intention.

L'utilisation d'un système de gouvernance informatique pour assurer le bon déroulement des activités de cybergouvernement occupe une place essentielle dans les dispositions institutionnelles, car c'est elle qui permet d'assurer la solidité de la structure organisationnelle. Etant donné que les projets de cybergouvernement, pour la plupart d'entre eux, concernent en général plusieurs organismes, ils sont très exposés aux conflits qui viennent perturber le processus normal de mise en oeuvre du cybergouvernement. Afin de garantir la coordination entre les organismes concernés, un comité ad hoc est chargé de résoudre les différends entre eux. Ce comité ne se compose pas uniquement de membres des organisations auxquelles s'appliquent le projet, mais aussi de professionnels indépendants censés adopter une position neutre lors du processus de coordination.

3 Bonnes pratiques appliquées par les pays Membres (contributions aux travaux de l'UIT-D)

Au cours des trois ans de la troisième période d'études (2010-2012), 12 cas d'initiatives de cybergouvernement ont été soumis à la Commission d'études à sa réunion de septembre. Deux cas concernant le Bangladesh ont été réduits à un en raison de la similarité de leur contenu. Des résumés de chaque contribution sont présentés ci-après suivant leur ordre chronologique de soumission. Les textes intégraux de chaque contribution sont reproduits en annexe à la fin du Rapport.

3.1 Projet INV (Information Network Village, Village réseau d'information) (République de Corée)

Ce projet vise à permettre aux habitants des zones isolées d'accéder à de riches contenus dans des domaines tels que l'éducation, la médecine et l'agriculture, de façon à réduire la fracture numérique entre les zones urbaines et les zones rurales. Il prévoit également la fourniture de moyens permettant de vendre directement des spécialités locales aux consommateurs, ce qui augmente les gains retirés de la production locale. Par conséquent, ce projet contribue à stimuler l'économie locale dans le but d'équilibrer le développement à l'échelle nationale. On s'attend à ce que le fait de former les habitants aux compétences de base en matière d'Internet entraîne une augmentation de la demande de services de cybergouvernement[3].

- Construire une infrastructure Internet large bande dans des villages d'agriculteurs/de pêcheurs, dans des zones isolées et dans d'autres endroits où la révolution de l'information n'avait pas eu lieu, en vue de combler l'écart dans ce domaine entre zones urbaines et zones rurales. On espérait en outre consolider les bases du cybergouvernement et de la démocratie électronique.
- Créer du contenu d'information, notamment un marché en ligne pour les produits locaux afin de générer des avantages pratiques et de moderniser les économies locales pour permettre un développement national équilibré.
- Le projet a également été conçu de manière à permettre à la population locale d'accéder plus facilement à l'information en matière d'éducation, de médecine, de culture et d'agriculture.
- Un "Comité de gestion du Projet INV" a été créé pour chaque village. Le Comité a identifié des éléments essentiels concernant le fonctionnement du village réseau d'information. L'élaboration d'un modèle économique a également été encouragée, afin que le Comité puisse fonctionner de façon autonome, même en l'absence d'aides publiques. Chaque village ayant ses propres caractéristiques, les modèles INV ont été élaborés avec soin, en fonction des besoins locaux, puis répartis dans l'ensemble du pays après une évaluation stricte.

[3] Présenté à la première réunion de la Commission d'études 2, le 14 septembre 2010.

- La réussite du projet tient en premier lieu au fait qu'il prévoit l'apprentissage de l'utilisation des systèmes d'information.
- Ce programme prévoit l'organisation de différentes manifestations afin de mieux faire connaître le projet INV auprès du public.
- Le projet INV vise à doter la population locale de capacités accrues dans le domaine des technologies de l'information afin de lui permettre de survivre dans une société de l'information qui évolue rapidement. Par exemple, l'un des objectifs est de proposer aux populations locales des services publics en ligne dans le cadre du projet de cybergouvernement local.
- Le projet INV a permis d'obtenir les résultats décrits ci-après. Tout d'abord, la mise en oeuvre des initiatives susmentionnées a contribué à réduire la fracture numérique du fait du renforcement de l'utilisation de l'Internet par les "démunis" de l'information que sont par exemple les populations rurales.
- Les populations des zones isolées ont pu profiter de ces services de cybergouvernement grâce aux formations dispensées dans le cadre du projet INV.
- En outre, plusieurs dispositions ont été mises en place afin de renforcer l'attractivité du projet INV, comme celle consistant à inclure le programme de commerce électronique dans le projet INV, de façon à augmenter les bénéfices retirés de la vente de produits en ligne.
- D'autres pays prennent pour référence le projet INV, destiné à réduire la fracture numérique dans les zones ayant un accès limité à l'information comme les villages d'agriculteurs ou de pêcheurs.
- Les villages participants sont invités à nouer des partenariats avec des entreprises privées souhaitant créer des villages dans le cadre du projet INV.
- A l'occasion d'un déplacement dans un village réseau d'information, un cadre d'Intel (premier fabricant mondial de puces) a salué le projet coréen INV comme étant un exemple sans équivalent de mise en place du numérique dans les villages d'agriculteurs ou de pêcheurs.

3.2 Système coréen de passation des marchés publics en ligne (KONEPS) (République de Corée)

Le système KONEPS traite de façon électronique la totalité des opérations relatives aux marchés publics, de la parution des appels d'offres au paiement en passant par l'attribution et l'établissement des contrats. Dans la mesure où le système se connecte aux services d'échange de données du gouvernement, il n'est plus nécessaire de soumettre des documents papier tels que les certificats d'inscription au registre du commerce ou des attestations fiscales. Le système permet d'accéder à une version numérisée de 160 formulaires officiels (réponses aux appels d'offres, contrats, demande d'inspection et demande de paiement) qui sont ainsi traités de façon électronique. Etant donné qu'il permet de traiter en ligne les processus relatifs aux paiements (y compris les rapports de recettes, les demandes d'inspection et la facturation), il peut réduire concrètement les délais de paiement, car les différentes unités chargées d'établir les contrats, de mener les inspections et de procéder aux paiements entrent les tâches qu'elles ont menées à bien dans le système commun, ce qui permet de rationaliser les processus relatifs aux paiements.

Il a été décidé que les différents organismes ne devraient pas élaborer chacun leur propre système d'achat électronique. Au contraire, il a été proposé d'élaborer un système type à utiliser moyennant quelques adaptations. Des lignes directrices destinées à éviter les doublons sont parues en juin 2001 et visaient à éviter les gaspillages budgétaires. La révision de la législation et de la réglementation dans la mise en oeuvre des projets de cybergouvernement n'est pas moins importante que la conception du système en lui-même[4].

- Les technologies d'infrastructure utilisées pour le système KONEPS comprennent une signature électronique fondée sur une infrastructure de clés publiques (PKI), une technologie de sécurisation des documents, des normes d'échange de données informatisé et des services web à grande échelle.
- Le système KONEPS permet la publication électronique des informations relatives à tous les appels d'offres lancés par des organismes publics et représente ainsi un guichet unique pour la passation des marchés publics.
- Le système KONEPS est également relié au système de comptabilité publique, d'où la possibilité pour les services d'achats de gérer les paiements par transfert de fonds électronique.
- Le service PPS (Public Procuring Service) a continué à développer le service de passation de marchés sur téléphone mobile et, avec l'explosion de l'utilisation des smartphones, les services mobiles deviendront de plus en plus populaires dans le domaine des achats.
- Le système KONEPS a permis d'améliorer considérablement la transparence du processus de passation des marchés publics.
- Lors du Congrès mondial des technologies de l'information, le service PPS a été désigné organisme public le plus innovant pour ces services utilisant les technologies de l'information.
- Afin de développer la forme intégrée du système de passation des marchés, le système KONEPS a été examiné selon les trois différents points de vue, à savoir les services, les données et l'architecture technique.
- En outre, le système KONEPS sera intégré au système de travail du service PPS (Public Procuring Service), de sorte que les fonctionnaires de ce service puissent tirer pleinement parti des initiatives de cybergouvernement.
- Actuellement, les données font l'objet d'un traitement séparé suivant le type d'éléments de service et de méthodes de travail au sein des structures PPS.
- Enfin, sur la base de l'intégration des services d'achat et du réalignement des données résultant de l'exploitation du système KONEPS, il sera procédé à l'analyse de la structure du système, et celui-ci sera reconçu conformément au cadre eGovFrame, un cadre de référence pour l'élaboration d'applications de cybergouvernement.

3.3 Sur la voie du cybergouvernement (Ouganda)

Le Gouvernement de l'Ouganda est fermement convaincu que les TIC peuvent non seulement révolutionner le mode de fonctionnement du Gouvernement, mais aussi améliorer la relation entre l'Etat et ses administrés, entre l'Etat et les entreprises et entre l'Etat et ses organismes. Le Programme "Sur la voie du cybergouvernement" a débuté en Ouganda avec la politique en matière de TIC de 2003, qui insistait principalement sur la nécessité de construire une infrastructure TIC à l'échelle du pays. Une

[4] Présenté à la deuxième réunion de la Commission d'études 2, le 11 septembre 2011.

enquête sur l'état de préparation électronique du pays a été ensuite menée en 2004 et en 2005, les pouvoirs publics ont été formés aux méthodes de travail électroniques.

En 2006, avec l'aide du Gouvernement de la Chine, l'Ouganda a commencé à mettre en place une infrastructure de cybergouvernement dans tout le pays. La première phase du projet visait tous les grands ministères centraux établis à Kampala et Entebbe et concernait également les villes de Bombo, Jinja et Mukono. Le réseau permet de fournir des services vocaux, de vidéoconférence et de données de base aux ministères.

Les services entre ministères sont actuellement gratuits. Une expérience de collaboration est en cours entre quatre ministères, qui utiliseront la même plate-forme logicielle. La deuxième phase concerne les régions orientale, septentrionale et occidentale de l'Ouganda et a commencé fin 2011. Le secteur privé a également mis en place une infrastructure TIC dans l'ensemble du pays, laquelle peut être utilisée pour le cybergouvernement[5].

- Des lois régissant le cyberenvironnement ont été adoptées, à savoir la Loi sur les transactions électroniques, la Loi sur les signatures numériques et la Loi sur l'utilisation abusive de l'informatique, et entreront en application d'ici la fin de l'année.
- L'infrastructure nécessaire étant disponible, l'Ouganda a élaboré un cadre régissant la mise en oeuvre du cybergouvernement. Tous les gouvernements de district du pays disposent d'un site web élaboré dans le cadre du Programme de développement des communications rurales (RCDP). Des informations concernant les services publics, les investissements et les entreprises sont publiées sur ces sites web, malgré les problèmes que posent la mise à jour régulière des informations et le fait que les frais d'hébergement des sites et de l'Internet sont à la charge des districts.
- Le portail web du Gouvernement de l'Ouganda est en cours d'élaboration et servira de passerelle d'accès aux services publics comprenant des liens vers le secteur privé.
- En collaboration avec l'ONUDI, le Ministère des TIC met actuellement en place des centres d'information de district expérimentaux dans six districts (Mityana, Iganga, Lira, Rukungiri, Kamwenge et Busia) pour renforcer l'accès des citoyens aux services TIC.
- Un centre national de données destiné à faciliter le stockage, l'utilisation, le partage et la sécurité de nombreuses données publiques a été créé.
- Les initiatives menées par le secteur privé reposent pour la plupart sur la téléphonie mobile, étant donné qu'en Ouganda le taux de pénétration de la téléphonie mobile est supérieur au taux de pénétration informatique/Internet.

3.4 Mise en oeuvre de la connectivité large bande dans les zones mal desservies en Ouganda

La Commission des communications de l'Ouganda (UCC) a créé le Fonds pour le développement des communications rurales (RCDF) en vue de stimuler la fourniture de services de télécommunication dans les zones rurales ou mal desservies. Le RCDF est donc un mécanisme pour mettre à profit les investissements dans l'infrastructure et les services de communication dans les zones rurales mal desservies du pays.

[5] Présenté à la deuxième réunion de la Commission d'études 2, le 11 septembre 2011.

Il a ainsi été reconnu que, même si le secteur avait été libéralisé et s'était ouvert à la concurrence, certaines régions du pays qui n'étaient pas viables sur le plan commercial n'attireraient pas d'investissements privés dans l'infrastructure et les services. Les principaux objectifs du RCDF sont de fournir un accès aux services de communication de base à une distance raisonnable, de veiller à ce que des investissements soient effectivement consentis dans le développement des communications rurales et de favoriser l'utilisation des TIC en Ouganda.

La politique de l'Ouganda en matière d'accès universel (2010) suit les principes du programme de développement mondial que représentent les Objectifs du Millénaire pour le développement (OMD), auxquels l'Ouganda a souscrit, et du plan de développement national du pays (2010), qui était au départ lié à la vision nationale appelée Vision 2025. Cette politique est également le prolongement de la politique d'accès universel précédente (2001) et s'inscrit dans le cadre de la politique du pays en matière de TIC et télécommunications.

La faible pénétration de l'Internet dans les zones rurales tient principalement aux coûts de l'accès, à la largeur de bande insuffisante, aux problèmes d'alimentation électrique et, en particulier dans le cas des communautés rurales, à l'illettrisme et à l'absence de contenus locaux intéressants rédigés en langue vernaculaire. Par conséquent, le principal objectif de la nouvelle politique est de garantir la fourniture d'une connectivité large bande et d'appuyer l'élaboration de contenus locaux.

Toutefois, le principal handicap dont souffre aujourd'hui le secteur des TIC en Ouganda est l'absence de réseau d'infrastructure large bande pour assurer un accès plus rapide et favoriser l'utilisation des TIC en général et de l'Internet en particulier. Cette situation est surtout due aux énormes besoins de capitaux, auxquels le secteur privé seul ne peut pas répondre et qui supposent donc une intervention spéciale de l'Etat.

Le Gouvernement de l'Ouganda a entrepris d'appuyer l'interconnexion de toutes les grandes capitales locales et des principales villes à l'infrastructure dorsale nationale de données, afin de pouvoir fournir aux utilisateurs un large éventail de services TIC à moindre coût. Cette mesure devrait faciliter la mise en place de points d'accès aux services de données dans les établissements publics, dans un premier temps en priorité dans les établissements d'enseignement professionnel, universitaires et secondaires et dans les unités de santé publiques des niveaux IV et III. Une connectivité large bande sera assurée et permettra de raccorder des sous-provinces sélectionnées à l'infrastructure dorsale nationale haut débit. Il s'agit là d'une solution pour assurer la connexion du "dernier kilomètre" dans les sous-provinces. Pour ce faire, une étude détaillée est en cours en vue de déterminer les solutions technologiques les plus économiques (hertzien, câble) qui pourraient être mises en oeuvre pour chaque emplacement[6].

- **Cybergouvernement**: Le projet facilitera la collecte des données auprès des pouvoirs publics à tous les niveaux, des gouvernements locaux jusqu'au gouvernement central. Ces données seront prises en considération dans les statistiques démographiques nationales et dans d'autres statistiques socio-économiques.
- **Cyberéducation**: Le projet facilitera le cyberapprentissage, qui est de plus en plus répandu en Ouganda. Par exemple, les principales universités locales ont des campus satellites à l'intérieur du pays, où elles proposent maintenant un enseignement à distance et en ligne.
- **Cybersanté**: Le projet facilitera la transmission de données et les communications vocales depuis les communautés rurales vers les centres de santé, les hôpitaux de district, les hôpitaux référents régionaux et, enfin, l'hôpital référent national, et dans le sens inverse. On s'attend à un trafic supplémentaire entre le Ministère de la santé et les bureaux de district, ainsi qu'entre le Ministère et les centres de santé.

[6] Présenté à la deuxième réunion de la Commission d'études 2, le 11 septembre 2011.

En ce qui concerne l'Internet, la pénétration, l'accès et l'utilisation restent très faibles en Ouganda, le taux d'internautes étant estimé à environ 5% de la population totale. L'Internet reste en outre largement confiné aux centres économiques urbains, du fait des considérations commerciales des fournisseurs de services privés. Même si la politique appliquée auparavant par l'Ouganda consistait à financer l'installation de points de présence Internet dans tous les districts mal desservis, l'Internet haut débit et les questions liées à la qualité de service (pannes) sont les principales préoccupations des utilisateurs finals.

3.5 Système d'information des collectivités territoriales (LGIN)

La Constitution de la république de Corée stipule que "Les collectivités territoriales sont chargées des questions relatives au bien-être des résidents, à la gestion du foncier; elles peuvent, dans les limites de la loi, prendre des dispositions réglementaires relatives à leur autonomie locale". Lorsque ce projet a été mis en oeuvre, on comptait 16 gouvernements provinciaux, dont sept municipalités et neuf administrations provinciales, ainsi que 234 municipalités/districts. Les responsables des collectivités territoriales gèrent et supervisent les affaires administratives sauf si la Loi en dispose autrement. Les fonctions exécutives locales incluent celles qui sont déléguées par le gouvernement central, comme la gestion des propriétés du domaine public, la fourniture des services, le calcul des impôts, la collecte des impôts locaux et les redevances afférentes à divers services. Les gouvernements provinciaux disposent de services scolaires qui sont chargés des questions liées à l'enseignement et aux activités des élèves et des étudiants dans chaque communauté. Pour l'essentiel, les gouvernements provinciaux servent d'intermédiaire entre le gouvernement central et les subdivisions secondaires des collectivités territoriales (municipalité/district).

- Les administrés exercent de fortes pressions sur les gouvernements et demandent une diminution du coût des services officiels, une amélioration des services aux administrés et un partage plus efficace de l'information entre les zones de compétences.
- Les fonctionnaires sont confrontés à un nouvel environnement de travail dû à un système nouvellement mis en oeuvre comme le LGIN.
- Cette stratégie s'étend aux cas des processus opérationnels et des services d'application.
- Cela a permis de partager l'information entre agences gouvernementales, ce qui a contribué à l'amélioration du fonctionnement interne des collectivités territoriales et à l'efficacité du service public.
- De plus, les collectivités territoriales partagent entre elles informations et données, ce qui réduit le nombre de documents nécessaires à la fourniture des services publics.
- La simplification des flux de travail dans la réalisation du projet LGIN a éliminé les procédures qui se chevauchaient et les travaux de gestion nécessaires à la fourniture des services publics.
- La plus grande efficacité de l'administration publique conduira à une amélioration de l'environnement administratif et les administrés auront davantage confiance dans leur administration.
- Le système LGIN est une infrastructure d'information conçue pour tous les domaines du service public.
- Des services mobiles sont disponibles dans des zones d'application limitées.

Le système LGIN est nécessaire pour que les applications de cybergouvernement du gouvernement central prennent effet, étant donné que divers services publics organisés au niveau central sont supposés être répartis via les filières correspondantes des collectivités territoriales.

Les facteurs de succès du projet défini ci-dessus se mettent en ordre au fur et à mesure des enseignements que nous acquérons dans le cadre de notre expérience de la mise en oeuvre de ce projet. Le système LGIN a pu atteindre son niveau actuel de réussite en répondant efficacement aux questions résumées ci-après[7]:

- Comment régler le différend relatif au projet entre les organismes en présence.
- Comment financer le projet et répartir les coûts entre les collectivités territoriales et le gouvernement central.
- Comment traiter les chocs psychologiques de ceux qui acceptent le nouveau système technique et qui craignent la précarité de l'emploi.
- Comment éviter une perte importante provoquée par un échec potentiel dû à des processus compliqués de mise en oeuvre et à l'ampleur du projet conduit au niveau national.
- Comment obtenir le soutien des responsables politiques et des gouvernements afin de jouir de conditions favorables pour le financement et pour la révision des lois et des réglementations pertinentes, etc.

3.6 Aperçu des services fondés sur les TIC au Bangladesh

Bien qu'il compte parmi les pays les plus densément peuplés au monde, le Bangladesh reste l'un des pays du Sud de l'Asie où la télédensité est la plus basse. Jusqu'à présent, seule une proportion relativement faible de la population avait accès aux télécommunications. Il y a seulement 10 ans, la télédensité était inférieure à 1%, mais l'avènement de la téléphonie mobile a changé la donne et la télédensité s'élève aujourd'hui à 46% au Bangladesh.

La situation générale dans le pays s'est améliorée dans une certaine mesure grâce au développement rapide du marché mobile. L'utilisation des technologies de l'information et de la communication (TIC) dans les services publics s'est généralisée ces dernières années.

A ce jour, différentes technologies (échange de données informatisé, téléphonie interactive, messagerie vocale, courrier électronique, fourniture de services web, réalité virtuelle et infrastructure publique essentielle) ont été utilisées pour prendre en charge les fonctions particulières du cybergouvernement.

La cybergouvernance est l'utilisation des technologies de l'information par les services publics pour fournir des services et des informations et des activités destinées à encourager les citoyens à participer de façon démocratique au processus de décision en rendant le gouvernement plus transparent et plus responsable. Pour ce faire, il faut mettre au point un portail et un recueil d'informations officielles sur Internet de qualité pour que les citoyens aient accès à toutes les informations nécessaires auprès des différents ministères. Le public devrait pouvoir télécharger toutes sortes de formulaires et d'applications. En outre, pour réduire la bureaucratie, il est possible d'ajouter une fonctionnalité de soumission en ligne. Ce portail web destiné à renforcer la transparence et à faire baisser la corruption permet également de répondre aux appels d'offres, de remplir une déclaration d'impôt et d'attribuer des terrains. Cependant, il convient de ne pas se méprendre sur le fait que l'administration publique sur mobile ne représente qu'une des formes possibles de communication électronique avec les pouvoirs publics, et qu'elle n'a de sens que s'il existe un système de cybergouvernement[8].

[7] Présenté à la troisième réunion de la Commission d'études 2, le 17 septembre 2012.

[8] Présenté à la troisième réunion de la Commission d'études 2, le 17 septembre 2012.

- Le cybergouvernement est l'utilisation des technologies de l'information par les services publics pour fournir des services et des informations et des activités destinées à encourager les citoyens à participer de façon démocratique au processus de décision en rendant le gouvernement plus transparent et plus responsable.
- Les produits et services devraient être proposés sur le marché mondial moyennant les stratégies de commercialisation orientées TIC qui conviennent.
- Il est possible de créer une ligne de réseau d'entreprises spécialisée pour inciter les entreprises à utiliser les TIC.
- Un système de bourse en ligne permettrait à un nombre croissant de courtiers de différentes communautés d'être présents sur le marché des capitaux
- Le système juridique et le système de santé peuvent également jouer un rôle important dans tous les domaines de la société.
- L'instauration dans tous les hôpitaux publics d'un système efficace de gestion de la relation patient-médecin permettra d'améliorer les services de santé dans les zones isolées.
- L'environnement du "village planétaire" dans lequel nous vivons aujourd'hui change, prend forme et évolue au rythme de l'Internet.
- Afin de rester compétitif sur le marché mondial, il est devenu impératif pour le Bangladesh de suivre ce rythme en mettant en oeuvre le cybergouvernement.
- Au Bangladesh, le cybergouvernement n'en est qu'à ses débuts, mais le pays a fait ses premiers pas sur la voie d'une révolution Internet.
- Il y a de fortes chances pour que le cybergouvernement se développe au Bangladesh.

La numérisation du Bangladesh est en cours. Une infrastructure de réseau pérenne et fiable à l'échelle du pays renforcera les autoroutes de l'information et comblera le fossé numérique qui sépare les zones rurales et les zones urbaines. La décentralisation et les services publics numériques peuvent être une réalité pour tous les citoyens.

3.7 Mise en oeuvre de la cybergouvernance en République kirghize – Expérience et futures étapes

Les pouvoirs publics du Kirghizistan adoptent une attitude très positive en soulignant la très grande importance des technologies de l'information et de la communication (TIC) en tant que moyen d'accélérer le développement du pays. La stratégie de développement à moyen terme (2012-2014) du pays et le programme spécial d'administration publique "Stability and Life of Dignity" ("pour une vie stable et digne") indiquent clairement l'urgence de la demande relative à l'introduction du cybergouvernement dans le pays et au passage à un mode de gouvernance électronique qui permettra de répondre aux besoins des simples citoyens. Actuellement, les organismes chargés de l'administration publique de la République kirghize, et en particulier les organismes publics centraux, présentent un niveau d'informatisation satisfaisant. La plupart des ministères ayant à traiter une très grande quantité de données sont munis de serveurs dédiés servant, entre autres, à héberger des bases de données et des systèmes de courrier électronique et à donner l'accès à l'Internet, ou possèdent même des services chargés du traitement et de la gestion des données. De nombreux ministères et administrations publiques élaborent leurs propres réseaux locaux et systèmes informatiques reliés à l'Internet.

Le cadre juridique du cybergouvernement en République kirghize est largement suffisant et se compose de 16 lois sur les TIC. Toutefois, il convient d'élaborer et d'adopter des lois supplémentaires, afin de pouvoir poursuivre la mise en oeuvre des services électroniques et de l'échange d'informations dans le pays (par exemple, établir une loi sur le commerce électronique et unifier les normes et exigences techniques).

En 2002, la République kirghize a adopté la Stratégie nationale et Plan d'action "Les TIC au service du développement de la République kirghize" portant sur la période 2002-2010. L'évaluation de la mise en oeuvre de cette stratégie par le PNUD en 2007 a révélé que seulement 30% des objectifs avaient été atteints.

Le Kirghizistan a déjà reconnu l'importance de fournir un accès aux technologies et aux services modernes à la totalité des citoyens et des entreprises. Le cybergouvernement et les cyberservices donneront à l'administration publique la possibilité d'utiliser les technologies de l'information pour fournir des services de meilleure qualité aux citoyens et aux entreprises, ainsi qu'aux autres acteurs de la gouvernance[9].

- En 2012, le **Ministère des finances** de la République kirghize a lancé quelques cyberinitiatives sur la transparence du budget (www.okmot.kg), telles que: l'initiative "Transparent budget" (http://budget.okmot.kg) – système automatique servant à fournir des données sur les recettes et les dépenses du budget central et des budgets locaux. C'est la première fois dans l'histoire du pays que les simples citoyens et les entités juridiques disposent d'un libre accès au détail des informations relatives à l'exécution du budget de l'Etat. Les données sont présentées de façon à fournir le détail des informations du niveau des destinataires individuels à celui des organismes publics et des régions. Elles sont mises à jour en ligne par l'intermédiaire d'une interconnexion électronique avec la base de données du Trésor public; l'initiative "State e-procurement" (http://zakupki.okmot.kg) – système automatique pour la passation des marchés publics, qui inclut la réponse aux appels d'offres, la participation aux enchères et autres informations et actions en ligne; l'initiative "On-line economic mapping" (http://map.okmot.kg) – carte électronique de la République kirghize qui permet de visualiser la totalité des données socio-économiques de chaque zone géographique du pays.
- Le **Comité national de la statistique** de la République kirghize travaille activement à la mise en oeuvre de la collecte et de l'analyse des données statistiques à l'aide de méthodes électroniques. Cet organisme a élaboré et adopté sa stratégie générale sur les TIC, qui court jusqu'à 2020.
- L'**Administration fiscale, les douanes et les organismes public chargés du contrôle des frontières**, utilisent eux aussi les outils électroniques de manière active dans leurs travaux (déclaration d'impôt électronique, échange interorganismes de données électroniques, etc.).
- Le **Fonds social, le Fonds de l'assurance-maladie obligatoire, le Ministère de la santé et le Ministère du développement social** améliorent activement leurs systèmes d'information et bases de données sectoriels dans l'optique de la fourniture de services sociaux électroniques et de l'échange interorganismes de données.
- Le **Ministère de la justice et le Ministère de l'intérieur** ont commencé à introduire un flux de documents électroniques au sein des ministères et à utiliser des outils logiciels afin de mettre en place des systèmes de gestion des ressources humaines appropriés.
- Le **Ministère des affaires étrangères** a commencé à introduire un visa électronique ainsi qu'un flux de documents électroniques.

L'expérience pratique liée au lancement de différents projets sectoriels de cyberservices a montré que les pouvoirs publics devaient prendre en main la promotion des TIC au service du développement du pays à l'échelle nationale. Le manque de coordination des efforts dans ce domaine peut entraîner des doubles emplois, ainsi qu'une utilisation inefficace des ressources fournies par les donateurs et les pouvoirs publics eux-mêmes. Une mauvaise coordination des travaux entre organismes rend l'interconnexion électronique encore plus complexe. La création d'un organe chargé d'assurer une coordination efficace de l'utilisation des TIC, ainsi que l'établissement au niveau national de normes sur l'interopérabilité

[9] Présenté à la 3ème réunion de la Commission d'études 2, le 17 septembre 2012.

électronique et d'une infrastructure intégrée unifiée pour les cyberservices, sont des conditions essentielles du succès de la mise en oeuvre du cybergouvernement en République kirghize.

3.8 Mesures prises pour améliorer l'accès aux services administratifs par la coopération interservices grâce à des terminaux mobiles au Japon

La nouvelle stratégie exposée dans les feuilles de route en matière de technologies de l'information et de la communication (TIC) des *Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society* (Centre stratégique pour la promotion d'une société de réseaux d'information et de télécommunication évolués) fixe les objectifs suivants en ce qui concerne les programmes visant à diversifier les méthodes d'accès aux services administratifs, la rénovation du portail de l'administration publique et les mesures visant à encourager les citoyens à utiliser les services publics en ligne: en 2011, vérifier et présenter la méthode d'accès mobile aux services administratifs avec authentification à partir des téléphones mobiles et démontrer la validité de cette méthode; de 2012 à 2013, sur la base de la démonstration précédente, introduire, développer et promouvoir les services de manière partielle dans des zones de test, et les déployer progressivement à l'échelle nationale; d'ici à 2020, établir les cyberservices d'un haut niveau de praticité, à savoir les services "à guichet unique".

Conformément à ce programme, le Ministère des affaires intérieures et de la communication (MIC) a conduit en 2011 le projet "Promouvoir des services administratifs par la coopération interservices (Vérification des méthodes visant à améliorer la convivialité des téléphones mobiles utilisés comme moyens d'accès), sur la base d'une enquête et des résultats de recherche issus de "la recherche et de l'étude de la diversification des moyens d'accès aux services de cybergouvernement, etc. (recherche et étude des technologies d'accès aux services de cybergouvernement à l'aide des téléphones mobiles, etc.)" datant de 2009.

Des terminaux mobiles dotés de fonctions de communication en champ proche vont être commercialisés en 2012. Ils assurent le stockage des données personnelles des utilisateurs des services, aussi bien en ligne que hors ligne, au moyen de dispositifs inviolables fonctionnant à l'aide d'informations d'identification, tels que la combinaison identité d'utilisateur/mot de passe, les points et les coupons, et permettent la lecture des informations. A l'aide de ces fonctions, l'authentification des utilisateurs pour accéder aux services de cybergouvernement par l'intermédiaire des terminaux mobiles devient plus pratique, et la totalité des citoyens, quelle que soit leur génération, disposent d'un accès facile et sûr aux services administratifs par l'intermédiaire des terminaux mobiles.

Les recherches conduites par le MIC en 2009 visaient à étudier la sécurité des espaces suivants pour le stockage des informations d'authentification émises par les fournisseurs de services à l'intention des utilisateurs et leur servant de moyen d'accès aux services de cybergouvernement: 1) système public de carte à circuits intégrés, qui s'utilise en plaçant la carte nationale d'identité délivrée par les pouvoirs publics à proximité du téléphone mobile; 2) système public de carte pour téléphones mobiles, qui s'utilise en insérant les cartes adéquates, délivrées par les pouvoirs publics, dans les terminaux mobiles, etc. 3) système public d'informations d'identification qui s'utilise en entrant à l'aide du clavier les informations fournies par les pouvoirs publics dans les terminaux mobiles, etc. Les dispositifs inviolables sont censés être: 1) les cartes à circuits intégrés complètes pour le système de carte à circuits intégrés; 2) les dispositifs de mémoire flash contenant des puces de circuit intégré pour le système public de cartes pour téléphones mobiles; 3) les cartes UICC (carte à circuits intégrés universelle) pour le système public d'informations d'identification.

A défaut de l'étude précédente, il était nécessaire, pour stocker et utiliser les informations d'identification ou les informations des utilisateurs dans des dispositifs inviolables, de mettre au point et d'utiliser une application pour téléphones mobiles (ci-après application mobile) pour chaque opérateur de services. En outre, les utilisateurs devaient télécharger et installer séparément des applications mobiles émanant des fournisseurs de services. En d'autres termes, la fourniture d'un service inviolable présentait des inconvénients pour les fournisseurs de services comme pour les utilisateurs. Afin de créer un environnement pratique pour les utilisateurs et dans lequel il soit facile d'assurer la fourniture et

l'exploitation des services, nous avons étudié des spécifications techniques en vue d'élaborer un système d'accès mobile.

Afin de résoudre les difficultés précédentes, nous avons étudié un système qui puisse être utilisé à la fois par les utilisateurs et les fournisseurs de services. En d'autres termes, nous avons étudié les spécifications techniques d'un système d'accès mobile composé de serveurs assurant le stockage et la lecture sécurisés, communs à l'ensemble des fournisseurs de services, ainsi que d'une application mobile, commune à l'ensemble des services, assurant le stockage et l'utilisation des informations d'identification dans des dispositifs inviolables. En outre, il est procédé à une vérification expérimentale des spécifications techniques, à l'identification des problèmes au vu du lancement et de l'exploitation, et à l'étude de ces problèmes en vue d'y apporter des solutions.

Les habitants des pays en développement sont de plus en nombreux à posséder un terminal mobile, et dans ces pays, le nombre des utilisateurs de smartphones est aussi en augmentation. Par conséquent, il est certainement nécessaire de prévoir également un accès mobile aux services publics dans les pays en développement[10].

3.9 Cybergouvernement au Liban

La Feuille de route sur le cybergouvernement reflète le ferme engagement de nos pouvoirs publics à mettre en place un portail de l'administration publique, afin d'améliorer et de faciliter l'accès des citoyens aux services et aux informations fournis par les pouvoirs publics.

La stratégie de cybergouvernement vise à atteindre les objectifs stratégiques suivants: établir une administration publique qui soit centrée sur les citoyens (et non sur la fonction publique), axée sur les résultats et basée sur le marché (encourageant activement l'innovation), qui suive des principes de bonne gouvernance, et qui garantisse le développement économique et l'inclusion sociale[11]. Cette stratégie s'articule autour des initiatives suivantes:

- e-Reform: fournit l'occasion idéale de réorganiser les processus administratifs de façon à tirer parti des technologies et à utiliser les TIC comme fer de lance du processus de réforme.
- e-Citizen: regroupe tous services fournis actuellement aux citoyens par les administrations publiques et qui pourraient l'être électroniquement.
- e-Business: concerne les services publics qui présentent une importance pour les entreprises libanaises et les investisseurs étrangers. Le fait d'améliorer la fourniture de ces services favorisera la croissance du secteur privé au Liban et se traduira par le développement économique du pays.
- e-Community: il est largement reconnu que les TIC jouent un rôle central dans la participation à l'économie du savoir qui se dessine, et qu'ils représentent une occasion exceptionnelle d'accélérer la croissance économique, de favoriser le développement durable et l'autonomisation, et de réduire la pauvreté.
- Les différentes initiatives de cybergouvernement dans différents domaines, tels que les affaires juridiques, les infrastructures TIC, les applications verticales, ainsi que diverses normes et politiques nationales.

La Feuille de route en matière de cybergouvernement est définie comme un ensemble d'activités de grande échelle et d'étapes charnières essentielles selon différents points de vue: juridique, administratif, infrastructures, réorganisation des processus opérationnels, interopérabilité et portail de l'administration

[10] Présenté à la 3ème réunion de la Commission d'études 2, le 17 septembre 2012.

[11] Présenté à la 3ème réunion de la Commission d'études 2, le 17 septembre 2012.

publique. L'exécution de cette feuille de route reposera sur un plan de renforcement des capacités qui rendra les employés des administrations publiques à même d'utiliser la totalité des projets de cybergouvernement de manière efficiente et efficace.

La prochaine étape consiste à élaborer les versions préliminaires de différentes lois, décisions et projets techniques, que les pouvoirs publics libanais pourraient adopter:

- Projet de loi – Transactions électroniques
- Projet de loi – Loi sur le barème des traitements dans le secteur des technologies de l'information (TI)
- Adoption d'une loi sur les transactions électroniques
- Simplification des procédures.

3.10 Projet MWANA (Zambie)

Le rôle et l'influence des TIC en Zambie ont rapidement augmenté en raison de facteurs sociaux et de l'évolution dynamique des technologies de l'information et de la communication (TIC). Selon l'enquête ZICTA, relative à l'utilisation des TIC, sur les 12 millions d'habitants que compte la Zambie, 7,8 millions ont accès à la téléphonie mobile et 4 millions à l'Internet. La hausse de la demande de services évolués et l'augmentation de l'utilisation des TIC au sein de la population ont poussé les pouvoirs publics et le secteur privé à se montrer plus innovants et à investir massivement dans les réseaux d'accès aux télécommunications[12].

Objectifs:

- Renforcer le diagnostic précoce du VIH chez le nourrisson, dans le but à la fois d'augmenter le nombre de mères recevant des résultats et d'entrer en liaison avec elles de manière plus rapide et plus efficace à l'aide de l'application SMS (santé sur mobile).
- Améliorer le taux de suivi post-natal et augmenter le nombre d'enregistrements de naissance, tant pour les naissances en milieu hospitalier que pour celles qui ont lieu dans les communautés, tout en augmentant la fréquentation des établissements de santé par les mères, et ce au moyen d'un suivi assuré par des travailleurs de santé communautaires à l'aide de l'application "RemindMi".
- Améliorer la fourniture de services aux citoyens par les pouvoirs publics.
- Réduire les formalités administratives et les délais de traitement lors de la fourniture de services publics.

Technologies et solutions déployées:

- La technologie SMS, qui représente une innovation majeure en Zambie, où elle a permis de réduire les délais de réception des résultats du test DBS servant à établir un diagnostic précoce du VIH chez le nourrisson, d'améliorer la communication entre les fournisseurs de soins et les volontaires au sein des communautés et, plus important encore, d'encourager les patients à retourner dans les établissements de soin pour obtenir leurs résultats de test avec davantage de confiance.
- La technologie RapidSMS, qui concerne le diagnostic précoce du VIH chez le nourrisson, et permet l'utilisation de messages SMS pour envoyer les résultats des tests de dépistage du VIH des laboratoires où ils sont établis au personnel des installations où a lieu la collecte des échantillons. Les résultats arrivent sur des téléphones dans les petites installations et sur des imprimantes pour

[12] Présenté à la 3ème réunion de la Commission d'études 2, le 17 septembre 2012.

SMS dans les plus grandes. Le système assure également le suivi des échantillons et transmet en temps réel les informations au personnel des provinces et des districts.

- L'application RemindMi sert à assurer le suivi des patients pour la fourniture de soins post-natals. Des messages SMS sont envoyés à des agents auprès des communautés, dont le rôle consiste à se mettre en rapport avec les personnes s'occupant de nourrissons et à leur demander de renvoyer ces derniers en milieu hospitalier pour leur faire subir un bilan post-natal à six jours, six semaines et six mois, où à l'occasion de circonstances particulières, comme l'arrivée de résultats dans l'installation dont ils relèvent.

Un plan visant à étendre le projet à l'échelle nationale a été élaboré. Il prévoit d'abord une phase de préparation, puis le passage à une phase itérative, qui consistera à rendre des installations opérationnelles et à les ajouter au système, ainsi qu'à évaluer les points forts et les points faibles de ces nouvelles installations. L'objectif est d'établir d'ici à 2015 un réseau d'installations de santé assurant la fourniture de services de diagnostic précoce du VIH chez le nourrisson sur l'ensemble du territoire. La phase de préparation visera à renforcer les infrastructures techniques et physiques, les moyens de suivi et les capacités humaines, afin que le système puisse subir sans dommage les tensions liées au changement d'échelle. Tout au long du processus d'extension, le projet fera l'objet d'un suivi étroit, afin de veiller à ce que son déploiement ait un effet positif sur les problèmes de santé visés.

3.11 Services de cybergouvernement au Monténégro

Le Monténégro, conscient de l'importance du développement et de l'application des TIC, a pris des mesures significatives en ce sens dans le passé, comme en atteste le classement établi dans le cadre du Forum économique mondial en fonction de l'indice de préparation au réseau (NRI), où il occupe la 44ème place sur un total de 138 pays, loin devant d'autres pays européens de la région. Avec un taux de pénétration de la téléphonie mobile de près de 200% et un taux de pénétration de l'Internet en constante augmentation, il est clair que le secteur des TIC au Monténégro connnaît une phase de croissance intense[13].

- La durabilité des TIC est l'objet de plusieurs programmes, qui portent respectivement sur les aspects fondamentaux des TIC (cadre technologique, cadre pour le spectre des fréquences radioélectriques, cadre pour la protection des consommateurs), l'infrastructure TIC, le cadre juridique et réglementaire, et la sécurité de l'information, avec comme objectifs l'amélioration de l'infrastructure large bande et l'élaboration d'un cadre juridique et réglementaire favorisant la concurrence et la durabilité dans le secteur des TIC.
- Les TIC au service de la société, avec les programmes de cyberapprentissage, de cybersanté et d'inclusion électronique, qui visent à encourager tous les acteurs de la société moderne à utiliser les TIC.
- Les TIC dans l'administration publique, avec le programme de cybergouvernement, dont le but est d'encourager les administrations publiques à utiliser les TIC de manière innovante afin d'améliorer la qualité des services fournis par les pouvoirs publics.
- Les TIC au service du développement économique, avec un programme sur la recherche et développement et l'innovation, qui vise à encourager l'utilisation des TIC dans le développement de la science et de la recherche, afin d'établir des systèmes TIC productifs et durables via la création d'une base de données de talents et la promotion de la créativité et de l'entrepreneuriat.

[13] Présenté à la 3ème réunion de la Commission d'études 2, le 17 septembre 2012.

- Afin de mettre en oeuvre le cybergouvernement au Monténégro, le Ministère de la société de l'information et des télécommunications met en oeuvre le projet de portail de l'administration publique "www.euprava.me", par l'intermédiaire duquel toutes les administrations publiques et les entités autonomes locales fourniront des services électroniques aux particuliers et aux entreprises, ainsi qu'à d'autres entités publiques.
- Le système eDMS (Electronic Document Management System) est un projet qui vise principalement à informatiser et à électroniser les processus opérationnels des pouvoirs publics du Monténégro, afin de réaliser des gains de temps et d'efficacité, de réduire les coûts et d'améliorer la gestion des ressources documentaires.

Les mesures et efforts à venir porteront sur le cadre d'interopérabilité, qui par nature ne constitue pas un document technique, et s'adresse à ceux et celles qui participent à la définition, à la conception et à la fourniture de services publics.

Bien que dans la quasi-totalité des cas, la fourniture de services publics passe par l'échange de données entre des systèmes d'information, l'interopérabilité est un concept plus large, qui inclut la possibilité d'établir des collaborations autour d'objectifs d'intérêt général fixés d'un commun accord.

4 Outils pour de bonnes pratiques

4.1 Kit pratique pour les services fondés sur les TIC utilisant les communications mobiles[14]

Le kit pratique pour la création de services fondés sur les TIC décrit comment utiliser les communications mobiles pour les services de cybergouvernement et comment il est possible d'intégrer tous les services fondés sur les TIC nécessitant une authentification et une connexion sécurisée, comme le cybergouvernement sur mobile (m-gouvernement), le paiement sur mobile (m-paiement), les services bancaires sur mobile (mobi-banque) et la santé sur mobile (m-santé). Cette partie du rapport décrit les principes généraux de la création de ces services, ainsi que les Recommandations UIT-T liées aux aspects sécurité.

- Les communications mobiles, outre leur objet principal – communications vocales et transfert de messages entre utilisateurs – s'avèrent très utiles pour d'autres applications comme le commerce, la santé et le gouvernement sur mobile, entre autres. Il faut toutefois bien comprendre que le "m-gouvernement" n'est que l'un des différents moyens de communication électronique avec l'administration publique et qu'il en va de même pour la santé, l'enseignement, le commerce et le paiement sur mobile.

Malgré la petite taille de leurs écrans et claviers, les appareils mobiles offrent de grandes possibilités à l'usager de services de cybergouvernement. En raison de la rapidité de l'évolution technologique et des avantages considérables des communications mobiles, les "cyberservices", fondés sur les terminaux mobiles et précédés du préfixe "m" (*m-gouvernement, m-santé, m-paiement, m-apprentissage, etc.*), sont très prometteurs. En effet:

- Tout le monde ne possède pas un ordinateur personnel, mais en règle générale, chacun de nous, ou presque, a un téléphone mobile (selon le rapport de l'UIT "Tendances des réformes dans les télécommunications – 2012", fin 2011, on comptait dans le monde 6 milliards d'abonnés au mobile, et près de trois milliards d'internautes).

[14] Cette partie est le résumé de la contribution d'Intervale, dont la totalité figure dans l'Annexe.

- Les téléphones mobiles sont toujours à proximité de leurs utilisateurs et sont connectés en permanence.
- Il arrive que les communications mobiles soient les seuls moyens de communication disponibles.
- Les communications mobiles sont au moins aussi sûres que l'Internet.

4.1.1 Principes applicables à la sécurisation des services mobiles

En règle générale, les systèmes mobiles utilisés pour la fourniture de services à distance sécurisés (cybergouvernement sur mobile, médecine sur mobile ou commerce sur mobile) doivent avoir une infrastructure qui assure la transmission sécurisée des blocs de données entres l'utilisateur de terminal mobile et le prestataire de services. Pour garantir la sécurité, cette infrastructure doit comporter un élément authentification et cryptage. Les blocs de données transmis peuvent contenir des informations confidentielles appelant un traitement sécurisé. L'échange de données ne doit s'effectuer qu'entre utilisateurs agréés, ne doit pas être accessible à des tiers et doit être enregistré correctement pour éviter les risques de non-répudiation. L'authentification de l'utilisateur résulte de l'authentification de multiples facteurs.

4.1.2 Identification et authentification

A des fins d'identification, il est demandé au Client de valider son identité et d'établir un lien unique entre son appareil mobile et son compte dans la base de données du prestataire de service. Après l'identification initiale, le client devrait se voir délivrer un "code secret" qui l'authentifiera à l'avenir dans ses interactions avec ledit prestataire. Ce "code secret", aussi appelé "signature mobile", est l'un des éléments de l'authentification. En pratique, la signature mobile est une clé cryptographique unique qui peut aussi servir à crypter des données. Une telle clé permet donc à la fois de crypter des données et d'authentifier l'utilisateur. Le second élément de l'authentification peut être fourni par le code PIN ou mot de passe de l'utilisateur, qui lui donne accès aux applications installées sur l'appareil. Ce code PIN empêche que des applications ne soient utilisées sans autorisation.

Les systèmes existants de paiement sur mobile mettent déjà en oeuvre leurs propres procédures de sécurité, aux termes desquelles les prescriptions de sécurité sont déterminées par des accords conclus entre les fournisseurs de services et leurs clients. Bien évidemment, les applications de cybergouvernement doivent être sécurisées par un système contrôlé par l'Etat et conforme à la législation nationale relative à la signature électronique. Ce système doit assurer la transmission sécurisée de données confidentielles entre les organismes publics et les utilisateurs agréés, avec possibilité de signature électronique. Il peut aussi être utilisé pour les services de cybersanté ou d'autres nouveaux services pour lesquels les données doivent être protégées. Même si les systèmes privés de paiement sur mobile disposeront probablement de leurs propres moyens de protection, les solutions complexes, qui proposent une authentification centralisée, ne sont pas à exclure, et certains prestataires de services (le plus souvent, de services financiers) utilisent aussi leurs propres procédures de cryptage et de vérification. Il est donc logique de fournir, avec les applications mobiles, plusieurs blocs indépendants ayant différents jeux de clés. La Figure 2 présente un modèle unifié d'authentification pour les appareils prenant en charge les services mobiles et l'Internet.

Les centres d'identification et d'authentification étant nombreux, tous doivent appliquer des règles uniformes pour délivrer à leurs clients des identités mobiles ou mID, enregistrées dans le répertoire central du système pour assurer le bon acheminement des messages.

L'option Service Enabler assure un appui technologique et joue un rôle très important dans cette infrastructure. Elle assure l'intégration de différents moyens d'accès, l'interopérabilité avec les prestataires de services et le centre d'authentification, et fournit aux utilisateurs des applications pour ces moyens d'accès (ordinateurs personnels et terminaux mobiles).

Tous les centres d'identification et d'authentification doivent se conformer aux mêmes règles régissant l'attribution des identificateurs mID, enregistrés dans un répertoire central du système pour assurer le bon acheminement des messages.

4.1.3 Gestion des clés

La cryptographie peut être utilisée avec des clés aussi bien symétriques qu'asymétriques pour le cryptage des données transmises et la création de signatures sur mobile. L'avantage du chiffrement symétrique (Normes 3DES, AES) est qu'il emploie des algorithmes faciles à mettre en oeuvre dans les appareils informatiques bon marché. La production de clés symétriques est une opération simple qui ne nécessite pas de moyens spéciaux. Toutefois, par définition, l'utilisation d'une même clé, partagée entre l'utilisateur et le fournisseur de services (centre d'authentification du fournisseur), peut amener l'utilisateur à contester la transaction menée à bien. Il est cependant à signaler que les systèmes de paiement sur mobile, désormais capables de créer des systèmes fiables d'enregistrement des transactions en cas de litige, utilisent sans problème la cryptographie par clés symétriques.

La cryptographie par clés asymétriques utilise l'infrastructure à clé publique (PKI) pour relier deux clefs différentes appartenant à une même personne: une clef "publique", avec une identité publique, et une clef "privée" qui est placée en sécurité et protégée contre toute tentative d'intrusion (par exemple, dans une carte SIM ou une carte à puce spécialement protégée). Les interactions mathématiques entre ces deux clefs sont gérées de telle façon qu'une opération exécutée avec une clef peut être "reliée" à une autre clef, sans divulgation des données relatives à la clef privée. Ce dernier point est particulièrement intéressant pour la création d'une signature électronique, puisque la signature effectuée par la clef privée n'identifie le détenteur de celle-ci qu'en relation avec la clef publique associée – dont l'identité est connue. Dans la technologie PKI, le plus important est, d'une part, d'assurer la confidentialité des clés privées et, d'autre part, de vérifier la relation entre les clés publiques et les clés privées. Pour ce faire, il faut gérer avec prudence la procédure d'enregistrement lors de la délivrance des clefs, ainsi que la procédure de certification au terme de laquelle est confirmée l'identité de la clef publique. Ces éléments sont gérés par des entités appelées autorité d'"enregistrement" et autorité de "certification". Dans le cas de la signature sur mobile, leur fonction première est de reconnaître le caractère unique de la relation établie entre l'utilisation de la clef privée et l'identité enregistrée de la personne, du fait qu'il/elle est le détenteur de la clef publique associée.

Les méthodes de chiffrement asymétrique nécessitent l'utilisation de moyens informatiques plus onéreux, mais peuvent s'appliquer à différents modèles d'interaction. L'utilisation de la "double clé" offre de plus grandes possibilités d'adaptation et facilite le règlement des différends. Il en résulte un modèle de confiance plus efficace, assorti d'une simplification de la gestion administrative et des services (par exemple, nombre d'applications et de modèles d'interaction différents peuvent être pris en charge par une seule paire de clés asymétriques). En conséquence, les documents décrivant des cadres d'interopérabilité pour les signatures électroniques à l'échelle mondiale sont presque exclusivement axés sur les méthodes de cryptage asymétriques.

4.1.4 Sécurité

La sécurité est l'élément le plus important, pour les systèmes de paiement comme pour les systèmes de cybergouvernement ou de cybersanté, applications mobiles comprises. Les normes en la matière sont énoncées dans les Recommandations du Secteur de la normalisation des télécommunications de l'UIT, qui a publié un manuel intitulé "Sécurité dans les télécommunications et les technologies de l'information". Ce manuel présente un aperçu des normes UIT-T existantes et de leur application pratique à la sécurité des télécommunications[15]. Ces normes doivent être respectées. Même si elles ont le titre de recommandations, il est essentiel de s'y conformer pour assurer la compatibilité et l'homogénéité des systèmes de télécommunication d'un pays à l'autre.

Puisque ces systèmes font intervenir de nombreux acteurs, les questions de sécurité relèvent de plusieurs catégories:

a) Sécurité des points d'extrémité

b) Sécurité des applications sur mobile

c) Sécurité des réseaux mobiles

d) Identification du demandeur, incluant l'identification en bonne et due forme de la personne à l'origine de la transaction financière.

Avant l'époque des téléphones intelligents ou smartphones, il était relativement facile pour les opérateurs de gérer les applications mobiles sur téléphone mobile. Fondamentalement, ils avaient le contrôle des applications qui pouvaient être téléchargées sur l'appareil et de leurs caractéristiques en matière de sécurité. La situation s'est compliquée avec l'apparition des smartphones et la capacité de télécharger gratuitement des applications tierces. Aujourd'hui, il est pour ainsi dire impossible d'être totalement certain que chaque application exécutée sur un appareil mobile provient d'une source fiable. En conséquence, les utilisateurs de mobiles sont exposés à de nouveaux risques comme l'usurpation d'identité, le hameçonnage ou encore la perte de données personnelles.

Les mesures de sécurité correctement conçues et appliquées viennent à l'appui de la politique de sécurité qui est définie pour un réseau particulier et facilitent l'application des règles établies par les gestionnaires de la sécurité.

La mesure de sécurité concernant le contrôle d'accès protège contre l'emploi non autorisé des ressources du réseau. Le contrôle d'accès assure que seuls les personnels ou les dispositifs autorisés peuvent accéder aux éléments de réseau, aux flux d'informations, aux services et aux applications. En outre, le contrôle d'accès en fonction des prérogatives (RBAC) institue différents niveaux d'accès, afin de garantir que les personnes et les dispositifs ne peuvent avoir accès aux éléments de réseau, aux informations emmagasinées et aux flux d'informations et ne peuvent les manipuler que s'ils y ont été autorisés.

La mesure de sécurité concernant l'authentification sert à confirmer les identités des entités qui communiquent. L'authentification assure la validité des identités déclarées des entités en communication (par exemple, une personne, un dispositif, un service ou une application) et donne l'assurance qu'une entité ne tente pas d'usurper l'identité d'une autre entité ou de reprendre sans autorisation une précédente communication.

La mesure de sécurité concernant la non-répudiation donne les moyens d'empêcher une personne ou une entité de nier avoir exécuté une action particulière liée aux données, en fournissant une attestation des diverses actions dans le réseau (telle qu'une attestation d'obligation, d'intention ou d'engagement; une attestation de l'origine des données, une attestation de propriété ou une attestation de l'emploi des ressources). Elle assure la mise à disposition de la preuve qui peut être présentée à une entité tierce et être utilisée pour prouver qu'un certain type d'événement ou d'action a eu lieu.

La mesure de sécurité concernant la confidentialité des données protège les données de leur divulgation. La confidentialité des données assure que le contenu des données ne pourra être compris par des entités non autorisées. Le chiffrement, les listes de contrôle d'accès, et les permissions d'accès aux fichiers sont des méthodes souvent employées pour assurer la confidentialité des données.

La mesure de sécurité concernant la communication assure que les informations ne seront acheminées qu'entre les extrémités autorisées (les informations ne sont ni déviées ni interceptées au cours de leur acheminement entre ces points).

La mesure de sécurité concernant l'intégrité des données assure l'exactitude ou la précision des données. Les données sont protégées contre toute modification, suppression, création et reproduction. La mesure signale ces activités non autorisées.

La mesure de sécurité concernant la disponibilité assure qu'il n'y a pas déni de l'accès autorisé aux éléments de réseau, aux informations emmagasinées, aux flux d'informations, aux services et aux applications en raison d'événements ayant une incidence sur le réseau. Des solutions de récupération en cas de catastrophe sont aussi comprises dans cette catégorie.

La mesure de sécurité concernant le respect de la vie privée assure la protection des informations qui pourraient être déduites de l'examen des activités dans le réseau. Des exemples de telles informations sont notamment les sites Web que l'utilisateur a visités, le lieu géographique de l'utilisateur, ainsi que les adresses Internet et les noms des services de noms de domaine dans un réseau de fournisseur de services.

4.1.5 Technologie mobile

A ce jour, le terme "communications mobiles" est le plus souvent associé à la norme GSM des deuxième et troisième générations. Ces systèmes utilisent différents sous-systèmes pour la voix et le transfert de données (technologies de commutation par répartition dans le temps et de commutation par paquets), ce qui représente une étape intermédiaire dans l'évolution des communications mobiles. Les réseaux de prochaine génération (NGN), qui se substituent aux réseaux existants, donnent aux abonnés un accès au large bande et n'utilisent que la technologie de commutation par paquets.

Les réseaux NGN assurent des services de transmission de la voix, des images, de texte et multimédias en tant qu'applications de la procédure universelle de transmission de données par lots. En conséquence, les technologies de transmission de données par SMS et MMS, largement utilisées aujourd'hui, pourraient bien céder la place à de nouvelles technologies, sans même que les usagers remarquent ces changements. Toutefois, les solutions technologiques mises au point pour les services sur mobile devraient être capables de s'adapter à l'évolution des communications mobiles.

Même si on utilise aujourd'hui couramment les terminaux mobiles, ceux-ci n'étaient pas conçus au départ pour des systèmes nécessitant de solides moyens d'authentification. Les terminaux de différents fabricants, voire les différents modèles de terminal d'un même fabricant, peuvent employer des algorithmes différents, d'où une complexité accrue, et dans certains cas, l'incapacité de créer des applications qui exécutent toutes les fonctions attendues du système. Par exemple, une application devrait pouvoir être activée automatiquement dès réception d'un message en provenance d'un système de paiement sur mobile (à la demande d'un commerçant). Malheureusement, une telle application ne peut être mise en oeuvre sur chaque terminal mobile.

Pour uniformiser le fonctionnement de ces systèmes, il faut normaliser d'autres protocoles, tâche dont peut se charger l'UIT, de même que les équipementiers. Un autre point important concerne l'emplacement de l'application crypto et la gestion de l'accès à cette application. Comme indiqué au chapitre "Sécurité", pour parvenir au niveau de sécurité maximal, ces applications doivent être logées dans un module spécial (élément de sécurité matérielle), qui protège les informations mémorisées contre toute tentative d'accès non autorisé. Les cartes SIM ou UICC peuvent servir de module, pour autant que la question de la délégation des droits administratifs d'accès à la carte SIM, appartenant à l'opérateur de service mobile, soit résolue. Il est facile de trouver une solution lorsque ces deux fonctions sont exécutées par la même entité, mais dans les autres cas la situation se complique. La création de terminaux mobiles équipés d'un élément de sécurité matérielle supplémentaire peut être considérée comme une solution aux problèmes de la gestion conjointe des cartes SIM, grâce à un module de sécurité intégré ou à une carte mémoire infalsifiable spécialement installée.

Il existe différentes technologies de transfert des données sur les réseaux mobiles: CSD, SMS; USSD, GPRS, EDGE, LTE, par exemple. Chacune d'elles a ses avantages et ses inconvénients. Ainsi, le SMS est très fiable et facile à mettre en oeuvre, mais la longueur des messages est limitée. En revanche, elle n'est pas limitée dans le cas du GPRS, mais cette technologie est moins fiable et doit être adaptée pour être utilisée avec les terminaux mobiles, notamment en mode itinérance, qui est par ailleurs très onéreux. Le progrès technologique a entraîné la mise en oeuvre généralisée dans les smartphones de services de géolocalisation utilisant les systèmes GPS ou GLONASS. La géolocalisation élargit de beaucoup les

fonctions des terminaux mobiles, ce qui explique que ces services soient couramment utilisés dans les applications pour appareils mobiles qui sont, de plus en plus souvent, des smartphones.

4.1.6 Conclusions

Comme le montrent les exemples de mise en oeuvre dans plusieurs pays (Union européenne, Japon, Etats-Unis, Russie, etc.) décrits dans l'Annexe, les niveaux de développement et d'utilisation des appareils mobiles pour le gouvernement, la santé, le paiement et l'apprentissage sur mobile, entre autres, varient d'un pays à l'autre. Toutefois, dans notre univers mondialisé, le taux de pénétration des innovations technologiques augmente en flèche, ce qui se traduit par la convergence progressive des niveaux de développement et la réduction de la fracture numérique entre pays développés et pays en développement. Aujourd'hui, les pays développés disposent déjà de systèmes de paiement électronique et de m-gouvernement parfaitement fonctionnels. Dans certains pays en développement, la simple utilisation du SMS pour transférer des données d'un établissement médical à l'autre donne des résultats concrets, raccourcissant les délais de réception des résultats des tests VIH pour le diagnostic précoce du nourrisson, comme décrit dans le projet MWANA mis en oeuvre en République de Zambie[16]. On voit donc que, très rapidement, la fracture technologique se réduira. Les systèmes actuels les plus évolués fondés sur la technologie mobile offrent toute une gamme de services, qui ne cesse de s'étendre, non seulement avec les services de paiement sur mobile et les services bancaires sur mobile, mais aussi avec les services de géolocalisation. Par ailleurs, comme indiqué dans le Livre blanc sur les paiements mobiles[17], publié par le Conseil européen des paiements en 2012, le terminal mobile devrait constituer un "porte-monnaie numérique" qui remplacera par l'authentification et la signature numérique les multiples mots de passe, pièces d'identité et cartes de fidélité des commerçants.

Tout comme un porte-monnaie ordinaire, le porte-monnaie "numérique" contient des données permettant d'identifier son détenteur, des données relatives aux moyens de paiement à sa disposition, et, dans certains cas, des données personnelles (images, documents, etc.). Il peut inclure des informations sur les pièces d'identité, des signatures et certificats numériques, des informations sur la connexion, des adresses pour la transmission de données, ainsi que des renseignements sur les moyens de paiement. Il peut aussi inclure d'autres applications, comme des points bonus, des billets ou des documents de voyage. Une fois l'authentifiant approuvé par le central, on peut accéder à un compte personnel de commerçant ou naviguer sur les réseaux sociaux (Facebook, LinkedIn, etc.), ce qui est très pratique et évite d'avoir à mémoriser de nombreux mots de passe liés à de multiples comptes. A court terme, on peut supposer que des appareils mobiles seront distribués pour servir de terminaux utilisés pour le cybergouvernement et les soins de santé, comme le prouvent de récentes initiatives présentées à ITU Telecom 2012 par l'UIT et l'OMS.

On voit donc que le développement rapide des systèmes fondés sur le mobile s'explique entre autres par les mesures de sécurité appliquées aux services. Les mesures de sécurité – élément commun essentiel au cybergouvernement, aux services financiers et à la cybersanté – doivent être conformes aux recommandations de l'UIT-T.

En application de ces recommandations, la cryptographie est utilisée pour l'authentification et le codage des données transférées, en remplacement des mots de passe employés dans les anciens systèmes. Cette technique renforce considérablement la sécurité des appareils mobiles et en facilite l'emploi, ce qui augmente le succès des services utilisant ces appareils.

4.1.7 Recommandations

- Le téléphone mobile, qui est désormais totalement implanté sur tous les marchés et offre une excellente qualité de service, est un terminal de paiement idéal et un moyen de communication sûr.
- L'important est de proposer des interfaces de téléphone mobile conviviales donnant aux usagers des conditions homogènes d'utilisation, quel que soit l'appareil pris en charge, même si les smartphones les plus évolués présentent de magnifiques écrans couleur et des interfaces tactiles.

Les conditions d'utilisation restent fortement tributaires du petit format des appareils, qui limite, par exemple la quantité d'informations pouvant être affichées et la possibilité pour l'utilisateur de saisir des textes complexes.

- L'appareil mobile est un "porte-monnaie numérique", qui permet de mémoriser des données concernant son détenteur, les moyens de paiement à sa disposition et, éventuellement, des données personnelles à son sujet (par exemple, images, documents, etc.). Il peut inclure des informations sur les pièces d'identité, des signatures et certificats numériques, des informations sur la connexion, des adresses de facturation et de livraison, ainsi que des renseignements sur les moyens de paiement. Il peut aussi inclure d'autres applications, comme des cartes de fidélité, des billets ou des tickets.
- Il est conseillé aux clients de ne pas se lier à un seul opérateur de réseau mobile ou à une seule banque et de se réserver la possibilité de choisir leurs prestataires de services.
- Les parties prenantes à un dialogue par voie électronique devraient être autorisées à utiliser une authentification à deux facteurs au minimum, et le transfert des données devrait se faire en mode sécurisé à l'aide de moyens cryptographiques.
- Il est conseillé d'utiliser un niveau de sécurité 4 ou 3, conformément à la Recommandation UIT-T Y.2740.
- Les clients devraient savoir quel est le niveau de sécurité du système, lequel devrait être précisé dans l'accord. L'authentification de l'utilisateur peut être réalisée par le centre correspondant.
- Pour garantir la sécurité, l'appareil mobile doit être doté d'une application spéciale pour mobile qui assure l'authentification et le cryptage.
- La vision d'avenir la plus vraisemblable est celle d'un marché sur lequel coexisteront de multiples applications, avec plusieurs services disponibles sur un seul appareil mobile.
- L'enregistrement et la mise en service d'une application mobile doivent être exécutés dans un environnement sécurisé. L'accès à cette application serait facilité pour le client s'il pouvait se baser sur une relation de confiance entre lui-même et son prestataire de service.
- Pour parvenir au niveau de sécurité maximal, les applications mobiles doivent être intégrées dans l'élément de sécurité matérielle.
- Le choix de l'élément de sécurité est lourd de conséquences pour le modèle de service et les rôles des différentes parties prenantes. Il existe à ce jour trois types d'éléments de sécurité: carte UICC, élément de sécurité intégré et élément de sécurité amovible, par exemple carte micro SD.
- L'activateur de service assure l'appui technologique et l'intégration de différents moyens d'accès, l'interopérabilité avec les fournisseurs de services et le centre d'authentification.
- Il est recommandé d'utiliser des applications mobiles ayant plusieurs blocs indépendants avec différents jeux de clés.
- Le client peut avoir de multiples identités mobiles (mID), en lien avec son numéro MSISDN. Il faudrait mettre en place des règles uniformisées pour la délivrance de ces numéros, enregistrés dans le répertoire central du système, afin d'assurer le bon acheminement des messages aux clients.
- Tous les centres d'identification et d'authentification doivent respecter les mêmes règles d'attribution aux clients d'identificateurs mobiles (mID), enregistrés dans le répertoire central du système, afin d'assurer la livraison des messages aux clients.
- Les systèmes mobiles devraient, autant que possible, utiliser des technologies et infrastructures déjà largement déployées.

4.2 Evaluation de l'efficacité du cybergouvernement et de son incidence en Corée (République de Corée)

4.2.1 Introduction

Aujourd'hui, de nombreux projets dans le domaine des technologies de l'information, notamment la mise en place à l'échelle nationale de systèmes de cybergouvernement très lourds, sont lancés non seulement dans les pays développés, mais aussi dans les pays en développement, et ce car il est de plus en plus reconnu que ces projets favoriseront l'efficacité et la transparence des processus administratifs. Toutefois, faute d'une gestion adaptée, les résultats escomptés ne se produiront pas, avec, même dans le pire des cas, un gaspillage des fonds publics. Par conséquent, il conviendrait de procéder à une gestion de l'efficacité bien planifiée lors de la mise en oeuvre des projets.

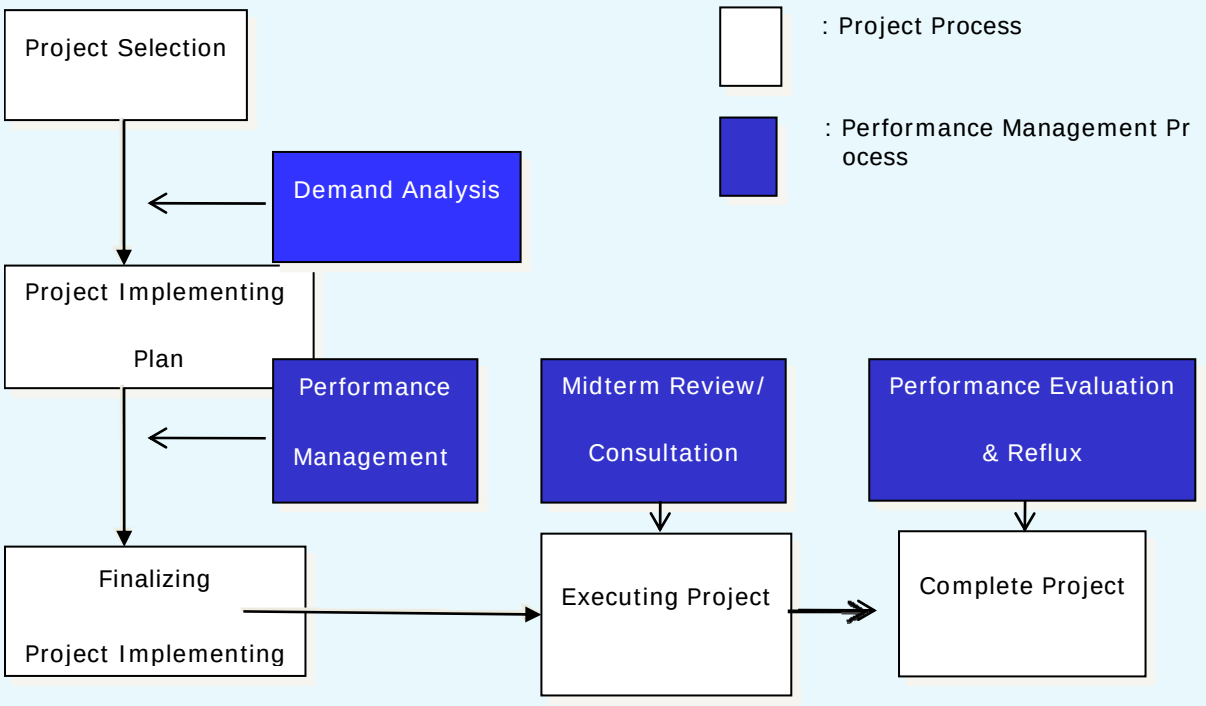
La gestion de l'efficacité s'inscrit dans une démarche beaucoup plus large qu'une simple évaluation. En règle générale, l'évaluation a lieu une fois le projet terminé, tandis que la gestion de l'efficacité s'inscrit dans une démarche globale. Son objectif est donc d'offrir la capacité de gérer le projet correctement. A cet égard, en ce qui concerne la gestion de l'efficacité des projets de cybergouvernement, les pouvoirs publics coréens ont mis en place une approche globale dans le cadre de laquelle l'entité s'occupant de la mise en oeuvre d'un projet de cybergouvernement bénéficie d'un service de consultation préalable et d'une analyse à mi-parcours.

On trouvera ci-après des informations plus détaillées sur le modèle de gestion de l'efficacité des projets de cybergouvernement et sur ce qui a été fait pour généraliser la pratique de gestion de l'efficacité à toutes les entités s'occupant de la mise en oeuvre de projets de cybergouvernement.

4.2.2 Organisation de la gestion de l'efficacité des projets de cybergouvernement

La gestion de l'efficacité des projets de cybergouvernement concerne la totalité du processus de mise en oeuvre d'un projet (choix, mise en oeuvre et évaluation). La figure ci-après illustre l'organisation de la gestion de l'efficacité du cybergouvernement.

Figure 1 – Organisation de la gestion de l'efficacité du cybergouvernement



L'analyse de la demande, qui comprend les deux étapes du processus d'examen, permet de choisir un nouveau projet, lequel est ensuite confirmé. Avant la mise en oeuvre du nouveau projet, chaque entité doit élaborer son propre plan de gestion de l'efficacité qui décrit les méthodes de suivi et d'évaluation du projet et devrait donc prévoir une définition claire de l'objectif du projet et une description précise des indicateurs permettant de mesurer les résultats.

Par conséquent, l'entité de mise en oeuvre doit évaluer le projet sur la base du plan de gestion de l'efficacité qu'elle a élaboré. Pendant la mise en oeuvre, un service d'examen à mi-parcours/de consultation est assuré pour les projets de grande envergure (environ 10% du nombre total de projets de cybergouvernement). Ce service permet non seulement d'évaluer l'état d'avancement, mais aussi de résoudre les éventuels problèmes.

L'évaluation et le retour correspondent à la dernière étape de la gestion de l'efficacité. Les projets sont évalués selon cinq catégories: S, A, B, C et D. Un projet noté S sera prioritaire lors de l'affectation du budget suivant (avec parfois une augmentation du budget, si nécessaire). La note A signifie que le projet se poursuit sans modification.

Les projets notés B devraient subir des modifications au cours de l'étape suivante, tandis que les projets notés C doivent subir de profondes modifications. Les projets ayant reçu la note D doivent être complètement revus, faute de quoi aucun budget ne sera affecté.

4.2.3 Orientations futures

Mise en place en 2009 en Corée, la gestion de l'efficacité des projets de cybergouvernement devient essentielle et n'est plus une simple possibilité. Les projets de cybergouvernement nécessitent une gestion plus rigoureuse de l'efficacité que tout autre projet. Par conséquent, une analyse approfondie de la demande afin de choisir les nouveaux projets ainsi qu'un diagnostic et des consultations à mi-parcours ont été mis en place. Nous sommes convaincus qu'il faudra encore améliorer et modifier la gestion de l'efficacité pour s'adapter à l'évolution de l'environnement dans lequel les projets de cybergouvernement sont mis en oeuvre.

4.3 eGovFrame: Plate-forme ouverte avec innovation ouverte

4.3.1 Aperçu

L'application de divers cadres de développement est à l'origine de nombreux problèmes, comme les difficultés de maintenance des systèmes, la dépendance des fournisseurs et le manque de compatibilité opérationnelle entre systèmes. Pour les résoudre, le Gouvernement coréen a élaboré un cadre de développement standard pour le cybergouvernement, appelé eGovFrame. Pour normaliser ce cadre logiciel, eGovFrame, de nombreuses parties prenantes ont exprimé leurs opinions et fait part de leurs questions. De grandes entreprises craignaient l'effondrement d'un marché dominé, les organismes publics étaient préoccupés ne sachant pas où obtenir un soutien technique stable, les développeurs rejetaient les outils nouvellement créés, le gouvernement était préoccupé par l'efficacité des activités et les PME étaient concernées par la promotion du projet centré uniquement sur les grandes entreprises. De nombreuses parties prenantes devaient se mettre d'accord sur la normalisation du cadre logiciel. Pour réaliser la normalisation du cadre logiciel en répondant à ces questions, nous avons mis en oeuvre une stratégie d'innovation ouverte en quatre phases: 1) Sourçage ouvert; 2) Processus ouverts; 3) Résultats ouverts; et 4) Ecosystème ouvert. Le cadre eGovFrame ainsi que la stratégie d'innovation ouverte seront examinés de manière approfondie.

Le Gouvernement coréen a exécuté de nombreux projets de cybergouvernement et a développé de nombreuses applications dans ce domaine. Des cadres logiciels ont été appliqués à bon nombre de ces projets. Le cadre logiciel est un outil utile pour augmenter la productivité et améliorer la qualité du développement d'applications et, aujourd'hui, il est devenu un outil courant que l'on utilise pour le développement d'applications de cybergouvernement, mais ces cadres présentent également parfois des inconvénients. Pour y remédier, le Gouvernement coréen s'est efforcé de normaliser un cadre logiciel - l'eGovFrame. De nombreuses parties intéressées ont exprimé leurs opinions et fait part de leurs questions. Pour résoudre ces problèmes, nous avons mis en oeuvre une stratégie d'innovation ouverte et avons créé l'écosystème ouvert du cadre eGovFrame.

4.3.2 Le cadre eGovFrame dans son contexte

La Corée considère que la cybergouvernance est un outil essentiel à utiliser pour améliorer la compétitivité de son gouvernement, en s'appuyant sur les meilleures technologies mondiales de l'information et de la communication (TIC), y compris l'Internet large bande. Après avoir préparé le terrain à la cybergouvernance, le Gouvernement coréen a inscrit ce sujet national majeur sur son agenda pour les années 2000. En conséquence, la cybergouvernance est fermement ancrée dans tous les secteurs du Gouvernement coréen et a donné des résultats visibles. La communauté internationale a fait un excellent accueil à l'efficacité du cybergouvernement de la Corée. Ce cybergouvernement est considéré comme l'un des meilleurs du monde par les organisations internationales, notamment l'Organisation des Nations unies et plusieurs systèmes de cybergouvernance sont désormais exportés à l'étranger.

Pour obtenir ces résultats, le Gouvernement coréen a exécuté de nombreux projets de cybergouvernance et a développé de nombreuses applications dans ce domaine. Des cadres logiciels ont été appliqués à bon nombre de ces projets. Le cadre logiciel est un outil utile pour augmenter la productivité et améliorer la qualité du développement d'applications et, aujourd'hui, il est devenu un outil courant que l'on utilise pour le développement d'applications de cybergouvernance, mais ces cadres présentent également parfois des inconvénients.

En appliquant des cadres logiciels, les projets de cybergouvernance deviennent très dépendants des cadres des entreprises de TI. En conséquence, il est difficile d'entretenir une application sans le soutien technique du fournisseur de cadre qui a mis en oeuvre l'application d'origine. Dans le cas de projets continus, le cadre appliqué dans le projet précédent constitue un obstacle technique aux nouveaux compétiteurs, ce qui constitue un cercle vicieux avec des inégalités sur le marché des logiciels. La dépendance vis-à-vis d'un cadre d'entreprise de TI provoque un certain nombre de problèmes. Premièrement, la logique d'une application dépend également d'un certain cadre. Deuxièmement, du fait

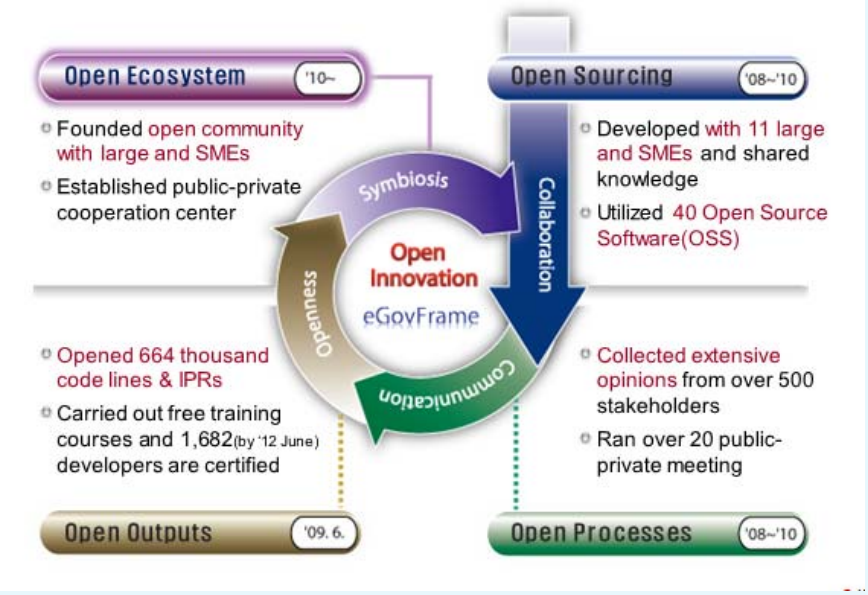
que certains cadres sont comparables à une boîte noire, seul le fournisseur du cadre peut entretenir l'application et il crée ainsi la dépendance. Troisièmement, des cadres multiples sont à l'origine d'activités redondantes dans la constitution des processus d'application, le recrutement, l'enseignement et la maintenance.

Pour résoudre ces problèmes, le Gouvernement coréen a normalisé un cadre logiciel, l'eGovFrame (Cadre standard de cybergouvernance). L'eGovFrame est un ensemble normalisé d'outils logiciels pour développer et exploiter des applications de cybergouvernance afin d'améliorer l'efficacité de l'investissement dans les TIC et la qualité des services de cybergouvernance. Il insiste sur l'amélioration de la possibilité de réutilisation et de la compatibilité opérationnelle des applications de cybergouvernance en définissant un cadre standard pour le développement de logiciels de cybergouvernance, assurant ainsi l'indépendance vis-à-vis des entreprises de TI en adoptant des outils logiciels ouverts et neutres et en améliorant la compétitivité des PME du secteur des TI, en partageant ouvertement les outils via les diverses filières.

4.3.3 Stratégie d'innovation ouverte

Afin de résoudre les problèmes posés par la normalisation d'un cadre logiciel pour la cybergouvernance, nous avons élaboré une stratégie basée sur le modèle de l'innovation ouverte désigné par l'expression Stratégie d'innovation ouverte. La normalisation du cadre de cybergouvernance ne pouvait être le résultat des seuls efforts du Gouvernement coréen. Elle exige non seulement des efforts et de la promotion mais aussi la connaissance de nombreuses parties prenantes, leur participation, leur coopération et leur retour d'information. Pour respecter ses exigences afin de réaliser la normalisation et l'application du cadre de cybergouvernance, notre stratégie est composée de quatre phases, sourçage ouvert, processus ouvert, résultats ouverts et écosystème ouvert. La Figure 2 illustre la structure d'ensemble de la Stratégie d'innovation ouverte.

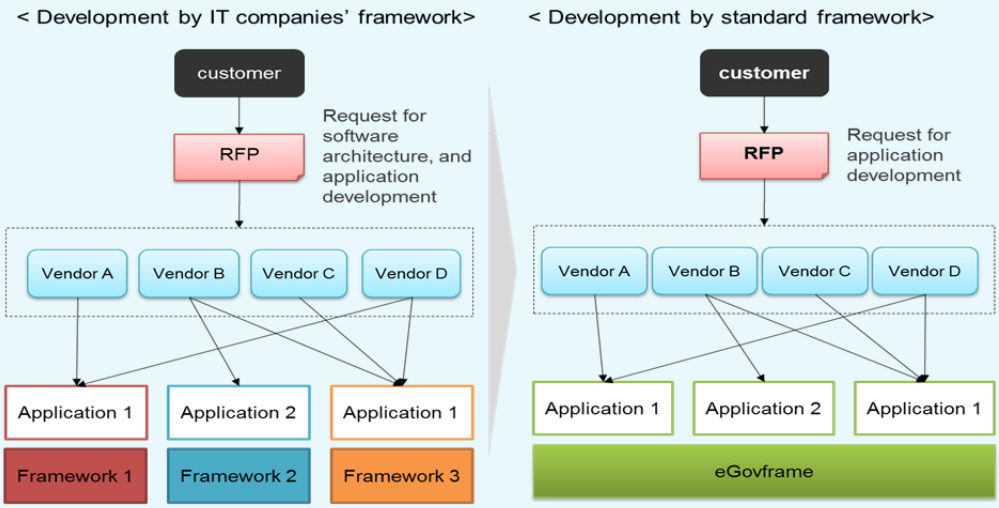
Figure 2 – Stratégie d'innovation ouverte



Sourçage ouvert

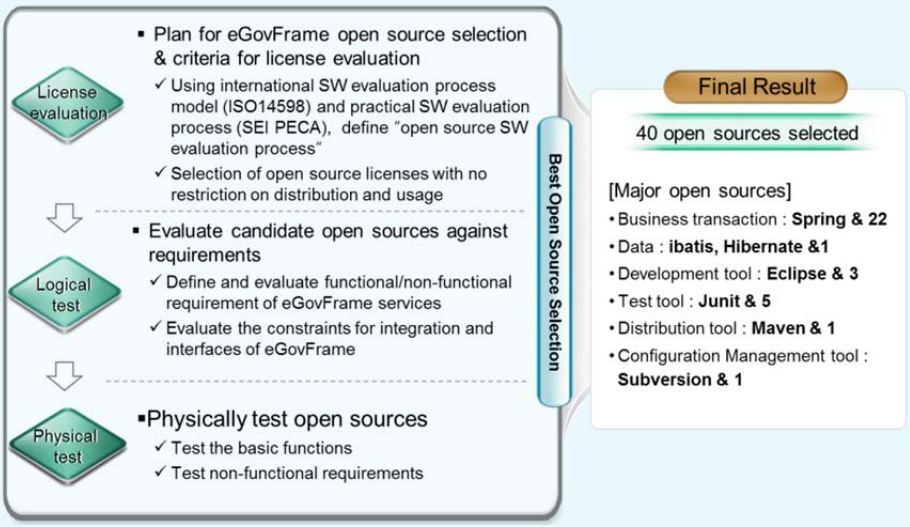
Afin de normaliser l'eGovFrame, on a procédé à des analyses d'environnement et de fonctionnalités des cadres de cinq grandes entreprises du secteur des TI, ainsi qu'à une enquête et à des entretiens approfondis avec toutes les parties intéressées. Au final, on a retenu quatre environnements se composant de 13 groupes de services et 54 fonctionnalités de services. Pour éviter le développement répété de plusieurs fonctions entre systèmes de gouvernement, on a procédé à une analyse de 67 projets de cybergouvernance, des années 2004 à 2007 et, plus précisément, 31 114 fonctionnalités ont été examinées. Les critères d'extraction des fonctionnalités communes pour les composants étaient la forte probabilité de travaux de développement répétés, la réutilisation de systèmes gouvernementaux et l'adoption de normes. Après cinq processus d'affinage, 219 composants communs ont été définis.

Figure 3 – Schéma recherché de l'eGovFrame



Pour réduire la dépendance vis-à-vis des grandes entreprises du secteur des technologies de l'information, on a sélectionné des sources ouvertes connues et ayant fait leurs preuves. En utilisant le modèle international de processus d'évaluation de logiciels (ISO 14598) et le processus pratiques d'évaluation de logiciels (SEI PECA), on a défini le processus d'évaluation du logiciel ouvert pour l'eGovFrame. Dans le premier test logique, on a évalué 175 logiciels ouverts par rapport à des exigences axées, pour l'essentiel, sur les contraintes d'intégration et des interfaces de l'eGovFrame. Dans le second test physique, 85 logiciels ouverts, issus du premier test de logique, ont été évalués en ce qui concerne les fonctions de base et les exigences non fonctionnelles. Au final, on a sélectionné 40 logiciels ouverts pour la composition de l'eGovFrame. L'eGovFrame à source ouverte présente plusieurs avantages. Il peut facilement adopter des technologies évoluant rapidement et être utilisé dans des applications de cybergouvernance à l'étranger.

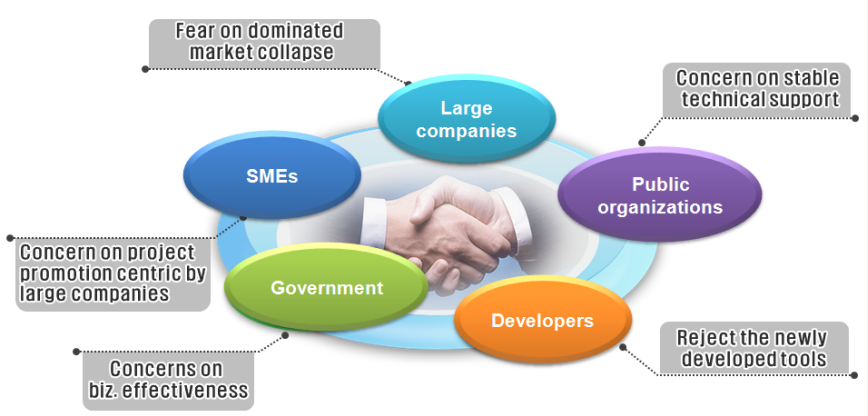
Figure 4 – Evaluation et sélection finale de la source ouverte



Processus ouverts

Les processus de développement sont ouverts au public qui crée l'environnement permettant de recueillir de nombreuses opinions de plus de 500 parties prenantes. En outre, nous avons organisé 20 réunions avec le secteur public et le secteur privé, qui ont permis à de nombreuses parties prenantes de mieux se comprendre et à un consensus de se dégager.

Figure 5 – Un grand nombre de parties intéressées à l'eGovFrame



Résultats ouverts

Tous les résultats, comme les codes sources et les diagrammes ER, sont communiqués au public et sont disponibles sur le site Internet de l'eGovFrame (www.egovframe.go.kr), qui constitue un environnement propice encourageant la participation volontaire de développeurs, de fournisseurs ainsi que de fonctionnaires du gouvernement, au processus de mise en oeuvre. Nous avons également organisé des formations gratuites et 1 236 développeurs ont reçu une certification.

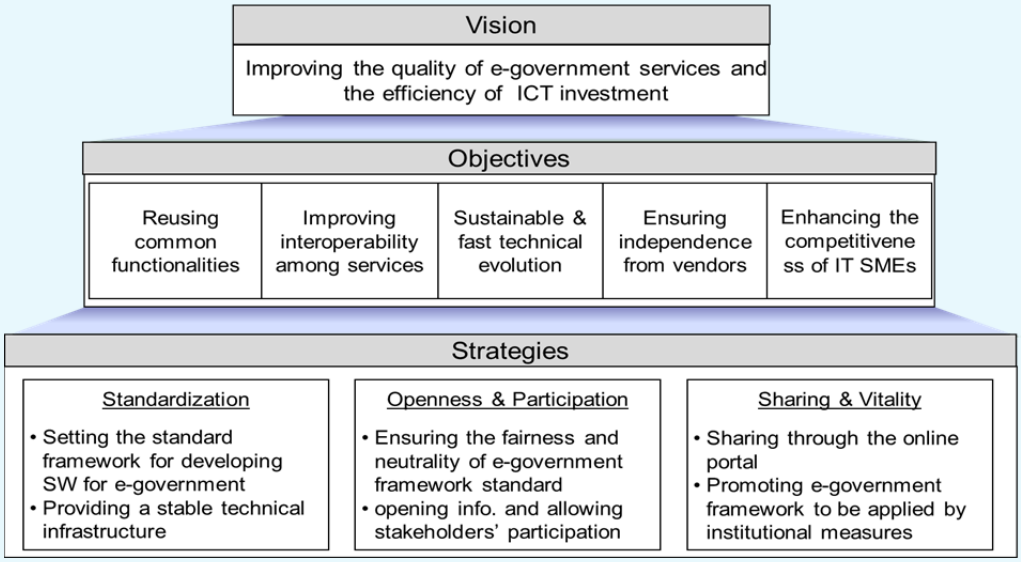
Ecosystème ouvert

Nous avons créé une communauté ouverte avec des grandes entreprises et des PME et établi un centre de coopération public–privé. Ces entités forment le noyau qui fait la promotion de l'eGovFrame au niveau mondial, fournit un appui technique solide et ne cesse d'apporter des améliorations. L'amélioration permanente de l'eGovFrame est assurée par cette communauté ouverte, par des réunions trimestrielles d'experts et par un forum ouvert qui regroupe les partenaires du secteur public et du secteur privé. Ainsi, nous établissons l'écosystème ouvert pour l'eGovFrame.

4.3.4 Evolution et avantages de l'eGovFrame

Ce projet vise à fournir un jeu normalisé d'outils logiciels dénommé eGovFrame pour le développement et l'exportation d'applications de cybergouvernance afin d'accroitre l'efficacité des investissements dans les TIC et la qualité des services de cybergouvernance. Il a pour objectif d'améliorer la réutilisation et la compatibilité opérationnelle des applications de cybergouvernance en définissant un cadre standard pour le développement de logiciels pour la cybergouvernance, assurant ainsi l'indépendance vis-à-vis des entreprises de TI en adoptant des outils logiciels ouverts et neutres et en améliorant la compétitivité des PME du secteur en partageant ouvertement les outils via les diverses filières.

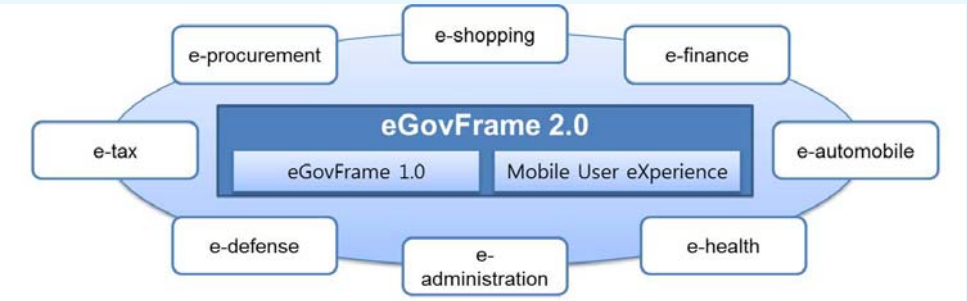
Figure 6 – Vision et stratégies de l'eGovframe



L'eGovFrame est issu de logiciels à code source libre, connus et ayant fait leurs preuves; tous les codes source sont ouverts et accessibles via le portail en ligne par toutes les parties prenantes. Il se compose de quatre environnements logiciels: environnement d'exploitation pour les applications, environnement de développement pour les développeurs d'applications, environnement de gestion qui regroupe les responsables du cadre et environnement opérationnel pour les opérateurs d'applications.

Au cours de l'étape de développement d'applications, on peut économiser environ 30% du coût et des efforts de développement en appliquant l'eGovFrame. Cela signifie que l'eGovFrame fonctionne comme un tampon pour adapter diverses applications à un type spécifique d'infrastructure. Il sert également de base commune au développement de fonctions courantes. La version la plus récente, eGovFrame 2.0, a été mise en service en octobre dernier avec un composant Mobile User eXperience (voir Figure 7).

Figure 7 – eGovframe 2.0



Sector	Projects with eGovframe	Sector	Projects with eGovframe
Administration	national Representative portal	Media	broadcasting telecommunication integration information system
Transportation	Seoul metropolitan rail transit management system	Patent	patent net system
Medical	hospital strategy management system	Tax	national tax office ITSM enhanced system
Military	war fighting symbology management system	Port	Incheon U-port system
Customs	global high-tech port logistics system	Culture	national assembly electronic library system
land	land information management system	Education	university information management system

Secteur	Projets avec eGovFrame	Secteur	Projets avec eGovFrame
Administration	Portail national représentatif	Média	Système d'information relatif à l'intégration des télécommunications et de la radiodiffusion
Transport	Système de gestion de transit ferroviaire métropolitain de Séoul	Brevets	Système net de brevets
Médecine	Système de gestion stratégique d'hôpitaux	Fiscalité	Système amélioré ITSM de la fiscalité nationale
Militaire	Système de gestion symbolique de combat	Port	Système U-port d'Incheon
Douanes	Système de logistique portuaire high-tech global	Culture	Système électronique de la Bibliothèque nationale
Terre	Système de gestion de l'information de terre	Education	Système de gestion de l'information des universités

4.3.5 Expansion et avenir de l'eGovFrame mobile

Avec l'utilisation croissante de dispositifs mobiles de pointe comme les téléphones intelligents et les tablettes, la demande de services basés sur des dispositifs mobiles est en pleine expansion, tant dans le secteur public que dans le secteur privé. Pour répondre à cette nouvelle demande et pour améliorer la qualité et l'efficacité de l'eGovFrame, on a lancé fin 2011 la version eGovFrame 2.0, à laquelle ont été intégrés le HTML 5 et de nouvelles caractéristiques de l'interface utilisateur. Cette version est compatible avec au moins trois navigateurs mobiles (Chrome, Safari et FireFox). De nombreux services de cybergouvernance mobile en Corée ont été développés en utilisant l'eGovFrame 2.0 (voir Figure 7).

Pour utiliser des caractéristiques mobiles comme les vibrations, le contrôle par caméra, la boussole, etc., l'eGovFrame 2.0 comportera également de nouveaux composants compatibles avec la création d'applications mobiles. Cette nouvelle version devrait encourager les développeurs de logiciels à mettre au point une variété de services Internet mobiles et d'applications mobiles.

4.3.6 Opportunités pour d'autres pays

Fort de sa réussite, le Gouvernement de la République de Corée contribue au développement de l'informatisation au plan international. Ce cadre normalisé suscite le vif intérêt des pays qui souhaitent régler des problèmes de monopole de certains fournisseurs ou qui souhaitent davantage dépendre de logiciels à code source ouvert. L'eGovFrame est déjà utilisé dans plusieurs autres pays, comme le montre le Tableau 1.

Tableau 1 – Pays ayant adopté l'eGovFrame

Pays	Projets	Organismes concernés	Durée du projet
Bulgarie	Système administratif de l'université de Sofia	Université de Sofia	11/2011~10/2012
Equateur	Système de guichet unique	Administration des douanes d'Equateur	01/2011~03/2013
Viet Nam	Investissement dans la modernisation et l'extension du projet de réseau d'alimentation en eau	Ministère des ressources nationales et de l'environnement (MONRE)	09/2010~12/2013
Mongolie	Système d'enregistrement de l'Etat	Autorité générale chargée de l'enregistrement de l'Etat	07/2011~06/2012
Tunisie	Système d'approvisionnement électronique	Observatoire national des approvisionnements publics	11/2011~11/2012

D'autres pays en développement sont très désireux de bénéficier de l'expérience de la Corée dans le domaine du cybergouvernement, plus précisément ce qui concerne l'eGovFrame. Pour y répondre, le gouvernement coréen contribue de diverses manières à améliorer les services de cybergouvernance dans d'autres pays, notamment en coopérant activement avec des organisations internationales. Pour encourager d'autres pays à adopter l'eGovFrame, le code source peut être téléchargé depuis la version anglaise du portail (http://eng.egovframe.go.kr); le Gouvernement coréen propose également un soutien technique en ligne. De plus, des sessions de formation à l'eGovFrame sont également organisées dans le cadre, par exemple, du Programme Korea IT Learning (KoIL) et du Information Technologies Cooperation Center (ITCC) dont la mission est de promouvoir la coopération mutuelle dans le secteur des technologies de l'information entre la République de Corée et des pays partenaires.

5 Domaines d'application présentant un intérêt pour les pays en développement

5.1 Lignes directrices concernant l'identification des domaines d'application

Dans le monde hyper-technologique d'aujourd'hui, les TIC sont en train de devenir le pivot des programmes de modernisation de l'Etat, et ce non seulement dans les pays développés. Les pays en développement prennent conscience que le potentiel des nouvelles technologies transforme le mode de fonctionnement des services publics. Si l'on connaît bien l'utilisation par ceux-ci des TIC (le "cybergouvernement"), qui fait partie intégrante de l'activité de l'Etat, il faut encore élaborer des lignes directrices concernant l'identification des domaines d'application et l'établissement de priorités dans l'intérêt des pays en développement. Ces lignes directrices devraient traiter des points suivants:

1) Caractéristiques particulières propres à chaque pays en développement (conditions économiques et sociales).

2) Besoins de chaque pays et capacités actuelles.

3) Priorité pour les applications présentant le plus grand intérêt pour les pays en développement.

4) Examen de l'utilisation de plates-formes mobiles et hertziennes pour les relations entre les pouvoirs publics et les administrés (demandes de renseignements et fourniture de services publics).

Les domaines d'application pour les pays qui commencent seulement à mettre en place des services de cybergouvernement peuvent être sélectionnés à la lumière des principes suivants:

- Programmes les plus étroitement liés à la vie quotidienne des habitants, de sorte qu'ils puissent bénéficier au maximum des nouveaux services électroniques.
- Programmes intégrant principalement divers processus d'activité, d'une organisation à l'autre.
- Optimisation des échanges d'informations entre organismes publics pour éliminer les doubles emplois dans la collecte et la gestion des données.
- Promotion de l'utilisation des TIC pour rationaliser les processus administratifs grâce à la méthode de remise à plat des processus (BPR).

Au même titre que ces principes, il nous faut prendre en compte, d'une part la pénurie de ressources nationales affectées au cybergouvernement, surtout dans les pays en développement, et d'autre part l'urgence qu'il y a à appliquer les principes du cybergouvernement pour faire progresser le pays. La solution repose sur trois éléments clefs: stratégie, sélection et concentration. Un petit nombre de projets de cybergouvernement sont sélectionnés sur la base des principes définis plus haut et les ressources, limitées, sont concentrées sur ces projets.

5.2 Infrastructures

- Modernisation du système juridique pour le cybergouvernement et la sécurité
- Formation du personnel et restructuration de la gouvernance dans le domaine des TIC
- Système d'authentification électronique

5.3 Services G2G

- Système de documents électroniques connecté aux systèmes publics, par exemple système de marchés publics, d'administration locale, de taxation, etc.
- Système d'administration locale
- Système de gestion des finances publiques (à l'échelle nationale et locale)
- Système d'échange d'informations

5.4 Services G2C et G2B

Expériences et enseignements concernant la mise en oeuvre de services conviviaux, l'intégration et la personnalisation des services publics, l'utilisation de plusieurs canaux, l'amélioration de la qualité des services en fonction des besoins des usagers et la commercialisation des services de cybergouvernement.

- Système de portail pour la fourniture de services publics aux administrés.
- Système de taxation sur Internet.
- Système de marchés publics en ligne.

6 Facteurs assurant la réussite des activités de cybergouvernement

6.1 Leadership présidentiel (Appui politique)

- Les projets nationaux dans le secteur des technologies de l'information, en particulier les projets de cybergouvernement, font généralement intervenir plusieurs organismes, d'où des risques de désaccord. La prise de décision est souvent interrompue par des rivalités bureaucratiques entre les ministères concernés.
- Assurer la coordination entre les organismes impliqués dans le déploiement des réseaux et la mise en oeuvre d'applications est peut-être le plus grand défi que doivent relever les projets de cybergouvernement. Chaque organisation doit tenir compte de son niveau de risque, de la nature de ce risque et des mesures d'incitation. Il est vraisemblable qu'il n'existe aucun modèle qui soit adapté aux besoins de toutes les organisations. Pour tenter de remédier à ce problème, une commission de haut niveau est créée à l'échelle interministérielle afin de résoudre les différends entre les organismes publics. L'efficacité des travaux de cette commission dépend de l'appui reçu au niveau présidentiel.
- Les projets du secteur des technologies de l'information nécessitent de très importants investissements, sans retour sur investissement immédiat. En outre, ces projets n'étant pas visibles, il n'est pas facile d'en présenter les résultats à ceux qui ont pour fonction d'affecter des crédits à des projets publics.
- Même si beaucoup sont conscients du potentiel offert par l'utilisation de ces technologies et de leurs incidences sur l'efficacité et la compétitivité, les responsables de l'affectation des crédits publics n'ont pas trouvé de preuves tangibles qui puissent les convaincre des avantages de ces technologies. Pour surmonter ce problème, il est essentiel que le Président exerce son leadership et reconnaisse le potentiel des technologies de l'information. Ainsi, le Président de la Corée a décidé en 1987 d'affecter des crédits extra-budgétaires à l'utilisation exclusive de projets dans ce domaine. Cette décision témoigne d'une ferme volonté politique en Corée dès le lancement de projets dans le secteur.

6.2 Equilibre entre l'offre et la demande de services de cybergouvernement

- Un plan directeur national type axé principalement sur l'offre est souvent considéré comme prioritaire dans le pays. Le gouvernement considère comme primordial le développement de services d'application qui sont d'abord proposés aux particuliers pour créer une demande. Toutefois, il faut se demander quelles sortes de services justifient les importants investissements consentis dans les projets de cybergouvernement. Le risque est en effet de créer une solution coûteuse pour résoudre un problème inexistant.
- L'accent mis sur l'offre n'empêche pas de tenir compte de la demande potentielle pour un service précis. Le problème est que les projets dans le secteur des technologies de l'information ont manifestement créé une demande qui rend pratiquement impossible de prévoir ce que sera la demande tant que l'offre n'existe pas. Il importe que la stratégie adoptée aille de pair avec la création de la demande, suite à la mise en oeuvre de systèmes TIC, par exemple grâce à la formation des utilisateurs éventuels du système, ce qui leur permettra de bénéficier pleinement des avantages de ces technologies.
- Afin d'équilibrer l'offre et la demande de services de cybergouvernement, il faut tenir compte de tous les aspects du service projeté. Ainsi, l'examen des transactions hors ligne entre l'administration publique et les administrés permet de tenir compte de la demande au moment de définir sur quels services porteront les projets de cybergouvernement. Cela pourrait compenser la non-prévisibilité de la demande, puisqu'on peut espérer que plus le nombre de transactions hors ligne sera élevé, plus la demande de services en ligne sera forte.

6.3 Ce qu'est le cybergouvernement

- Dans "cybergouvernement", l'accent est mis plus sur "gouvernement" que sur "cyber". Fondamentalement, ce concept vise à transformer l'administration publique pour qu'elle modernise ses relations, en interne et à l'extérieur, à l'aide des TIC. Les questions de cybergouvernement devraient être à l'ordre du jour de la réforme de l'administration publique et des projets de bonne gouvernance. La problématique de la modernisation de l'administration existe depuis que l'on a commencé à introduire des applications informatiques, mais son incidence réelle et concrète sur les méthodes de travail n'apparaît que très lentement.
- Au lieu de se contenter de mettre en oeuvre les technologies de l'information, les Etats doivent décider de la transformation des procédures administratives, la guider et la superviser, de manière à mettre ces technologies au service de la restructuration des processus.
- On attend du cybergouvernement qu'il se traduise par des changements radicaux et en profondeur dans les activités internes de l'Etat et les services proposés aux administrés. Ces changements sont fonction de la technologie employée, en particulier pour l'Internet, ce qui permet au secteur public de mener ses activités de manière intégrée. Encouragée par les échanges d'informations, l'intégration concerne généralement des groupes d'organismes publics ayant en commun certaines fonctions ou proposant un même service. La plupart des projets de cybergouvernement passent par une phase de remise à plat des processus avant le début de la mise en oeuvre proprement dite. Cette remise à plat se fait habituellement en plusieurs étapes: analyse des processus correspondant aux objectifs des organisations, suppression des doubles emplois, rationalisation des méthodes de travail et simplification des processus complexes.
- La suppression des doubles emplois et la rationalisation des processus impliquent de restreindre le nombre d'emplois offerts, ce à quoi risquent de s'opposer les personnes concernées. Celles qui sont habituées à des méthodes de travail traditionnelles sont peu enclines à accepter ces changements. Il nous faut donc créer des mesures d'incitation pour les fonctionnaires, ainsi que des structures assurant une coordination entre les organismes publics concernés. Ces mesures d'incitation peuvent être le recyclage ou le redéploiement d'employés selon leurs souhaits. Pour renforcer l'efficacité et la réactivité du secteur public, il faudra supprimer les processus inutiles, simplifier les processus complexes et uniformiser les processus différents.

6.4 Encourager les citoyens à s'engager et à participer

- Conséquence de l'élargissement des possibilités d'interaction entre l'administration et les administrés: ces derniers expriment de plus en plus leur volonté de participer à la prise de décisions, sous l'influence d'une part, de la démocratisation de la vie publique et d'autre part, de la généralisation de l'Internet qui facilite l'accès à divers organismes publics. Il faut bien réfléchir à la façon dont la technologie permet à un particulier de faire entendre sa voix, sans se perdre dans la masse des participants au débat public. Par exemple, l'administration devrait être en mesure de répondre aux opinions exprimées par chacun.
- Pour pouvoir s'exprimer utilement en ligne, les administrés doivent être aussi informés que possible des questions d'intérêt public, tandis que les responsables publics doivent être conscients des perspectives qu'ouvre l'Internet et des contraintes qu'il impose concernant la participation des citoyens à la prise de décisions.

6.5 Modernisation de la gestion des ressources d'information

Comme les projets de cybergouvernement se traduisent par une accumulation des ressources informatiques dans divers secteurs, il est impératif d'apprendre à gérer ces projets de manière à éviter le gaspillage de ces ressources. Avec ce mode de gestion, les organismes publics doivent collaborer en vue de partager et d'intégrer au maximum leurs ressources informatiques.

Une méthode de gestion telle que l'architecture d'entreprise tient compte des relations existantes ou en projet entre les processus d'entreprise et les ressources informatiques en vue d'assurer le partage des informations et l'intégration des processus dans les organisations et entre elles. Elle évite en outre aux organismes publics d'acheter en double des équipements informatiques, pour améliorer l'efficacité de leurs investissements.

Cette méthode met l'accent sur le partage des informations et l'amélioration de l'investissement en fournissant des lignes directrices et des modèles de référence pour chaque composante. Ces modèles de référence sont destinés à encourager l'identification et l'utilisation communes, le partage de données, des processus d'entreprise, des applications logicielles et du matériel informatique. Des lignes directrices sont établies pour une gestion rationnelle des ressources d'information, sur la base des éléments qui devraient rester stables dans le contexte de l'évolution des priorités de l'entreprise et des équipements technologiques.

6.6 Protection de la vie privée et sécurité des systèmes

- Dans la mesure où les informations conservées par un organisme sont de plus en plus souvent partagées avec d'autres parties dans le contexte du cybergouvernement, les utilisateurs de ces services craignent que des données personnelles ne soient utilisées mal à propos ou de façon abusive. Il faut parvenir à un compromis entre la protection des données personnelles et les échanges d'informations visant à accélérer le développement d'applications électroniques. Il est impératif de concilier le partage de données entre les organismes et l'élaboration de mesures de protection de la confidentialité.
- Etant donné que les inconvénients des applications informatiques commenceront à se faire sentir à mesure que le cybergouvernement évoluera, il faudrait renforcer les mesures de protection de la vie privée pour concilier les deux extrêmes. Les systèmes de cybergouvernement sont toujours exposés aux attaques de l'extérieur, et parfois même de l'intérieur. Il faut donc prévoir à l'avance des mesures techniques, juridiques et institutionnelles visant à lutter contre le piratage, la contrefaçon et la fraude.

6.7 Stratégies d'adoption des services de cybergouvernement

- Même quand des cyberservices sont à disposition, leur adoption par le public et par les entreprises n'est pas automatique. Les particuliers ne sont prêts à les accepter que s'ils pensent pouvoir en retirer un avantage réel. Il est fréquent que les services électroniques soient facturés en dessous de leur prix réel au début de la mise en oeuvre de projets de cybergouvernement, ce qui pose la question de l'opportunité de poursuivre ces projets.
- Il faudrait analyser attentivement les applications Internet utilisées dans le secteur public pour définir comment les moderniser de manière que les usagers en expérimentent les avantages. Les canaux d'accès doivent être suffisamment larges pour que l'accès soit facile et le nombre d'hyperliens doit être suffisamment faible pour que l'utilisateur moyen puisse trouver le site qui lui donnera les informations et services demandés.
- Au lieu de s'occuper de toutes les applications, il est préférable de se polariser sur quelques-unes – les plus importantes – qui facilitent les interactions en ligne entre administration et administrés. Lorsqu'on décide de moderniser des applications de cybergouvernement, il faut viser en priorité les services les plus demandés par les particuliers, pour que le plus grand nombre ait accès à leurs avantages.

7 Lignes directrices relatives à la promotion des activités de cybergouvernement et identification des domaines d'application du cybergouvernement pour les pays en développement

7.1 Portée

Les présentes lignes directrices traitent de la promotion des activités de cybergouvernement et de l'identification des domaines d'application du cybergouvernement pour les pays en développement.

7.2 Objet des Lignes directrices

2.1 Les présentes lignes directrices ont pour objet de guider les pays en développement en les aidant à identifier les facteurs de succès des activités de cybergouvernement et les domaines dans lesquels les applications de cybergouvernement peuvent leur être le plus utiles.

2.2 Ces lignes directrices présentent:

a) des indications permettant d'identifier les domaines d'application du cybergouvernement intéressant les pays en développement, chaque pays ayant sa spécificité;

b) les facteurs à prendre en compte pour assurer la réussite des projets de cybergouvernement dans les pays en développement.

7.3 Lignes directrices pour l'identification des domaines d'application intéressant les pays en développement

3.1 Il existe un grand nombre d'applications de cybergouvernement, domaine dans lequel toutes les activités, ou presque, peuvent être transformées par l'utilisation des technologies de l'information et de la communication.

3.2 L'identification de ces domaines d'application dans les pays en développement doit tenir compte des facteurs suivants:

c) Caractéristiques particulières propres à chaque pays en développement (conditions économiques et sociales).

d) Besoins de chaque pays et capacités actuelles.

e) Priorité pour les applications présentant le plus grand intérêt pour les pays en développement.

f) Examen de l'utilisation de plates-formes mobiles et hertziennes pour les relations entre les pouvoirs publics et les administrés (demandes de renseignements et fourniture de services publics).

g) Stratégies et mécanismes nationaux pour parvenir à une simplification de l'organisation et de l'administration et instaurer une collaboration entre organismes publics (services G2G).

h) Expériences et enseignements concernant la mise en oeuvre de services conviviaux, l'intégration et la personnalisation des services publics, l'utilisation de plusieurs canaux, l'amélioration de la qualité des services en fonction des besoins des usagers, la commercialisation des services de cybergouvernement, la protection des données personnelles et la sécurité des transactions liées au cybergouvernement (Services G2C et G2B).

7.4 Lignes directrices pour assurer le bon déroulement des activités de cybergouvernement

4.1 Pour s'assurer du bon déroulement des activités de cybergouvernement, les pays en développement devraient être en mesure de créer les conditions propices à la bonne mise en oeuvre de ces projets.

4.2 Plusieurs facteurs de réussite ont été identifiés sur la base de l'expérience de pays ayant mis en place des systèmes évolués de cybergouvernement. Il convient de prendre en compte ces facteurs dans la mise en oeuvre de tels systèmes:

i) Coordination efficace et forte volonté politique. Assurer une coordination entre les différentes organisations concernées pour ce qui est du déploiement du réseau et de la mise en oeuvre du système d'applications est peut-être le principal obstacle que doivent surmonter les projets de cybergouvernement.

j) Equilibre entre l'offre et la demande pour les services de cybergouvernement. En règle générale, un plan pour les TIC directeur national type axé principalement sur l'offre est souvent considéré comme prioritaire dans le pays. Le gouvernement considère comme primordial le développement de services d'application qui sont d'abord proposés aux particuliers pour créer une demande. Toutefois, il faut se demander quelles sortes de services justifient les importants investissements consentis dans les projets de cybergouvernement. Le risque est en effet de créer une solution coûteuse pour résoudre un problème inexistant.

k) Définition claire et correcte du concept de cybergouvernement. Dans "cybergouvernement", l'accent est mis plus sur "gouvernement" que sur "cyber". Fondamentalement, ce concept vise à transformer l'administration publique pour qu'elle modernise ses relations, en interne et à l'extérieur, à l'aide des TIC. Les questions de cybergouvernement devraient être à l'ordre du jour de la réforme de l'administration publique et des projets de bonne gouvernance.

l) Encourager les citoyens à s'engager et à participer. Conséquence de l'élargissement des possibilités d'interaction entre l'administration et les administrés: ces derniers expriment de plus en plus leur volonté de participer à la prise de décisions, sous l'influence d'une part, de la démocratisation de la vie publique et d'autre part, de la généralisation de l'Internet qui facilite l'accès à divers organismes publics. Il faut bien réfléchir à la façon dont la technologie permet à un particulier de faire entendre sa voix, sans se perdre dans la masse des participants au débat public.

m) Efficacité du suivi et de l'évaluation, avec un système de retour d'expérience adapté. La réussite ne se mesure pas à l'aune du bon démarrage d'un projet de cybergouvernement. Ce qui importe, en fin de compte, c'est l'achèvement du projet et les résultats obtenus. Parallèlement aux efforts déployés pour mesurer les avantages de l'investissement dans le secteur des TIC, il convient de prêter attention au suivi et à l'évaluation des projets de cybergouvernement pour bien comprendre les besoins des usagers et leurs attitudes face aux services électroniques. Les résultats de cette évaluation devraient être intégrés dans le mécanisme de retour d'expérience.

n) Gestion innovante et efficace des ressources d'information. Comme les projets de cybergouvernement se traduisent par une accumulation des ressources informatiques dans divers secteurs, il est impératif d'apprendre à gérer ces projets de manière à éviter le gaspillage de ces ressources. Avec ce mode de gestion, les organismes publics doivent apprendre à collaborer en vue de partager et d'intégrer au maximum leurs ressources informatiques.

o) Protection des informations confidentielles. Dans la mesure où les informations conservées par un organisme sont de plus en plus souvent partagées avec d'autres parties dans le

contexte du cybergouvernement, les utilisateurs de ces services craignent que des données personnelles ne soient utilisées mal à propos ou de façon abusive. Il faut parvenir à un compromis entre la protection des données personnelles et les échanges d'informations visant à accélérer le développement d'applications électroniques. Il est impératif de concilier le partage de données entre les organismes et l'élaboration de mesures de protection de la confidentialité.

p) Stratégies pour faire accepter les services de cybergouvernement par les administrés. Même quand des cyberservices sont à disposition, leur adoption par le public et par les entreprises n'est pas automatique. Les particuliers ne sont prêts à les accepter que s'ils pensent pouvoir en retirer un avantage réel. Il est fréquent que les services électroniques soient facturés en dessous de leur prix réel au début de la mise en oeuvre de projets de cybergouvernement, ce qui pose la question de l'opportunité de poursuivre ces projets..

Annexes

Annex 1: **Full Transcripts of contributed cases**

Annex 2: **Toolkit to create the ICT-based services using the mobile communications for e-government services**

Annex 1: Full Transcripts of Contributed Cases

Case 1: The INV (Information Network Village) Project (Republic of Korea)

1) Overview

The project aims to enable the people in remote areas to access to rich contents such as education, medical information, and agricultural skills reducing the digital gap between the urban and rural areas. It also provides capabilities to trade local specialties directly to consumers, gaining more money from the local production. Thus the project plays a role in boosting the local economy to balance the regional development nationwide. Training the basic internet skills for the people in remote areas is expected to expand the demand for the e-government services.

At the beginning the project has progressed very cautiously to avoid the potential waste of resources by taking the step-by-step strategy.

2) Objectives and strategies

There were several major objectives for the INV project. First, it aimed at building broadband internet infrastructure in agricultural/fishing villages, remote areas and other sites alienated from the information revolution in order to address an information gap between urban and rural areas. It was also hoped to cement the foundation for E-government and electronic democracy.

Second, the project aimed to create information content including online marketplace for local products to generate practical benefits and rejuvenate local economies for balanced national development. Third, it was designed to enable local residents to have easier access to information on education, medicine, culture and agricultural skills via the internet in daily life. Before the INV project was launched, cases for electronic villages in Europe and the U.S. (Tele-cottage, Tele-village) were analysed. The finding was that given the Korean situation, it was imperative for the central government to provide administrative, financial, and technical support.

Several strategies were carefully devised to efficiently carry out the project. First, “Information Network Village Planning Group” was formulated consisting of related organizations in the government as well as in the private sector to make sure close cooperation among relevant organizations. Second, the central government organizations and local governments (Municipality, Province, and City/District) took up different roles. MOGAHA set up the blueprint for the project, secured budget and support, prepared the legal, policy foundation and established a collaboration system for related organizations, while local authorities worked on building information content, and providing internet training for the residents.

Third, from the very beginning of the project, active engagement of local residents was emphasized. “Management Committee for INV Project” was formulated for each village with 15 resident representatives. The Committee identified critical issues in relation to information village operation. The creation of a business model was also encouraged, so that the Committee would be able to stand as a self-sustainable body even in the absence of government support. Fourth, pilot INV sites were selected for even representation of urban areas, agricultural/fishing villages and mountainous villages. In consideration of unique local characteristics, INV models were carefully designed in line with local needs and spread nationwide after strict evaluation.

3) Implementation

The project was implemented mainly in six tasks with an attempt to set up an internet environment, a precondition to realizing the contents envisioned in the information network village project.

a. High-speed Internet infrastructure

Establishing the high speed internet involves laying fibre optic cables underground and the installation of high-speed main devices. It also includes the connection of ADSL lines to each household and the construction of the internet network in the Village Information Center.

b. Village information center

Each village selected in the project was provided with resources to build an Information Center, equipped with PCs, LAN, beam projector and other devices. The Center produces an environment where residents can use the internet whenever they want to and learn how to adapt to information society. The Center is usually located at a place easily accessed by the residents such as a village hall or local public office.

c. Granting PCs

One of the most distinct characteristics of the program is free distribution of PCs. Selected households were provided with PCs in accordance with the distribution guidelines mapped out by the Operation Committee for the Information Network Village. This part of the project is to encourage the residents to join the program and raise the household PC penetration rate to 70%.

d. Internet Contents

Out of the six tasks, the most important is creating and providing information content in a way that makes the residents the biggest beneficiaries. Contents owned by various sectors of the government and private providers are collected, and customized. Contents specific to a certain local area are also available for the local people in a customized form. Since selected villages for the INV project are in remote areas, where school children are relatively ill positioned compared to urban kids, educational contents are provided through the cyber learning tools. A cyber marketplace has also been put in place to promote online transactions for special local products, bringing more income to residents.

e. Training Program

Learning how to use information systems through the INV project is a critical factor for the success of the project. Residents get basic internet skills training in various educational sites such as schools, local government training centres, and private institutes.

f. Public Awareness Program

This program involves holding various events to boost public awareness of the INV project. This program is an important part of the project, because success is not guaranteed by the residents' efforts only, but it also requires continuous interest and support from urban people, who serve as customers in the cyber market place. The information network village logo characterizing the project was designed to represent the identity and uniqueness of more than 380 villages. On top of that, aggressive public image making efforts were carried out, including running TV features, and subway and newspaper advertisements.

4) Changes and outcomes

The INV project is focused on advancing the IT capabilities of local residents to ensure they are able to survive in the rapidly changing information society. For instance, one of the goals of the INV project is to offer local residents public services online through the local e-government project. Since it was launched, the project has gone through 8 phases until the end of 2009, with each phase taking a year. The number of the villages involved in each phase is given in Table 1.

Table 1: Number of villages involved in each phase

Phase(Year)	1('01)	2('02)	3('03)	4('04)	5('06)	6('07)	7('08)	8('09)	Total
No. of Villages	25	78	88	89	26	34	30	12	380

Table 2: Statistics for outcomes (2001→2008)

	2001	2008
PC Diffusion	21%	72%
Broadband Internet	9%	66%

As a result of the INV project, the following outcomes have been achieved. First, the implementation of the aforementioned initiatives contributed to eliminating the digital divide by improving the internet usage environment for the information have-nots such as rural residents. The basic statistics describing the outcome of the INV project are shown in Table 2.

Second, a firm foundation was laid down for local people to receive e-government services available through e-government initiatives strongly driven by the Korean government. The need to visit public offices and the requirement to submit reference documents were dramatically reduced. Residents in the remote areas were enabled to enjoy those e-government services as a result of the training provided by the INV efforts.

Third, the improvement of the internet usage environment strengthened the foundation for participatory democracy. The success of e-government is shown by the overall increase of internet access among the residents. More information villages are being built in preparation for the full-fledged electronic democracy. The existing information villages serve as an education center for participatory democracy. This is in line with the decentralization initiative driven by the central government.

Fourth, it contributed to rejuvenating local communities. In the survey carried out by the Management Committee for the INV project, more than 60% of the residents in the information villages responded that residents were able to strengthen bonds with each other thanks to various online and offline activities enabled by the information system. In particular, the village information center is utilized to hold a village meeting, and show films or sport events such as World Cup Soccer games. It also serves as a center to nurture the sense of community and instill residential pride.

Fifth, the information network village contributed to enhancing regional competitiveness. Previously, local products were sold mainly through Agricultural Cooperative purchases, individual sales, and contract-based cultivation. After the launch of the INV project, the telecommunication-based sales increased. The information village homepage (www.invil.org) is serving as a tool to promote local competitiveness and provide information on how to deal with joint product shipments. The number of villages increases as agricultural income growth contributed by online trade of local products has been large enough to induce competition among participating villages and to provide corresponding incentives to potential villages.

Finally, the outcome of the INV project has proved that the project can solve new social problems in Korea. For instance, in Inje, a remote area in Kangwon Province, young Vietnamese ladies who have become Korean citizens through international marriage were recently provided with chances to talk with their families in their hometown using networked screens in the Inje village information center. The story grabbed media attention and demonstrates the project's effectiveness in solving social issues caused by the increase of multi-cultural families in Korea.

5) Challenges and success factors

When the project was proposed by MOGAHA, the government budget office initially rejected the proposal since it thought the INV cannot make a success. The INV is a regional IT project which could produce the desirable output only when people in the region are willing to take part in the project. However, people in the region don't show eagerness on the project since they are mostly senior citizens who are not good at using the computers. After a serious debate between the budget office and MOGAHA, the project was able to obtain the support of the budget office, when the issue of digital divide had been raised to indicate that the gap between the urban and rural areas in taking advantage of internet technology should be taken care of by the government policy.

In implementing the project, training program for senior citizens has been paid much attention to address the issue of digital divide. In addition, several incentives were created to attract people to the INV project such as placing the e-commerce program in the INV so that more profits are gained for those selling the products through e-trade.

6) International recognition and partnership with private enterprises

The INV project, designed to narrow the digital divide of information poor areas like farming and fishing villages, is being benchmarked by other countries. INV has drawn worldwide attention. It was introduced in various international workshops and seminars. It has been evaluated by development programs of international organizations such as the UN, OECD, and ADB as one of the best practices that can be applied to developing countries.

As a strategy for sustainable development of INV, we promoted the project in cooperation with private corporations. Participating villages are encouraged to set up sisterhood relationship with private companies interested in developing villages through the INV project. As one of these efforts, we held a field briefing for multinational IT companies which have branch offices in Seoul to seek cooperation.

In a visit to an information network village, for example, an executive of Intel (the world's largest chip maker) hailed the Korean INV project as an unprecedented example of digitalizing farming and fishing villages. In November 2004, when the Intel CEO visited the MOGAHA, he entered into a memorandum of understanding (MOU) with MOGAHA aimed at supporting INV and helping spread it to other countries. In accordance with the MOU, Intel helps the Korean government introduce the INV project and other e-government cases to 45 countries worldwide. The company also provides a future model of E-government, and shares the best practices of other countries to further promote IT applications in Korea.

Case 2: Local Government Information System (LGIN)

1) Overview of local Government structure in Korea

The Constitution of the Republic of Korea states that, "Local governments deal with matters pertaining to the welfare of local residents, manage property, and may within the limit of laws, enact provisions relating to local autonomy regulations." At the time of the project implementation, there were 16 Provincial governments, including seven metropolitan city governments and nine provincial governments, and 234 city/district governments. (Note: The number of each level of the local governments has slightly changed since then.)

Local government heads manage and supervise administrative affairs except as otherwise provided by law. The local executive functions include those delegated by the central government such as the management of public property, running facilities, tax assessment, the collection of local taxes, and fees for various services. Provincial governments have boards of education which deal with matters related to education and students' activities in each community. Provincial governments basically serve as intermediaries between the central and lower-level (city/district) local governments.

Lower-level local governments deliver services to the residents through an administrative district (*eup*, *myeon*, and *dong*) system. Each lower-level local government has several lower-level districts which serve as field offices for handling the needs of residents. *Eup*, *Myeon*, and *Dong* offices are engaged mainly in routine administrative and social service functions.

2) Strategies of the LGIN

Governments are facing serious pressure from constituents to drive down the costs of government services, improve customer service and more effectively share information across jurisdictional lines. Citizens are also asking governments to put the security and privacy issues at the center of government IT project implementation. The LGIN project would have been a failure without the consideration of these issues.

At the same time an e-government project should show a clear vision and goal. It is about where society is going and what the government is doing. Public relations and education should be used to share the vision and goals of the government with citizens. Citizen support has been essential to the success of the LGIN project since they are the end-users and final judges of the utility of the system.

Interfacing with the information system should be easy enough for users. If there are technical difficulties using the system, citizens who are not familiar with the technology might give up using the system which would make the project a failure. When designing the system interface for end-users, the characteristics of users should be taken into account. That is, system quality should reflect the end-user viewpoints. In the same context, management changes are a very important element impacting the probability of success of a project. Public officials are facing a new work environment due to newly implemented system like the LGIN. From a technical standpoint, standardization should be a core consideration. Information sharing across jurisdictions would be impossible without applying standardized technologies.

Sharing resources is a strategic approach to guarantee efficiencies and effectiveness as seen in the information sharing. The strategy extends to the cases of business processes and application services. OECD (2005), in an e-government project, titled “E-government for Better Government”, addresses the common business processes (CBPs) as a strategic tool to improve the seamlessness and quality of service delivery.

The concept of CBPs is similar to that of shared services that carry out functions common in various public organizations such as finance, procurement, and human resources. OECD defines CBPs as those business processes that exist in different organizations, and yet have, in essence, the same goals and outputs. This creates the possibility for the arrangements to conduct these business processes to be optimized and delivered in a more efficient and standardized manner.

Benefits from the CBPs approach can be expected in various areas, for example, avoiding duplicates, reusing application solutions, improving interoperability, and promoting integration across public organizations. In the meantime, there is a trade-off against this approach. It is pointed out that CBPs can rule out the opportunities for competition, innovation, and flexibility within government by imposing common solutions.

The Korean government has a relatively long history of making efforts to inventory common business processes linked to shared and integrated information system development. The CBP strategy has been a critical element in the process of implementing the LGIN system. This started back in 1997 at the local government level and in 2001 at central government level. Korea had 234 local governments at the city and district level. In 1997, a policy report indicated that all the 234 city/district governments had common business processes in 21 areas such as residents, vehicles, land, buildings, environment, construction, health, welfare, livestock, fisheries, water supply, and sewage. Based on the research results, the Korean government tried to streamline those 21 common business functions in local governments since 1997 by standardizing and redesigning business processes as well as by developing standardized and interconnected administrative information systems for the whole local governments nationwide. This is one of the pillars of e-government initiatives in Korea.

3) Implementation

The LGIN project was implemented with following two phases. Each phase went through the BPR (Business Process Re-engineering), analysing and streamlining work flows adequately fitted for the applications of IT. The first phase of the project took place between January 1998 and October 2000. It laid the foundations for transformation from the paper-based local administrations into the electronic framework. Ten work areas among the total of 21 parts were developed and implemented during the first phase. They include the management of citizenship, land registry, social welfare, environment, regional industry, rural village, construction, vehicle management, local tax, finances, and online public service.

While the digital management of data for the matters regarding citizenship and land registry, for example, had been initially established during the early 1990's, the LGIN project modified the databases in order to provide the information for relevant public officials in an online and real time format. That enabled information sharing among government agencies, leading to the improvement of internal operations of local governments, and the conveniences of public service delivery. In fact, information sharing across government bodies is a key concept in driving the success in the e-government initiatives.

The first phase of the project was preceded by the pilot test project, where five city/district governments had been selected to implement 10 work areas in advance. Errors and inconveniences had been detected in the course of developing and implementing the system in the selected local governments. The first phase had been immediately followed by the second phase of the project, starting in November 2000. It continued until the end of 2002. Eleven work areas common in 234 local governments had been developed and implemented during the period. They include family registration, disasters management, water and sewage, roads and transportation, livestock, management of civil defense, regional development, fishery, forestry, culture and sports, and management of internal administration. Along with the eleven new service areas, the interface system between the city/district and the provincial/central governments had been also developed and implemented during the second phase of the project.

The amount of the expenditure for the project reached 78 billion won (U$ 60 million) in the first phase and 80.8 billion won (U$ 62.1 million) in the second phase. While approximately 55% of the total cost had been invested by the central government, the remaining portion of expenditure was supported by local governments.

4) Outcomes and benefits

A network of 234 local governments was formed with the final accomplishment of the LGIN project at the end of 2002. In the meantime each local government was able to deal with internal administrations electronically producing clear, speedy, and precise processing of public services to conveniently deliver them to the customers. It is no longer necessary in some cases to go to the local office to take care of government services such as the issuance of verification documents. These affairs can be handled at home, in the office, or on the street. For example, some documents frequently requested by the private as well as public sectors for the purposes of verification are now immediately available at the kiosks installed in places convenient to citizens. Those documents include a certificate of resident registration and transcript of land register.

The documents are also available at home over the Internet. However, at the beginning of the service, there were not so many documents which were fully online over the Internet. An application for some verification certificates was processed electronically over the Internet, while it still had to be received by post or picked up at the nearest local office. Efforts to overcome limitations have been completed when those documents became available through home printers. Some documents including the land registry and the Certificate of Citizenship have been available through home printers since early October 2003. The process involves special techniques, for the prevention of forging documents as well as updating the law on the effectiveness of documents printed out at home and private offices.

Address change used to be required for several documents each time residences were changed. This time-consuming procedure is no longer necessary once the address change report is completed at the local office. This is because the change can now be registered simultaneously through the network on more than ten relevant registers, such as those related to ownership of vehicles and lands, and welfare. Public service applicants no longer face the problem that sometimes arises due to the omission and inaccurate entry of data. In addition, information and data of individual local governments are shared with each other, reducing the number of documents to process public services. For instance, it is no longer necessary to submit a certificate of local tax payment when we apply for a business permit, since the office responsible for the permit is allowed online to take a look at whether local tax has been paid.

The simplification of workflow in the process of the LGIN project has eliminated the overlapped procedures and management jobs involved in producing public services. Public officials are now relieved from the large amounts of manual paperwork that were previously required reducing the time it takes to process civil applications. The enhanced efficiency of public administration will lead to an improved public service environment as well as an increased trust in the government administration. The realization of the LGIN enables government policies to be planned and implemented on the basis of equal standards and procedures regardless of the location and characteristics of city/districts.

The LGIN project also put the Online Procedures Enhancement system (referred to as OPEN system) for civil applications. This system plays a significant role in the e-government initiatives from the standpoint of transparent procedures to reduce the possibility of corruption and irregularities. Initially developed by the Seoul Metropolitan Government as one of the anti-corruption programs, the OPEN system makes public the whole process of civil affairs administration from acceptance to the final processes by stage on the Internet.

The date and time are electronically reported in the system for the public when each application is processed. This being the case no official can delay or unduly interfere in any case or make any improper decision. Since the system allows universal access on the Internet, applicants do not have the burden of contacting officials or to offer bribes just to complete business. This way, the system significantly reduces the probability of any corruption and irregularities. Any citizen can access the OPEN system and see the contents of civil applications. The system enhances the effectiveness of internal monitoring and the online inspection by the audit department.

5) Towards more advanced local IT systems

As mentioned the LGIN system went through the major renovation in 2005, reflecting the technology advancement and the request of the users who filed complaints to the legacy system. The renovated system had been renamed as Saeol, meaning that the system supports to produce ‘innovative and trustful’ public administrations at the level of city/district governments. The Saeol system enables the public officials in the local governments to carry out their businesses in the more integrated way by utilizing the single window for public administrations. The system further delivers process-based electronic business integrations, thus leading into efficiency and transparency in managing the city/district governments.

The LGIN system is an information infrastructure that supports all areas of public service. It involves not only local governments but also metropolitan, provincial, and central governments. Various kinds of applications for enhancing customer services can be developed by these organizations by utilizing the information resources the LGIN offers. Therefore, the LGIN will be a root system of other applications. The new system will soon provide a higher level of public service by adopting state-of-the-art information technologies. Mobile services are available in limited application areas. The concept of a ubiquitous government will also be driven by the LGIN with an emphasis on ‘Anytime’ and ‘Anywhere.’

6) Difficulties and success factors

At the beginning of the project implementation, the Korean government faced resistance from some of the city/district governments, largely those belonging to Seoul metropolitan government. Since they had already deeply involved in developing the IT applications in various work areas, they were not willing to be part of the centrally developed system. Without the participation of those local governments in Seoul, however, the LGIN would not have yielded enough benefits in terms of CBP and interoperability of work flows across city/district governments. The trouble had been overcome:

– by the leadership of the ministry of the Korean government in charge of local government administrations;

– by the budgetary incentives provided by the informatization fund;

– by the Seoul government officials who had been recognized of the critical importance of the LGIN based on the CBP issues, and so on.

As the most IT application projects did, the LGIN also had come across the issue of how to fund the large investment required to develop the applications for 21 work areas and to implement them in 234 city/district governments. While the pilot projects had been paid by the informatization fund, the resources for each of the two stage projects had been mobilized by the central and local governments in appropriately- charged proportion. The proportion had been arranged not only by the rules prepared by the national budget office, but by the policy debate taking place among the members of the Special Committee for e-government.

Since the LGIN system was supposed to significantly transform the way the local officials handle their daily businesses, they were reluctant to accept the new and unfamiliar system. In addition, they sometimes feel the fear that their jobs might be taken away by the system. In order to reduce this type of psychological burdens, the project developed training programs for the local government officials to get accustomed to the new system, along with the job shifting opportunities for those who might have to be at risk of layoffs.

Since the LGIN project required a large scale investment for the whole of 234 city/district governments, the possible failure of the project could bring about an unimaginable amount of loss. Therefore, it was decided to follow the two stage process of implementation preceded by the pilot program. In the pilot program, five city/district governments had been selected to implement the project in 10 work areas in advance. Errors and inconveniences had been detected in the course of developing and implementing the system in the selected local governments.

The political environments during the time of project implementation made major contributions to the success of the LGIN project. Leaders in the political arena as well as in the central and local government recognized the significance of the IT applications in the public management and strongly supported the project by financing and providing favourable coordination in enacting and updating the laws and regulations required for the LGIN system to take effect.

7) Lessons learned for the developing countries

The LGIN system is necessary for e-government applications of the central government to take full effects, since various public services arranged at the central level are supposed to be distributed via the corresponding channels of local governments.

The success factors for the project identified above line up as lessons learned from our experience of project implementation. The LGIN system was able to achieve the current level of success by responding effectively to the issues summarized as follows:

– how to settle down the dispute on the project among the organizations at stake;

– how to finance the project and distribute the cost among local and central governments;

– how to deal with the psychological burdens for those who accept the new technical system and their potential fear over job insecurity;

– how to avoid a big loss from potential failure due to the complicated implementation processes and large scale of nation-wide project;

– how to obtain the support from the political and governmental leadership in order to get favourable conditions for financing and revising relevant laws and regulations, and so on.

The issues raised above had been settled down in the course of project implementation as discussed previously.

Case 3: e- Government Activities in Bangladesh (Bangladesh)

1) Introduction to e-Government in Bangladesh

Bangladesh, ranked among the most densely populated countries on the globe, remained one of the lowest in south Asia as far as teledensity is concern. Traditionally only a relatively small proportion of the population has had access to any telecom facility. Even 10 years ago, teledensity was below 1%, but the era of mobile telephony changed the scenario and Bangladesh currently enjoys over 46% teledensity.

The overall situation in Bangladesh has been improved to some extent by a rapidly expanding mobile market. Use of Information & Communication Technology (ICT) in government activities has become a common phenomenon in recent years. In the late 1990s, ICT introduced a unique concept--electronic government (e-government)--in the field of public administration.

To date, various technologies have been applied to support the unique characteristics of e-government, including electronic data interchange, interactive voice response, voice mail, email, web service delivery, virtual reality, and key public infrastructure.

2) e-Governance

E-governance is another area deserving attention. Electronic governance is using information technology by the public sectors to provide service and information, and encouraging citizens to participate democratically in the decision-making process by making government more transparent and accountable. A good official web portal and information depository needs to be developed to provide citizens with all necessary information from different government ministries.

All sorts of forms and application should be available for download by the public; also, to reduce bureaucratic complication, online submission can be added. For gaining transparency and reducing corruption, tender bidding, tax filing and plot allotment can also be made through this web portal.

3) Technologies and policies

We have issued Broadband Wireless License to three organizations; two operators are launched WiMAX. We hope that WiMAX can play a very crucial role in bridging the digital divide in Bangladesh. With the intent to enhance connectivity, we are now emphasizing on the establishment of infrastructures to connect the unconnected. Importance is being given on laying more optical fibre to reach the marginal people of the country.

In this regard, we have issued Nationwide Telecommunication Transmission Network (NTTN) license, to private companies. They are installing the telecommunication infrastructure countrywide. The licensee organization will establish fibre connection in order to facilitate the proliferation of broadband internet throughout Bangladesh. Apart from domestic connectivity, we are also thinking of boosting international connectivity.

We are in the process of examining the feasibility of availing terrestrial connectivity along with second submarine cable. We have formulated a 'National Broadband Policy' with a vision to build a people-centered, development-oriented Information Society, where everyone would be able to access, utilize and share information and knowledge easily and efficiently. Continuous encouragement to new and emerging technologies is a must for flourishing of ICT sector in the context of any country.

So, we look forward to promote newer technologies and concepts such as 3G, Next Generation Network (NGN), Long Term Evolution (LTE) etc. Web technologies also facilitate government links with citizens (for both services and political activities), other governmental agencies, and businesses. Government websites can serve as both a communication and public relations tool for the general public.

4) Applications

These far-reaching developments in e-government have encouraged governments around the world to establish an on-line presence by publishing statistical information on the Internet. Countries, irrespective of their developing characteristics, are constantly striving to improve the efficiency and effectiveness of e-government delivery services. They hope that e-government will emerge as a magical antidote to combat corruption, red tape, bureaucratic inefficiency and ineffectiveness, nepotism, cronyism, lack of accountability, and transparency.

All types of business including small, medium sized or big should incorporate ICT through e-business and e-commerce. Our products and services should be promoted in the global market with appropriate ICT technology-oriented marketing strategies. For the business community, inter-bank money transfer and transaction, loan system, L/C, finance, shipping, supply chain and credit can be done electronically to provide a suitable and friendly environment for the business to compete with other nations.

A dedicated corporate network line can be built to motivate the business community in ICT use. The newly installed Chittagong automation system can be a good example of how with less bureaucracy and quickly, goods could be released, providing more comfort to the business environment. Online stock trading system would involve more traders from different communities to participate in capital market.

The legal and the health system also play a significant role in all areas of the community. A knowledge-based online digital legal system consisting of case, records, law and policies is important for the judicial system. The lawyers should have enough resources available to defend their clients as well as the judges to make decision fairly. Without the access of these materials justice will be hard to achieve for the poor people.

Digitization of the judiciary system will also strengthen the democratic process of the country. Even though the private health sector has developed their management system, the public sector is way behind. A good patient-doctor management system on all public hospitals will improve the health services in remote areas. New technologies like telemedicine currently in use as pilot projects can be used more broadly for providing consultation for special cases on isolated localities. Like the judiciary, a similar knowledge depositary system for the doctors and nurses will improve the function of the health sector.

5) Conclusion

Digital Bangladesh is a continuous process of development. A sustainable and reliable nation-wide network infrastructure will strengthen the information highway of the country thus eliminating the digital divide between rural and urban areas. Decentralization and digital government services can be provided for all citizens.

Case 4: Overview on ICT-based Services in Bangladesh

1) Introduction to e-Government in Bangladesh

This contribution provides a comprehensive overview of the trends and developments in the telecommunications and digital media markets in Bangladesh. Subjects covered include:

– Key Statistics;

– Market and Industry Overviews and Analyses;

– Regulatory Environment and Development;

– Major Telecom Players (fixed and mobile);

– Infrastructure;

– Broadcasting (including Digital Media);

– Mobile Voice and Data Market;

– Internet, including VoIP and IPTV;

– Broadband (fixed and mobile);

– Scenario Forecasts (fixed-line, mobile and broadband subscribers) for 2015 and 2020.

Bangladesh, ranked among the most densely populated countries on the globe, remained one of the lowest in south Asia as far as teledensity is concern. Traditionally only a relatively small proportion of the population has had access to any telecom facility. Information communication technologies (ICTs) have appreciably taken the most important parts in each sphere of our daily life in the last decades. It includes from travel industry to all over health industries, banking, shopping, business communication, social communication, and communication between individual and governmental activities. “The e-service is a computer-based tool that can be used for 1) simply tasks and 2) make tasks possible to conduct. To simplify tasks means that tasks can be performed faster with less effort” (Cronholm, 2010). There are both e-services for e-commerce and e-services for e-government supporting private and public sector.

To date, various technologies have been applied to support the unique characteristics of e-government, including electronic data interchange, interactive voice response, voice mail, email, web service delivery, virtual reality, and key public infrastructure.

2) Analysis of e-Government development

E-governance is another area deserving attention. Electronic governance is using information technology by the public sectors to provide service and information, and encouraging citizens to participate democratically in the decision-making process by making government more transparent and accountable. A good official web portal and information depository needs to be developed to provide citizens with all necessary information from different government ministries. All sorts of forms and application should be available for download by the public; also, to reduce bureaucratic complication, online submission can be added. For gaining transparency and reducing corruption, tender bidding, tax filing and plot allotment can also be made through this web portal. However, we should understand that when we are talking about m-government we mean only one of ways of e-communication with government and it has sense only if e-government system exists.

There are four primary delivery models of e-government which usually take place:

– Government-to-Government (G2G)

– Government-to-Business (G2B)

– Government-to-Employees (G2E)

– Government-to-Citizens (G2C)

Mobile handsets (m-government) seem to be useful mainly in G2C model.

– Bangladesh's mobile market passed 80 million subscribers by the middle of 2011 as penetration neared 50%.

– This had been preceded by a significant five-year period in which the country saw mobile subscriber numbers grew almost 20 times.

– Of the six mobile operators, GrameenPhone was far and away the leader, claiming close to 35 million subscribers, or 44% of the total mobile subscriber base, as at mid-2011, despite the best commercial efforts of its competitors.

– Airtel Bangladesh became the fastest growing mobile operator in the country, its subscriber base-lifting 51% in the 12 months to August 2011; in the previous year Orascom had been the fastest mover.

– Internet penetration remains low (0.4% user penetration coming into 2011) and Internet subscription rates are considerably lower.

– Although broadband internet remains almost non-existent in Bangladesh, following the granting of a number of WiMAX licences, there were early signs that the market was about to change as the new WiMAX services were rolled out and started to attract customers.

– The fixed-line market experienced a major setback in the first half of 2010 when the regulator shut down five operators; the action had been taken as part of a major move against illegal VoIP services.

The number of fixed services decreased dramatically almost halving in a short period of time. The problem remained unresolved for 16 months; by August 2011 it appeared that a solution was at hand. But the market was going to take a long time to recover.

Table 3: Bangladesh: Key telecom parameters (2010-2012)

Category	2010	2011 (e)	2012
Fixed-line services[1]			
Total No. of subscribers	1.00 million	1.25 million	94.714 million
Annual growth	-40%	25%	
Fixed-line penetration (population)	0.6%	0.7%	0.74%
Fixed-line penetration (household)	3.0%	3.5%	
Internet			
Total No. of subscribers	280,000	330,000	2,94,15,693
Annual growth	17%	18%	19%
Internet subscriber penetration (population)	0.2%	0.2%	19.287%
Internet subscriber penetration (household)	0.9%	1.0%	
Mobile services			
Total No. of subscribers	68.6 million	85.0 million	94.714 million
Annual growth	31%	24%	10.73% (Up to July)
Mobile penetration (population)	46%	56%	62.10%

There are 6 satellite earth stations. Talimabad, Betbunia are two of them. Some info shows that the number is now 7. Bangladesh will send her first ever satellite Bangabandhu-1 into space in 2015.

Bangladesh is connected to SEA-ME-WE 4 or South-East Asia – Middle East – Western Europe 4. The landing site of the Bangladesh branch is located at Cox's Bazaar. Bangladesh is also a member of the proposed SEA-ME-WE-5, which will provide another submarine cable and connectivity for the country when its submarine cable is implemented within a couple of years. The company, BSCCL is the only submarine cable operator in Bangladesh.

Mobile Phone Subscribers in Bangladesh

The total number of Mobile Phone subscribers has reached 94.714 million at the end of July 2012 (Table 4).

Table 4: Mobile Phone subscribers in Bangladesh (July 2012)

Operators	Subscribers (in millions)
Robi	19.652
Banglalink	25.622
Citycell	1.685
GP	39.556
Teletalk	1.391
Airtel	6.806
Total	**94.714**

PSTN Phone Subscribers in Bangladesh

Phone Subscribers has reached **1141.603 thousand** at the end of July **2012** (Table 5).

Table 5: PSTN phone subscribers in Bangladesh (July 2012)

BTCL	**977,000**
Telebarta Ltd.	**56,424**
Jalalabad Telecom Ltd.	**10,900**
Onetel Communication Ltd.	**39,576**
Westec Ltd.	**17,000**
Sheba Phone Ltd. (ISL)	**1,081**
Banglaphone	**5,450**
SA Telecom	**18,033**
RANKS TELECOM LTD	**16,139**
Total	**1,141,603**

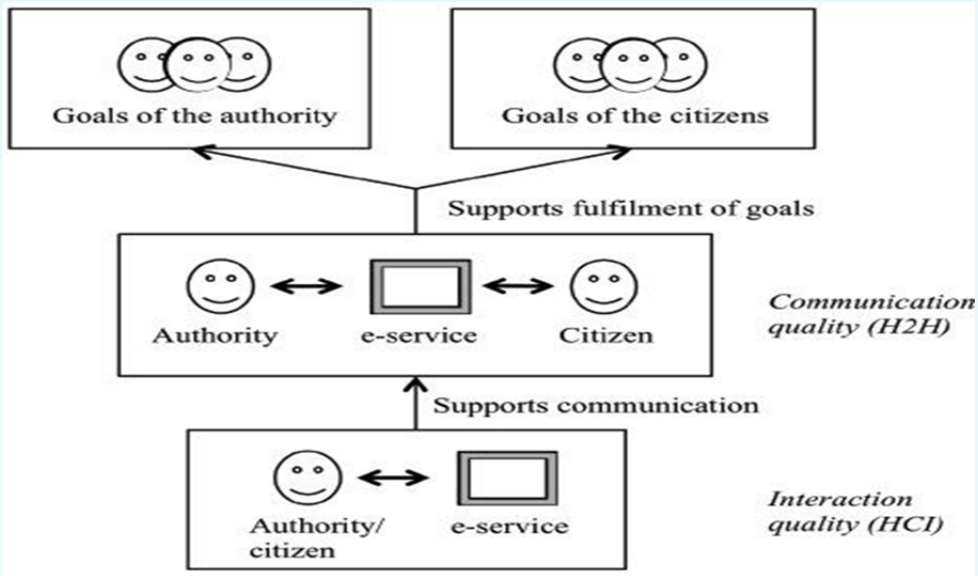
Operators at service

- IP Telephony Service Providers
- International Terrestrial Cables System Operators
- Vehicle Tracking Service Operators
- Nationwide Telecommunication Transmission Network Service Provider
- WBA Service Provider Licenses
- International Gateway Service Providers

– Interconnection Exchange Service Providers
– International Internet Gateway Service Providers
– Mobile Phone Operators
– PSTN Operators
– VSAT Providers with HUB, Providers and Users
– Internet Service Provides

3) Evaluation of Public e-Service

Communication criteria for evaluation of public e-service (Cronholm 2010)



4) Applications

These far-reaching developments in e-government have encouraged governments around the world to establish an on-line presence by publishing statistical information on the Internet. Countries, irrespective of their developing characteristics, are constantly striving to improve the efficiency and effectiveness of e-government delivery services. They hope that e-government will emerge as a magical antidote to combat corruption, red tape, bureaucratic inefficiency and ineffectiveness, nepotism, cronyism, lack of accountability, and transparency. All types of business including small, medium sized or big should incorporate ICT through e-business and e-commerce. Our products and services should be promoted in the global market with appropriate ICT technology-oriented marketing strategies. For the business community, inter-bank money transfer and transaction, loan system, L/C, finance, shipping, supply chain and credit can be done electronically to provide a suitable and friendly environment for the business to compete with other nations. A dedicated corporate network line can be built to motivate the business community in ICT use. The newly installed Chittagong automation system can be a good example of how with less bureaucracy and quickly, goods could be released, providing more comfort to the business environment. Online stock trading system would involve more traders from different communities to participate in capital market.

The legal and the health system also play a significant role in all areas of the community. A knowledge-based online digital legal system consisting of case, records, law and policies is important for the judicial system. The lawyers should have enough resources available to defend their clients as well as the judges to make decision fairly. Without the access of these materials justice will be hard to achieve for the poor people. Digitization of the judiciary system will also strengthen the democratic process of the country. Even though the private health sector has developed their management system, the public sector is way behind. A good patient-doctor management system on all public hospitals will improve the health services in remote areas. New technologies like telemedicine currently in use as pilot projects can be used more broadly for providing consultation for special cases on isolated localities. Like the judiciary, a similar knowledge depositary system for the doctors and nurses will improve the function of the health sector.

5) Conclusion

Bangladesh is a part of global village. The environment of this global village is changing, shaping and altering at internet speed. To stay competitive in the global market, it has become imperative for Bangladesh to keep pace with this speed by implementing e-government. In Bangladesh, e-government is just evolving, but the ball has been set rolling for an internet revolution. E-government is no longer a luxury but a reality. Now, it is estimated that more than 300 ISP‟s (Internet service Provider) are working in our country and there are near about 2,94,15,693 internet users (fixed and mobile) in the country. So, there is a vast chance for the expansion of e-government in Bangladesh. With 45.3% functional literacy rate (BANBEIS, 2010) and majority of the population based in rural areas, the people of Bangladesh predominantly rely on traditional and relatively low-tech ICT options to have access to information. The size of user base for public AM radio and terrestrial TV in Bangladesh is comparable to its South Asian neighbours (except Nepal, which enjoys an exceptionally high radio listenership rate).

Digital Bangladesh is a continuous process of development. A sustainable and reliable nation-wide network infrastructure will strengthen the information highway of the country thus eliminating the digital divide between rural and urban areas. Decentralization and digital government services can be provided for all citizens.

Case 5: Korea Online e-Procurement System (KONEPS), (Republic of Korea)

1) Overview

KONEPS is a single window for public procurement which provides integrated information on public tender for businesses. It is also a single repository of vender data, providing the entire public organization (approximately 40,000 organizations) with information on registered vendors (approximately, 220,000 businesses). Central and local governments as well as state-owned enterprises can use it by logging on to KONEPS.

Its main target is at the interactions between governments and private sectors' businesses where there have been for long time inefficiencies and corruptions. Many countries around the world have regarded the innovation of the procuring activities as one of the most critical agendas in securing transparency of the society, enhancement of the competitiveness of government operation and performance. Furthermore the paper-based procurement process requires an abundance of document exchanges, wastes time due to personal visits to the government offices. There are also many organizations involved in the process of the initial procurement request to the final payment stage.

KONEPS processes the entire procurement businesses online, from tender notice, awarding, and contracting to payment. By connecting to the government information sharing facilities, KONEPS eliminated the need for submission of paper documents such as business registration certificates and tax payment certificates. It digitized more than 160 official document forms for electronic processing, including bid, contract, inspection request, and payment request. As KONEPS deals with the payment

process online, including delivery report, inspection and payment requests, it can effectively reduce the payment lead time. This is because each unit in charge of contracting, inspection, and payment, respectively puts individual tasks on the common system, thus streamlining the payment processes.

2) Objectives and strategies

Since the 1990s, e-procurement has been viewed as one of the most important agenda in the reform of the public sector. The KONEPS project was selected as one of new reform initiatives in January 2001 by the Government Innovation Committee to enhance efficiency and transparency of government procurement. Related government departments including the Ministry of Planning and Budget, Public Procurement Service (PPS) and those interested groups such as vendors, internet technology companies, and public enterprises got involved in the discussion on how to innovate the public procurement through IT applications. The discussion dealt with planning, setting directions of procurement process innovation for public institutions and how to reduce the cost of procurement.

There has been a decision that individual departments should not develop an electronic procurement system separately. Instead, it was proposed to develop a standard system to be implemented with customization. “Guideline on prevention of duplicate development” was announced in June 2001 to avoid budget waste. In driving the e-government projects, the revision of law and regulation is no less important than building system itself.

3) Implementation and Technologies

Targeting improving efficiency and transparency in the public procurement process, PPS implemented the Electronic Data Interchange (EDI) system in 1999, e-Bidding system in 2000, and e-Payment system in 2001. While the individually developed systems in the consecutive years yielded productive results in the targeted areas, the absence of an all-inclusive single window for public procurement still left the users with inconveniences.

A framework to put electronic procurement into action was established in January 2002. In February 2002, PPS decided on a plan and selected a main contractor based on the evaluation of technical skills and estimated expense proposed by several system integrators. It also set the direction of development through analysing procurement work process and collecting opinions of related agencies in the workshop. The system opened in September 2002, along with user training, revision of laws, and updating regulations.

In the case of electronic procurement system, the revision of law and regulation was not difficult because there has been a consensus on the direction of revision in the course of setting up a framework and the range of revision was not so wide.

The infrastructure technology of building KONEPS is composed of Public Key Infrastructure (PKI)-based electronic signature, document security technology, electronic data interchange standards, and building large-scale web service. These technologies enable mission critical e-business to be safe and stable. KONEPS operates on the highest level of security.

For network security, it is equipped with dual firewalls, intrusion detection system, and security solutions. Intranet is separated from extranet, the login access and program modification history is automatically managed and program modifications are monitored online by an independent third party entity. For maximum compatibility with other system, its establishment and operation should comply with the open standards. Adopting business registration number (used in taxation) as company ID number, administrative standard institution code (used in administration) as institution ID number is a few illustrations.

Previously each government agency has used an independent ID number, so to connect with the systems it was indispensable to use translation table for compatibility. Since the number of institutions using KONEPS is huge, and KONEPS needs to link with tens of other external systems, applying and complying with open standards is a precondition for successful system building.

4) Changes and outcomes

KONEPS electronically publishes tender information from all public institutions, thus functioning as a single window to public procurement. It also enables the sharing of bidder information, allowing bidders to participate in all public biddings with one-time registration through KONEPS. KONEPS is also linked to the government accounting system, allowing the procuring institutions to administer payment through the electronic fund transfer.

KONEPS also runs an Online Shopping Mall, providing the electronic catalogue of purchase-available products. PPS sets the unit price contract of each item with individual venders, so that public organizations can directly place orders for those products, followed by the electronic payment.

As an early trial of the mobile service, KONEPS launched the mobile system in 2004 based on PDAs, allowing to search for tender information and to submit bidding. PPS continued to develop the mobile procurement service through the mobile phones, and as smart phones get widely diffused, mobile services will become more popular in the procuring market.

KONEPS has dramatically enhanced the transparency of the public procurement process. Competitive bidding opportunities, as well as micro-purchases subject to private contracts are increasingly advertised online thanks to the convenience of e-bidding. As bid results are opened online in a real time basis, there is no room for public officials to make arbitrary decisions. KONEPS has also enhanced the efficiency of procurement administration.

In addition, KONEPS has stimulated the development of IT systems in the private sector as the awareness of informatization has been raised based on accumulated experience of online transactions with KONEPS. This has played a prominent role in narrowing the digital divide for 110,000 businesses, most of which are SMEs.

The United Nations Division for Public Administration and Development Management announced the Korean PPS as the winner of the United Nations Public Service Awards 2003. KONEPS has also received attention from international organizations including the World Bank and OECD for its effectiveness in improving transparency. The OECD indicated that, the use of this system has dramatically reduced direct contracts of placing bids and receiving payment and the procurement process has been disclosed to the public, thereby improving the transparency and the credibility of procurement practices.

A series of global recognition for KONEPS are summarized in Table 6.

Table 6: Global recognition for KONEPS

Awarding Organization	Award	Date
UN	UN Public Service Award UN Public Service Award was established in July 2000 to raise public awareness of the improvement thereof. PPS was the first-ever awardee in the Asia-Pacific region.	June 2003
OECD	Best Case for Effects on the Private Sector The OECD reported that Korea's e-Procurement contributed towards the dissemination of IT in the private sector, and reached the level of "no further action required"	April 2004

Table 6: Global recognition for KONEPS

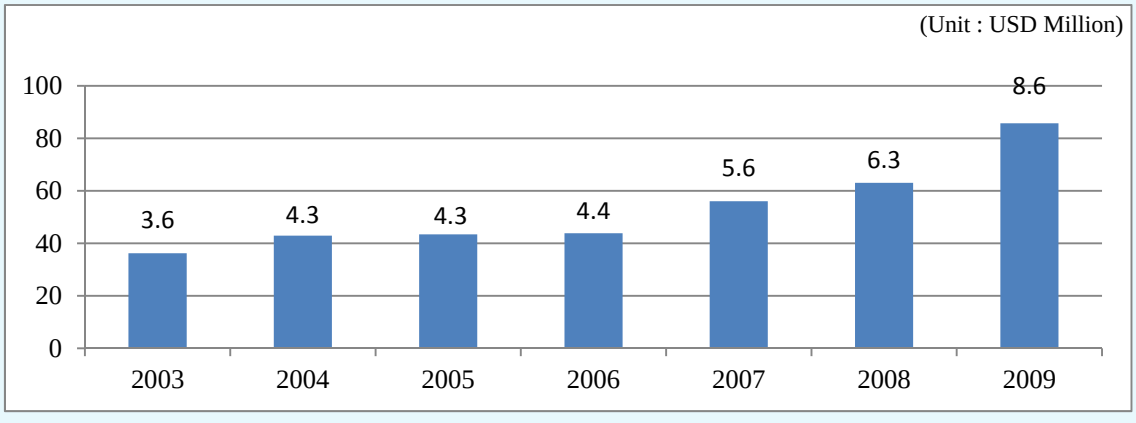
Awarding Organization	Award	Date
UN	Best Practice Model in e-Procurement KONEPS was selected as one of the best 23 practices in the world in the UN Global E-government Readiness Report 2004	November 2004
UN	KONEPS process reflected in UN/CEFACT standards KONEPS process was reflected in UN/CEFACT standards at the 6th UN/CEFACT Forum	March 2005
BSI	ITIL BS15000 Certification KONEPS received ITIL certification (BS15000) from British Standards Institution (BSI)	November 2005
WITSA	Global IT Excellence Award PPS was named as the public institution of best service innovation using information technology at WCIT	May 2006
AFACT	2007 eAsia Award KONEPS was named as a best practice model of e-Transaction in the public sector	August 2007

Source: 2009 Public Procurement Service the Republic of Korea "Annual Report"

There are many developing countries and international development banks that have expressed substantial interests in the public procurement innovations achieved by KONEPS. The Korean Government has actively involved in international cooperation project to share our experiences of successful implementation of KONEPS with countries such as Vietnam, Costa Rica, Mongolia, and Tunisia.

In 2009, the total transaction volume in KONEPS reached U$ 85.7 billion, while the number of public organizations and businesses registered in the system was 40 and 192 thousands respectively with a daily access count of over 186 thousands. The annual statistics of KONEPS transaction volume has shown in Figure 1.

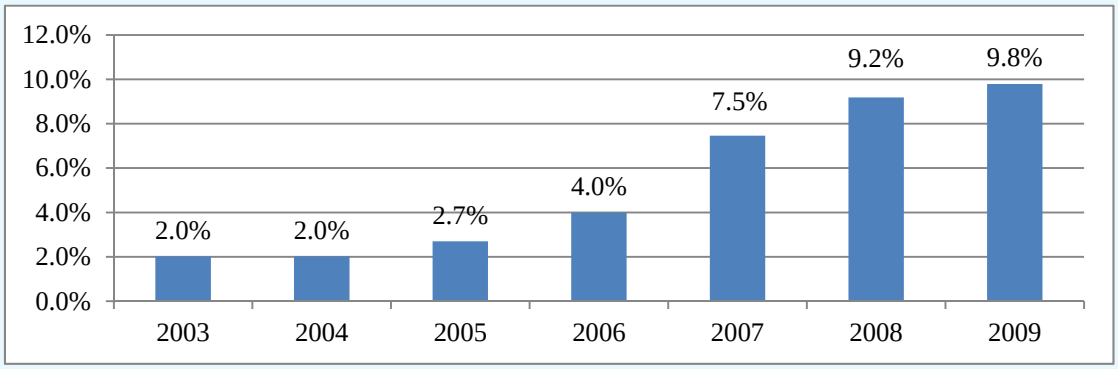
Figure 1: Transactions via KONEPS



Source: 2009 Public Procurement Service the Republic of Korea "Annual Report".

Since the establishment of KONEPS, PPS has promoted the use of electronic contracting among public institutions, the result of which has been sketched in Figure 2. In 2009, the ratio of e-contracting reached 97.9%.

Figure 2: Use ratio of e-Contracting



Source: 2009 Public Procurement Service the Republic of Korea "Annual Report".

5) Challenges and success factors

As was in the most e-government initiatives, it was difficult to promote coordination among agencies whose systems are supposed to be connected to KONEPS. The system has connected with 140 organizations including MOPAS (Ministry of Public Administration and Security), Financial Institutions, and various associations in order for the system to conduct its functions in a streamlining fashion with seamlessness.

Furthermore KONEPS has been connected to the National Fiscal System of central and local governments and the Digital Budget and Accounting System, so that the whole procuring process is streamlined from the stage of budget approval to the payment of contracts. Not all organizations were supportive to be included in a line with KONEPS since at the beginning they did not see any benefits of the connection from their viewpoints.

It is also difficult to understand and reflect user requirements into the system, since there are a huge number of institutions which get involved in using the system.

The common trouble, conflicts among organizations at stake, which we face in the process of implementing e-government system has been resolved by the coordination mechanism, such as the Special Committee for E-government, which was in effect during the years between 2001 and 2002, when the KONEPS had been established in the first place.

6) Next steps

There are several directions in consideration to get KONEPS shaped into the next generation. In order to develop the integrated form of procuring system, KONEPS has been reviewed from the three different viewpoints, that is, service, data, and technical architecture. First of all, the procuring service will be integrated to make sure the maximum benefits for the contractors.

For example, the current KONEPS has different structures depending on the type of tendering items such as commodities, facilities, and services. The structure of procuring processes will take the same format regardless of the type of items. In addition, KONEPS will be integrated with the work system for the PPS (Public Procuring Service), so that public officials in the PPS take full advantage of the e-government initiatives.

Secondly, data management will be integrated and realigned following the request of service users, leading to removing the duplicate and incompatibility. Currently the data is being individually administered depending on the type of service items, the work processes within the PPS structures.

Furthermore the data is stored according to different systems and operations in duplicate. This is the source of incompatibility of the same data across databases. We expect the realignment of data management will ensure the data integrity and compatibility.

Finally, based on the integration of procuring services and realignment of data resulting from the operation of KONEPS, its structure will be analysed and the system will be redesigned following the eGovFrame, a standard development framework for e-government. The framework is expected to enhance the stability and operational strength of the system.

Case 6: Uganda's road to e-Government (Uganda)

1) Background

The Government of Uganda has a strong belief that ICT has the potential not only to revolutionize the way Government operates, but to also enhance the relationship between government and citizens, government and business community and within government to government departments. Uganda's road to e-Government began with the ICT Policy of 2003 which mainly emphasized the need to build ICT infrastructure countrywide. Following the ICT policy, a national e-readiness survey was done in 2004. In 2005 an e-readiness was done specifically in Government.

2) Development of e-Government infrastructure

In 2006 with assistance from the Chinese Government, Uganda embarked on development of an e-government infrastructure countrywide. The first phase covered all central Government Ministries in Kampala and Entebbe and also covered towns of Bombo, Jinja and Mukono. The network provides the ministries with basic voice services, videoconferencing and data.

The services between the ministries are currently at no cost. Currently collaboration is being piloted between four ministries. This collaboration will see them operate on the same software platform. The second phase has covered the eastern, northern and western part of Uganda and will be operational by end of 2011. The private sector has also developed ICT infrastructure all over the country which can be used for e-Government.

3) Legal framework

Cyber laws have been put in place namely the Electronic Transactions Act, the Digital Signatures Act and the Computer Misuse Act. These are going to be implemented by end of the year.

4) e-Government framework

With the necessary infrastructure available, Uganda has developed an e-Government framework to guide in implementation of e-Government. The framework is guided by six principles namely:

a) Citizen-centric

b) Accessibility and choice

c) Trust, confidence and security

d) Better governance

e) Collaboration and integrity, and

f) Accountability

5) Public e-Government initiatives

a) All district Local Governments in the country have websites developed under the Rural Communication Development Program (RCDP). Public, investment and other business information opportunities are published on the websites despite the challenges of periodic updating and payment of web hosting and internet fees by the districts.

b) Government of Uganda web portal to act as a gateway to government services with linkages to the business sector is under development.

c) Establishment of pilot District Business Information Centers in six districts of Mityana, Iganga, Lira, Rukungiri, Kamwenge and Busia to enhance access to ICT services to the citizens are being set up by the Ministry of ICT in collaboration with UNIDO.

d) A National Data Centre to facilitate Government wide data storage, usage, sharing and security has been built.

e) A number of Government institutions have taken on computerization projects. Some of these include:

- Integrated Financial Management System (IFMS) by Ministry of Finance Planning and Economic Development (MoFPED);
- Integrated Resource Management System by Ministry of Defense;
- Local Governments Information Communication System (LoGICS) by Ministry of Local Government;
- Uganda Revenue Authority Countrywide Network (URANET) and Electronic Tax (e-Tax) by Uganda Revenue Authority;
- Electronic Funds Transfer System, Bank of Uganda/MoFPED;
- Community Information System (CIS) by National Planning Authority and Uganda Bureau of Statistics;
- Integrated Personnel Payroll System (IPPS) by Ministry of Public Service;
- Court Case Management System by the Judiciary;
- Land Information Management System by Ministry of Lands Housing and Urban Development
- e-Government Intercom (central government VOIP phones & Video Conferencing facilities) by Ministry of ICT
- Health Management Information System (HMIS)
- Education Management Information System (EMIS)
- Rural Information System to provide market information to farmers and other agriculture value chain stakeholders (Ministry of Trade, Tourism and Industry)

6) Private e-Government Initiatives

Most of the initiatives from the private sector are based on the mobile phone, considering that Uganda has a higher mobile phone penetration than computer/internet penetration. The initiatives include:

a) Payment of utility bills using mobile phones

b) Money transfers using mobile phones

c) Payment of school fees using mobile phones

d) Checking of commodity prices using mobile phones

e) E-banking and mobile banking

7) Future envisaged applications

a) e-Procurement

b) e-Document sharing in government

c) Electronic passport processing

d) e-Health and mobile health especially for rural areas

e) e-Education between urban and rural areas

8) Challenges

f) Cyber crime and cyber terrorism

g) Undefined cross-border jurisdiction for cyber litigation

h) Reliance on imported hardware and software

i) Reliance on foreign funding

j) Un-harmonised ICT Policies and Strategies

k) Inadequate Infrastructure

l) Adverse cultural beliefs and languages

m) Inadequate funding for ICT Projects

n) Inadequate human resources

o) Inadequate Public Private Partnerships (PPPs) frameworks

Case 7: Uganda's Approach to Implementing Broadband Connectivity in Underserved Areas (Uganda)

1) Introduction

Uganda Communications Commission (UCC) established the Rural Communications Development Fund (RCDF) to stimulate provision of telecommunications services in the rural and underserved areas. The RCDF is therefore acts as a mechanism for leveraging investments in communications infrastructure and services in rural underserved areas of the country.

This was recognition of the fact that although the sector had been liberalized and opened to competition some parts of the country which were non-commercially viable would not attract private capital for investment in infrastructure and services. The RCDF main objectives include to provide access to basic communication services within a reasonable distance; ensure effective investment in rural communications development and to promote ICT usage in Uganda.

2) Uganda's universal access policy framework

Uganda's Universal Access Policy (2010) is developed within the premise of the global development agenda, the Millennium Development Goals (MDGs), to which Uganda is one of the signatories; and its country-specific National Development Plan (2010) that was originally linked to the national vision called

Vision 2025. The policy is also developed building on the previous universal access policy (2001) and within the framework of Uganda's ICT policy and telecommunications policy.

a. Objective

One of the main reasons why the Internet has not spread to the rural areas are the cost of access, insufficient bandwidth and power issues and more important for the rural communities, illiteracy and the absence of relevant local content in vernacular. The new policy therefore has the main objective of ensuring provision of broadband connectivity and supporting the development of local content.

However, the main impediment for the ICT sector in Uganda today is the lack of broadband infrastructure network meant to accelerate access and use of the Internet in particular and ICTs in general. This is especially because of the heavy capital requirements that cannot be left to the private sector alone and thus requiring special intervention from government.

b. Broadband policy implementation

Uganda government has embarked on supporting the interconnection of all higher local governments' capitals and major towns with a national data backbone infrastructure so as to enable provision of wide array cost effective ICT services to the users. This expected to facilitate the establishment of institutional data access points with initial focus on vocational, tertiary and secondary educational institutions, and government health units for levels IV and III.

Broadband connectivity will be provided for selected sub-counties to connect to the high speed National Backbone Infrastructure. The connection is considered as a 'last mile' solution for the sub-counties. To this end, a detailed study to determine the most cost effective technological solutions (wireless, cable) that could be implemented for each location is underway.

Additionally, the study will help in identifying the districts that will not be covered by the national backbone infrastructure. The backhaul links will then be deployed to link such sub-counties to the identified districts. The initial proposal is to outsource the design and implementation of the proposed access network to competent telecommunications service providers.

The project once implemented is intended at lowering the price of bandwidth paid by the consumers while providing high quality and a wide variety of broadband services. The project will also entail providing computers and capacity building or training programmes to the end users such as schools, health centres and local governments.

3) Expected benefits

a. E-government: The project will help in collecting information from lower local governments upwards to the central government. The information will be part and parcel of the national demographics and other socio-economic related statistics.

b. E-education: The project will facilitate e-learning and already this is gaining popularity in the country. For example major local universities are having satellite campuses in upcountry locations in which long distance and online education are now being offered.

c. E-health: The project will facilitate data and voice flow from the rural communities to the health centre onwards to the district hospitals and regional referral hospitals and finally to the national referral hospital. The reverse flow will happen. Additional traffic is expected between the Ministry of Health head office and the district offices and also between the ministry and the health centres.

4) Conclusions

Internet penetration, access and usage in Uganda, is still very low and is estimated at (5%) users of the total population. This is also largely confined to urban commercial centres owing to commercial

considerations by the private service providers. Although Uganda's previous policy had supported the installation of Internet points of presence in all the underserved districts, the internet bandwidth speeds and quality of service issues (outages) has been of major concern by the end users.

Therefore the new policy objective is expected improve broadband uptake in selected underserved areas. This is envisaged offer lessons and experiences for developing a national broadband policy and subsequent rollout strategies for the country. Therefore, ITU-D Study Group meetings offer Uganda an opportunity to gain experiences on how other countries are addressing this developmental concern

Case 8: e-Government implementation in the Kyrgyz Republic-Experience and Further Steps

1) Country overview

With a human development index ranking of 126 out of 187, the Kyrgyz Republic is in the lower half of the medium human development countries. It raises seventeen places in the inequality-adjusted human development index. The country is 66 of 146 countries in UNDP's gender inequality index. The country's 2010 MDG report indicates that the country is unlikely to meet the MDGs for child and maternal mortality, tuberculosis, sanitation, and gender equality, although it is on track on extreme poverty reduction, access to basic secondary education, and access to improved water sources.

Since its independence in 1991, Kyrgyzstan has seen periods of democratic progress and of authoritarian backlash. With the fleeing of two presidents (in 2005 and 2010) after popular uprisings against authoritarianism, corruption and human rights violations; coupled with regional disparities and the repercussions of the inter-ethnic violence of June 2010, the country is going through a difficult process of transformation. In June 2010 several serious inter-ethnic confrontations took place in the south of the country. About 420 people died and 2,000 were injured, while over 2,000 houses and 300 businesses were destroyed.

As result of June 2010 referendum a new constitution has been adopted. The new Constitution defines the Kyrgyz Republic as a parliamentary republic (during the previous 18 years, the country was a presidential republic) thus making it the only country with a parliamentary system in Central Asia. Parliamentary elections held in October 2010 were contested by 29 parties, with five winning places in Parliament and three forming a new coalition Government. Presidential elections held in October 2011 resulted in peaceful transfer of power. However, peace and social cohesion cannot be taken for granted, as the root causes of conflict, including inter-ethnic mistrust and regional tensions, eroded credibility of state institutions, social exclusion and uneven access to economic opportunities remain to be addressed.

Kyrgyzstan in the past has seen concentration of powers around the presidency, with state institutions not perceived to be efficient, transparent or accountable. There is still work to be done to support the Government to strengthen the rule of law, address justice issues, reduce the prevalence of human rights violations, improve redress mechanisms and increase the independence and capacity of the judiciary, media (both public service and independent), the civil service and local government. Civil society's impact on decision-making still remains limited although its role has recently increased.

Kyrgyzstan has a GDP per capita of US$2200 (2010) and is classified as one of two low-income countries in the Europe and CIS region. The economy grew 3.9% per annum in 2000-2005 and 3.7% in 2005-2010. In 2011 the economy grew 5.7%. Poverty fell from over 62% in 2000 to 32% in 2009, but after the 2010 events it rose back to 33.7% that year, with an increasing proportion of the poor being female. Foreign debt is $2.803 billion as 2011, about 47% of GDP, while the budget deficit for 2012 is planned to be about 5.7% of GDP. There is a large informal sector, particularly in services and agriculture. Meanwhile, 26% of households have at least one member working abroad. Remittances had risen to US$1.7billion by 2011, slightly over 30% of GDP.

Life expectancy is 73.5 years for women compared to 65.3 years for men, and female literacy is high 97.7% (in the 15-24 age group). But despite progressive legislation on gender issues, women remain vulnerable to rising unemployment, a weak social protection system, and increased influence of patriarchal traditions in social relationships. Gender inequality, social and financial discrimination, and the additional unpaid work carried out by women mean that nearly 70% of the poor are now female.

About 32% of Kyrgyzstan's population is between 15 and 25 years of age. Young people do not have full access to education, employment, health care, family decision making, and entrepreneurship. With inadequate educational training and poor economic prospects, many young people turn to crime and drugs. Young women, especially in rural areas, are particularly vulnerable to gender-based violence.

The country has prepared a medium-term Country Development Strategy (2012-2014) in the context of a macroeconomic outlook that looks challenging, but with potential for directing the economy on sustainable development. The Strategy focuses on creating conditions for attracting foreign investment, reform of state regulation aimed at eliminating bureaucratic barriers and expanding economic freedom of business entities, as well as on launch and implementation of 40 national projects in the medium-term. All these fundamental factors will be crucial for long-term sustainable human development and achievement of the MDGs.

2) Background of e-government initiatives

The Government of Kyrgyzstan is taking a very active position by pointing the very high importance of the Information and Communication Technologies (ICTs) as a tool for faster country development.

The mid-term Country Development Strategy (2012-2014) and special Government Programme "Stability and Life of Dignity" clearly indicates the urgent demand for the e-government introduction in the country for governance e-transformation that will be responding to the needs of the ordinary citizens. The e-government is also expected to facilitate combating corruption, transparency and accountability of the public administration and contribute to the significant economic growth through increase of the business and intellectual activities of the society and country's integration into the global economy.

Analysis of the situation and preparedness of the Kyrgyz Republic for implementation of E-Government and E-Services and the related evaluation of the concepts, strategy papers and national programmes shows the strong commitment of the Kyrgyz Government to move from conceptual to implementation phase in fast mode and further promoting electronic services introduction (E-Services). This commitment of the Government is also strongly in line with the UNDP initiative aimed to support the Government of Kyrgyz Republic to ensure efficient and quick transition process from e-government conceptual to the implementation level.

The comparative analysis of the country situation shows relative advantage for Kyrgyzstan in terms of Internet penetration, Internet usage, and existing legal framework. Kyrgyz Republic is having relatively good position within the electronic and Internet space due to the fast expanding private sector's demand for access to ICT to spur business growth and adequate information infrastructure. The business growth is due to FDI inflow and investment loans received from the international organizations and high intellectual potential of the citizenry (i.e. one out of eight adult Kyrgyz citizens has university degree and the overall country literacy rate is above 95%).

a. Analysis of the existing Governmental Information Systems and Databases

Nowadays, there is a satisfactory level of computerization within the public administration bodies of the Kyrgyz Republic and especially in the central government agencies. In most of the ministries that operate with huge information data there are special dedicated servers to host databases, e-mail systems, Internet access and other services or even departments responsible for data processing and management. Many ministries and government administrations are developing their own local networks and information systems with access to Internet. As a result, there are many different types of information systems, databases, types of data, telecommunication infrastructure used, etc. that may block or hamper

the future opportunities for the inter-agency information exchange. Some of these systems are very old and are very difficult to maintain and develop further. Even within the institutions there are different types of technologies and data types that are making the future integration even more complicated. That is why the process of integration of state computer data and systems is very timely and should not be further procrastinated.

b. Analysis of the existing situation on E-services and the actual needs

The situation analysis pertaining to the existing E-Services shows that Kyrgyzstan is still at the early stage of E-Services deployment with its sufficient capacity for wider development. Most of the public agencies at the moment have information pages that present static (sometimes obsolete) information without provision of any real electronic services. But some of the key ministries take active steps on the introducing of the e-services.

c. Overview of the legal framework

The legal framework related to the E-Government in the Kyrgyz Republic is quite sufficient and comprises 16 laws on ICTs. However, the additional laws need to be prepared and adopted in order to open the door for further implementation of electronic services and information exchange in the country (for example, Law on e-commerce, unify technical standards and requirements).

Within the framework of reforming of the public service delivery system in Kyrgyz Republic in 2011, the Government Office has been conducted substantial work on optimization of procedures of public service delivery and improving their quality and availability to citizens. Approximately 45 governmental agencies have been inventoried to optimize their public services, which were decreased from 20,000 to 386 state services. These services formed the list of public services which was adopted by the Government Decree. The draft law "On Public and Municipal Services" was developed to implement the principles of social state to guarantee the constitutional rights of citizens for quality and access to public and municipal service delivery, currently under consideration of the Parliament. By the end of this year the Government Office will develop typical quality standards and technical regulations for assessment of public services' provision. E-services standards will be developed during 2013-2014.

d. Analysis of the interoperability framework – Existing situation and needs

Currently the inter-agency data exchange is mainly based on bilateral agreements. For provision of the high level electronic services, it would be needed to store part of information (personal and/or related data) in one place that may be accessible and updated by all government agencies based on the principle of one-stop-shop approach. There are no standards for data exchange or concept for interoperability framework of the government and these gaps should be addressed as the first step for establishing the enabling environment for further development of E-Services. In 2011-2012, the Government Office has introduced the pilot inter-agency e-document flow system among the Prime Minister's Office, Ministry of Finance, Ministry of Transport and Communications and Ministry of Economic and Antimonopoly Policy with plans to extend this initiative in 2013 to remaining ministries and agencies.

3) Objectives and strategies

Kyrgyz Republic adopted in 2002 the National Strategy and Action Plan "ICT for Development for the Kyrgyz Republic" for 2002-2010. The assessment of this strategy's implementation in 2007 by UNDP has revealed that only 30% of results were achieved. The country requires further strategic vision on ICT for Development based on international standards and best practices from other countries.

There is an understanding in Kyrgyzstan that the work on E-Governance shall be based on the firm belief that effective governance is an important requirement for the achievement of national economic, social and environmental objectives.

Kyrgyzstan has already recognized the importance of providing access to modern technologies and services for all citizens and businesses. The E-Government and E-Services will provide the opportunities to

the state administration to use information technologies for providing better services to citizens, businesses, and other actors of the governance. As a result, the administrative environment in the country will be improved in several key directions:

– increased transparency about the decision-making processes that will result in less corruption;

– increased government accountability for the state policy and implementation of the national strategies and concrete programmes and practices;

– participatory process where the citizens will be given the opportunity to control and directly participate in the governance process using the means of the electronic media;

– new and better services, including reduced time delays and accelerated delivery of services and information of critical importance for the business sector and small and medium enterprises in particular;

– reduced administrative costs based on higher efficiency and effectiveness of the administrative processes.

UNDP's support to the Kyrgyz Republic is provided in line with the Country Programme Action Plan (CPAP) for 2012-2016, which envisages the UNDAF/CPD Outcome #3: "By 2016, national and local authorities apply rule of law and civic engagement principles in provision of services with active participation of civil society."

The Government of the Kyrgyz Republic jointly with UNDP KR initiating the new e-Government implementation project with the following components:

Component A: Coordination of the E-Government implementation process

In support of the above mentioned government priorities and goals in the E-Governance area, the Government Office jointly with UNDP KR will establish a Coordination Center for ICT (CCICT or E-Gov Center), as the main governmental body for coordination of ICT and implementation of the E-Government services. CCICT will provide logistical and conceptual support, as well as consultancy services for the implementation of the ICT and E-Government strategies. This will be done through coordination mechanisms that will be established and implemented by the Center. The Center will also provide assistance to governmental and non-governmental institutions to implement concrete projects and initiatives including the following:

– Coordination of donor and government support to E-Government projects in Kyrgyzstan;

– Organize and maintain an information database for ICT stakeholders, E-Governance key players and potential future supporters of the E-Governance process;

– Establishment and re-establishment of coordination mechanisms for Information Society and E-Governance in Kyrgyzstan;

– Promotion of the E-Governance potential in the administration and business sectors;

– Preparation of all necessary reports on E-Governance implementation status on E-Services and connectivity between central and local governance programmes;

– Develop a strategy and organizational chart for development of E-Government concept and its implementation within the selected pilot regions in the country;

– Research and development of the best technology for implementation of E-Services within the E-Government programmes based on innovative and cost-effective technologies – digital TV, mobile phones, Wi-Max, etc.

Component B: E-Government architecture and standardization

CCICT will provide support to the development of the:

– all the necessary laws for establishment of the proper legal system for E-Governance development;

– back-office inter-exchange gateway/s and mechanisms for interoperability between the government organizations;

– mechanisms for introduction of e-services and support for their implementation;

The state information systems will be linked to a governmental Portal or Gateway that will provide an Integrated Environment for secured data exchange and linkages between the systems with a Central State Archive for E-Documents information. All these will provide linkages to the electronic services that would be provided to the Kyrgyz citizens.

Based on the principles of the interoperability framework that will be developed to support the inter-agency data exchange within the government, the work will continue to support the application of the developed technical requirements and/or standards within the concrete work on different gateways or exchange points. They will link the state owned information databases and connect them with a Central Archive that will record and manage the information flow of electronic documents and other related data required for the E-Services.

Component C: Creation of the Population Register

The creation of the Population Register will become a core element of the comprehensive e-Government architecture, as a single and unique source of the data on Kyrgyz citizens that will be provided to other government agencies and serve as a basis for their databases. The state agency responsible for the creation and updating of the citizen's personal data in the Kyrgyz Republic is the State Registration Service. This state entity is responsible not only for passport's issuing, but also for primary registration services (ZAGS), issuing the certificates on birth, marriage, divorce, confirming the maternity and paternity rights, death, etc.

At present, the ZAGS departments are lacking automatization and are paper based. In order to create the proper Population Register it is very important firstly create the e-ZAGS system and e-archive of the primary citizen's documents. The system for issuing the national passports also needs to be upgraded with new software and hardware tools.

4) Activities implemented

a. The **Ministry of Finance** of the Kyrgyz Republic launched in 2012 the few e-initiatives on budget transparency (www.okmot.kg) , such as:

– "Transparent budget" (http://budget.okmot.kg) - an automatic system for providing data on revenues and expenditures of the central and local budgets. It is for the first time in the country's history the ordinary citizens and legal entities have free access to the detailed data on implementation of the state budget. The presented data consist of information detailed from the level of individual recipients to the government agencies and the regions. The data is updated on-line through the electronic interconnection with Central Treasure Data Base;

– State e-procurement (http://zakupki.okmot.kg) – an automatic system for state procurements, including on-line registration, bid participation and other related information and actions

– On-line economic mapping (http://map.okmot.kg) –an electronic map of the Kyrgyz Republic, visualizing all socio-economic data for each geographical location of the country;

b. The **National Statistics Committee** of the Kyrgyz Republic actively works on implementation of the e–statistic data collection, analysis. The agency has developed and approved its ICT corporate strategy up to 2020.

c. The **Tax Committee, Customs and Border Management** state agencies also actively apply in its work the e-tools (e-declaration, inter-agency electronic data interexchange, etc.).

d. The **Social Fund, The Mandatory Medical Insurance Fund**, the **Ministry of Health** and the **Ministry of Social Development** actively upgrade their sectoral information systems and Data bases for e-social services provision and data inter-exchange.

e. The **Ministry of Justice**, the **Ministry of Internal Affairs** initiating the introduction of e-document flow within the ministries and software tools for proper Human Resource Management systems.

f. The **Ministry of Foreign Affairs** is initiating the process of the introduction of an e-visa and e-document flow.

UNDP KR is also taking active steps towards concrete implementation of E-Government concept throughout the introduction of sectoral E-Services and electronic documents interoperability within the public administration in the country. UNDP within the framework of its assistance to the Government of the Kyrgyz Republic provides technical assistance and expertise on development of the special software tools for the government agencies. The some of the examples a listed below:

a. Local self-governance area

Automated information system of an electronic municipality (AiylOkmotu-AO) «AYIL» (2007-2012) is a unique information system, developed as one of the components of e-government at the municipal level, designed to improve local government efficiency and the interaction with government authorities at all levels. In addition, it aims to raise awareness among local people on activities of municipal authorities and state administration. The system was tested in 14 pilot rural municipalities and further implemented in 409 rural municipalities out of 459 throughout the country. The system is automated the key AO specialist's functions: 1) land resource administration, 2) land tax administration, 3) municipal property administration, 4) social passport registration, 5) local population's applications and requests, 6) household book, 7) local population registration, including children. The system has "client-server" architecture and provides functioning in the network mode, with authorized access to the system given by system administrator. The system interface supports two languages – Kyrgyz and Russian. In 2012, it is planned to introduce 2 new software modules: 1) on AO budget formation and 2) local population's medical card. The system also will be automatically interconnected to the main government agencies' information systems, such as Ministry of Finance, Ministry of Health, National Statistic Committee, Tax Committee, etc. for further electronic data inter-exchange.

Following AYIL's introduction, UNDP has launched as the next step of its intervention- the automated system of an electronic region- "E-region" (2010-2012) (www.e-region.kg). It is also a unique information system based on web-technologies, which allows the building of an electronic interaction on "vertical" hierarchy – from rural municipality to the district and further, to province level. System allows not only have the web portal of all involved actors, but also to communicate between them in easiest and quickest way. The information system "An Electronic Region" is designed to build infrastructure for province development programs, budgeting and development of management documents in all regions of the Republic by enabling:

– Automated entrance of reporting data (43 electronic forma were created and –development indicators.
– Maintenance of data base of donors and investors.
– Support of internet-portals in the regions.
– Arranged citizenry appeals to local self-governments and regional public administration bodies.

b. Support to election processes (2011-2012)

– Ushahidi platform (monitoring of 2011 Presidential elections violations) - http://map.inkg.info

Developed software platform with user generated content allows for the use of mobile phones to report and e-map incidents of violence via SMS (to short number 4414), e-mail or web. During the pre- and after

election period about 5000 SMS were received, 2917 from them were processed and data uploaded and mapped.

– Special software for the creation and maintenance of the Unified Voter Registration system of the Kyrgyz Republic (2011-2012) was developed in order to create actual Voter list of KR. The system is now maintained by the Central Election Commission of the Kyrgyz Republic.

c. Support to State Registration Service (SRS)

State searching information system for the registration of the Kyrgyz Republic's population -the special software developed in order to make all processes on getting the citizen's legal documents (passports, primary registration certificates on birth, marriage, divorce, death, etc.) in electronic format. In order to improve the quality of public services, the Government of KR jointly with SRS established in 2011-2012 50 public service centres in the post office's premises among the country.

5) Changes and outcomes achieved

All of the above outlines the advanced status of the Kyrgyz Republic as of the country, which is well prepared for smooth implementation of the more comprehensive E-Government project. However, despite of the above listed activities by government agencies, the growth pace remains to be slow in comparison with the international trends in E-Government developments. Moreover, Kyrgyzstan is continuously falling down in the global ratings on E-Government readiness. This is a clear sign that the country should take immediate active steps towards E-Government implementation process in order to keep the good positions within the World Information Society. UNDP's assistance to Kyrgyz Government is aimed to facilitate overall process of E-government by using the vast UNDP international experience and practices, as well as through promoting coordination and smooth transition from the existing administrative business models to the electronic exchange of information and E-Services.

6) Challenges and success factors

The main challenges in the area of ICT Development in Kyrgyzstan are the following:

– Insufficient Funding or Allocation of Financial Resources- if there are not sufficient financial resources to complete all the aspects of E-Government – organizational, coordination, technical, and legislative, then the final outcome will be risked;

– Inadequate Institutional Arrangements or Weak Governance - coordination and governance of the inter-institutional relations and collaborative processes is crucial for the success of the e-Government that aims for global governance electronic solutions;

– Unexpected regulations or failure of legislation to pass or progress in the legislative process - legislative framework is needed for successful implementation of the e-Government outputs and problems with this may stop the project deliveries;

– Latent resistance on the mid and low level of the state and municipal servants may effect to timely implementation of the processes;

– IT/ICT literacy among the state and municipal servants are still low- it may influence to the speed of the deployment of the e-services and e-back-office arrangements.

Success factors are the following:

– The President of the country, Prime-Minister and other Governmental top leaders have deep understanding of the benefits and necessity of the e-Government introduction and are officially committed to launching the implementation process;

– The need of introduction of ICT-infrastructure among the central ministries and municipalities revealed that they understand the requirement for improved integration of their information systems;

– The citizen's readiness to deploy the e-services is high taking into consideration the IT-literacy rate, mobile networks coverage (about 100%) and Internet penetration;

– Common understanding of the benefits of ICTs deployment is an effective tool for transparent and accountable public service delivery and uncorrupted ways of its providing.

– Strong initiatives in ICT field already implemented by the National Statistics Committee and Ministry of Finance.

7) Lessons learned and next steps

The practical experience of the introduction of the different sectoral e-service's projects revealed the need for the Government's leadership in promotion of ICTs for the country's development at the national level. Lack of coordination of efforts in this area can cause duplication of efforts and inefficient use of resources provided by donors and Government itself. Uncoordinated work among agencies leads to further difficulties in electronic inter-connection. The creation of an effective coordination body on ICT and establishment of the national electronic interoperability standards and unified integrated infrastructure for e-services are critical in successful e-government implementation in the Kyrgyz Republic.

Case 9: Effort to make accessing the administrative business system more convenient using mobile terminals by service cooperation in Japan

1) Introduction

This paper aims to provide information by explaining the "Project Promoting Cooperative Business Administration Systems (Verification of Ways of Improving User-Friendliness for Mobile Phones as Means of Access)" commissioned by the Ministry of Internal Affairs and communications (M.I.C.) in 2011, for the benefit of the participants of the e-government system.

Under this project, we examined technical specifications as well as verification of technologies, specification of issues in light of the institution and operation aspects, studying solutions, and diffusing study results from standards organizations, for the purpose of implementing the foundational mobile access system through which mobile phones can access online services.

2) Overview

"[T]he New Strategy in Information and Communications Technologies (IT) Roadmaps" (decided in June 2010, revised in August 2011 and in July 2012) made by The Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (director-general: prime minister) presents the following goals regarding programs to diversify methods to access administration service, concerning the renovation of the governmental portal, and to encourage people to access the governmental service; in 2011, deliberation, verification, and demonstration of method for the mobile access to administrative services with authentication from mobile phones; from 2012 to 2013, based on the demonstration, introduce, develop and promote services partially in testing areas based on the demonstration above, and gradual nationwide deployment; by 2020, realization of the highly convenient electric administration services, namely a 'one-stop service'.

Based on such program, MIC conducted the "Project Promoting Cooperative Business Administration Systems (Verification of Ways of Improving User-Friendliness for Mobile Phones as Means of Access)"

in 2011, based on a survey and research results from the "research and study of the diversification of means of access to electronic administrative services, etc. (research and study of technology for mobile phones to access electronic administrative services, etc.)" in 2009.

3) Objectives and strategy

Mobile terminals with NFC (near field communication) functions are going to be commercialized in 2012. They realize both offline and online enclosure into tamper-resistant devices, of service users' personal information, in the form of authentication information such as ID/passwords, points and coupons, and enable the information to be read. Utilizing these functions, the authentication of the users becomes more convenient when accessing e-governmental services through mobile terminals, and all indifferent to generations of citizens have easy and secure access administration services through mobile terminals.

The research by M.I.C. in 2009 examined the security of the following spaces for storing ID information issued for the users by the service providers as a means of mobile access to e-governmental services: 1) public IC card system, used by placing the public ID card issued by the government near the mobile phone, 2) public card system for mobile phones, used by inserting the eligible cards issued by the government into the mobile terminals, 3) public identification information system, used by writing down the information issued by the government into the mobile terminals, etc. Tamper resistant devices are assumed to be 1) full-sized IC cards for the public ID card system, 2) flash memory devices containing the IC chips for the public card system for mobile phones, 3) UICC (universal integrated circuit card) for the public identification card system.

Without the examination above, in order to store and use ID information or users information in tamper-resistant devices, it was necessary to develop and operate an application for mobile phones (hereinafter, mobile app) for each service provider. Also, users need to download and install separate mobile apps provided by service providers. In other words, both service providers and users face inconvenience when a tamper-resistant service is provided. For the purpose of creating an environment convenient for users and in which it is easy for the service providers to provide and operate, we examined technical specifications to realize the mobile access system.

4) Implementation

In order to resolve the difficulties, we studied a system that both the users and service providers could commonly utilize. In other words, we studied the technical specifications of a mobile access system consisting of servers for storage and reading safely instead of each service provider and a mobile app utilized commonly for every service to store and use ID information in tamper- resistant devices. Further, verification by experimentation with technical specifications, the specification of issues in light of the institution and operation, and solutions to the issues are studied. In other words, the four following issues are studied.

The graphical explanation of this project outline is attached as Annex A.

Issue A: Examination of technical specifications for a mobile access system realizing online storage and use of ID information.

Issue B: Based on the examination results of issue A, the construction of an experimental environment, inspection of operability and user-friendliness from the viewpoint of both service providers and users, and verification of technologies.

Issue C: Based on the examination and verification results of issues A and B, the specification of possible issues in institutional and operational aspects when actually introducing the system, and deliberation on measures to solve the problems.

Issue D: Diffusion of results of the examination and verification of issues A to C in cooperation with appropriate standardization bodies in the study of the above issues.

5) Outcomes

The outcomes achieved in response to such issues are below.

Issue A: Multiple service providers which perform writing and reading of ID information into and from tamper-resistant devices have established technical specifications for a mobile access system composed of a common app by integrating a mobile access server that securely sends and receives ID information with a browser. With respect to ID information, established technical specifications for handling are not only e-certificates but optional information, such as other members' IDs, ticket information, etc. with a common method. To be compatible with various access methods depending on service providers, established the technical specifications that permit a common method (common protocol /API) applicable to any of the public IC card system (IC card), public card system for mobile phones (flash memory type device) or Universal Integrated Circuit Card (UICC).

Issue B: Used a mobile access server and common app within mobile terminals examined in issue A, constructed a demonstrative environment assuming virtual service operated on them, conducted function evaluation, performance evaluation, and dialog evaluation. The function evaluation revealed that the system examined in issue A had sufficient functions. The performance evaluation achieved performance measurement of the operation of the system using two types of mobile terminals and confirmed that writing of ID information and point information in about 6 seconds was possible. The dialog evaluation consulted with service providers and users and confirmed the operability, effectiveness and usability of the mobile access system.

Issue C: Among services which require identification when accessing information with smartphones, and which are highly needed, chose the following applicable services: (1) support service for aged persons (nursing care), (2) computerization of administrative procedures (applying for a residence certificate, etc.), (3) computerization of tax payments, etc. Analysed impacts or the risks, based on the "Risk Evaluation of the online procedure and Electronic Signature and Authentication Guideline" (CIO liaison conference, August 31, 2010) with regard to security and the authentication level required in the application service. It is concluded that Level 4 for security and authentication is necessary. It is confirmed that the mobile access system satisfies Level 4 requirements. Extracted are issues in operational and institutional aspects of services when using smartphones, and revealed issues in operating the mobile access system.

Issue D: Established an Exploratory Committee consisting of leading companies in the related field, such as NTT DOCOMO, INC., KDDI Corporation, SOFTBANK MOBILE Corp., and e-Access Ltd., and an expert, Mr Satoru Tezuka (Tokyo University of Technology). The committee was held four times. The results of the examination and verification of issues A to C were discussed. In order to create guidelines, draft guidelines were input to ARIB MC Committee. Official guidelines will be published within this fiscal year.

Examples of the utilization image of mobile access systems are: (1) writing ID information for certificates to Android terminal-tamper resistant devices, (2) applying for a certificate with an Android terminal online, (3) holding an Android terminal over the ministerial kiosk terminal (multi copy machine) installed at convenience stores and administrative bodies to receive a printed certificate. Another example is (first, holding the user's Android terminal over the Android terminal of an administrative officer or healthcare personnel, then, after authentication, the user's information (history of diagnosis and prescription) is displayed on the Android terminal of the administrative officers or healthcare personnel.

In order to realize the services above, further verification tests for overcoming technical difficulties will be conducted.

6) Difficulties

The main topics for consideration in the future in light of the operation, institution, and technology are listed below.

– **Operation:** Examination of the way of identification and operational procedures when issuing ID information such as certification for identification to tamper-resistant devices for the case of using the system used by not smartphone subscriber.

– **Institution:** Compliance with the Digital Signature Act when using an e-certificate for identification. Modification of provisions of on the application method for existing enrolment procedure in the municipal bylaws of some cities.

– **Technology:** Scheme such as a mobile access system considering the way of exchanging ID information between a smartphone and outer terminal through local communication.

7) Lessons learned and follow-up

More and more people in developing countries are going to have mobile terminals, and in those countries, the number of smartphones users is also increasing. An assumed area for public services must also be necessary for developing countries. We hope this information is valuable for your participants.

Case 10: e-Government in Lebanon

1) Introduction and country overview

The e-Government Roadmap presented here is based on the strong engagement of our government to build up an e-Government portal in order to improve and facilitate the citizen access to Public Services and Public Information.

The vision for the e-government strategy that focuses on the attainment of the following strategic objectives: A government that is Citizen-centered (not bureaucracy-centered), Results-oriented, Market-based (actively promoting innovation), has Good Governance, ensures Economic Development and Social Inclusion.

The four e-Government strategy pillars

– e-Reform: Provides the ideal opportunity to re-engineer government processes to take advantage of technology and use ICT as the spearhead of the reform process.

– e-Citizen: Groups together all the services that the government currently provides to the citizens in Lebanon and which are candidates to be provided electronically.

– e-Business: Focuses on those government services that are of importance to the Lebanese business community and foreign investors. More efficient delivery of these services will assist in promoting private sector growth in Lebanon and results in national economic development.

– e-Community: There is wide consensus that ICT is central to participation in the emerging knowledge economy, hold enormous potential to accelerate economic growth, promote sustainable development and empowerment and reduce poverty.

– The different e-Government initiatives in different fields as Legal, ICT Infrastructure, Vertical Applications and different national standards and policies.

The E-Government Roadmap is defined as a set of macro activities and critical milestones in different perspectives as Legal, Administrative, Infrastructure, Business Processes Reengineering, Interoperability and E-Government Portal. This Roadmap will be supported by a capacity building plan allowing the Government Employees to be able to use effectively and efficiently all E-Government Projects.

The success of this plan depends on a single cross-government vision and an effective cross-government decision making.

2) Objectives and strategies

a. Objectives and vision for e-Government in Lebanon

The e-Government vision for Lebanon centres around the attainment of a number of strategic objectives based on citizen and business-centric approaches. These are made possible by the facilitating role of Information and Communication Technologies (ICT) and backed up by the required institutional and legal frameworks. These objectives can be summarized as follows:

– Dissemination of all public sector information that a citizen is entitled to access through a number of communication channels, the Internet, hotlines, government service centres and traditional paper based methods.

– Delivering of all public sector services for citizens electronically whether for their individual use or on behalf of an establishment, through any government office or through the Internet regardless of the geographical location of this office or the residence of the citizen. Enable citizens and business to communicate electronically with Government, including making and receiving payments but not neglecting traditional paper based methods for citizens who do not have easy access to electronic facilities.

– Re-engineering government processes to ease conducting business with the government, through simplifying processes, using ICT to facilitate more delegation of responsibilities away from central control, reducing the number of required approvals/signatures (and if signatures are necessary ensure that these are electronic – no paper involved).

– Reduction to a minimum of the information and supporting documents required of a citizen to fill out in a public sector formality, regardless of the means by which this formality is being submitted.

– Provision of single points of notification for citizens to use for informing the government of any change in personal or business information. From this point, all concerned government information systems will be updated accordingly.

– Realization of the main government procurement processes electronically based on a harmonized commercial coding scheme. This is to serve as the leading example for electronic commerce at the national level and hence is intended to foster its growth. Use of a standardized commercially available system across all government would speed up this process; consideration should be given to contracting a commercially available entity to provide a managed service.

– Attainment of an intra-government electronic communication facility (e.g. by establishing an Intra-Government Portal) for the exchange of information electronically (providing all public service employees with e-mail addresses, linking the Portal to Government Data Centers for downloading/backup of information, providing Group Software and sharing services and information; also serious consideration can be given to outsourcing Public/ Private/ Partnership to the private sector).

b. Strategies and underlying principles of e-Government

To attain the e-Government vision for Lebanon, the strategy to be followed needs to be supported by a number of underlying principles. These principles can be summarized as follows:

– The government will assure the enactment of the required institutional, regulatory and legal frameworks to enable business to be undertaken electronically – in the country and abroad - in an orderly and timely manner.

– The government will undertake necessary measures to realize a comprehensive communications network infrastructure throughout the administration and to gradually roll out compatible information systems that exhibit open standards and interfaces to the replicated data repositories or centres in partnership with the private ICT industry in Lebanon.

– To ensure the successful implementation of e-Government, the efficiency, effectiveness and modernization of related services will be taken into account. These include the postal system, the banking system, courier delivery services and the overall legal environment.

– The government will ensure the security, integrity and privacy of citizens and business data by implementing a legal framework with state-of-the-art security systems that are in line with accepted international best practice.

– All citizens will be given the opportunity to be part of the electronic or networked society notwithstanding their financial, social or educational conditions or geographical location.

– All public servants will be given, by the nature of their new job functions, an equal opportunity to be part of the electronic or networked society, whether for their provision of services to the citizen or for intra-government communication.

– The government, in partnership with the private sector, academia and non-government organizations (NGOs), will work aggressively on the proliferation of ICT literacy throughout the country, whether through continuous enhancement of the education curriculum or through provisioning of targeted awareness campaigns and training programs.

– Adoption of electronic commerce by the private sector will be promoted, with government taking a leading-by-example role through its e-Procurement initiative.

– The government will be actively involved in partnerships with the local ICT industry to promote economic development by taking an increasing role in the implementation of e-Government projects in line with international best practices in this regard and will constantly work to develop this industry as a national resource for all Lebanese.

The Strategy for the Reform and Development of Public Administration in Lebanon, which has been defined by OMSAR, is based on the following programs:

– The program of reinforcing governance, accountability and transparency.

– The program of building the capacity of the public administration.

– The program of creating mechanisms to manage change and exchange experiences and best practices.

– The program for the reform and development of the human resources management.

– The program of enhancing services efficiency and reinforcing the relation between the administration and citizens.

– The program of enhancing IT usage and creating an E-Government Portal.

– The Lebanese E-Government is concerned by two of those programs:

– The program of enhancing services efficiency and reinforcing the relation between the administration and citizens.

– The program of enhancing IT usage and creating an E-Government Portal.

c. E-Government scope

The scope of the e-government Implementation is based on the following main components:

Multi-Channel Portal Interoperability Gateway Integration with Government Entities Automation of Processes User: Citizen, Business or others Government Employees

– Development of a multi-channel e-Government Portal which could be used by internet users, e-Government call centres, one-stop-shops, future e-Government centres as municipalities, internet cafes and others. This portal should be designed to allow access to all users regardless of their age and their knowledge of new technologies.

– Setting up of an interoperability gateway which will allow the exchange of data between different Ministries and Administrations. This gateway should be designed with a centralized processes defining for each government transaction, which administrations are involved in this transaction and, for each involved administration, which data should be used as inputs and outputs and which data should be checked or provided.

– Definition of an integration methodology based on the readiness level of each administration and based on different technical standards and protocols. The integration will allow administrations to be "connected" to the interoperability gateway in order to provide e-services and contribute to other e-services from other entities.

– Automation of internal processes for each administration. This component is based on systematic BPR (Business Process Reengineering) for all internal processes allowing the achievement of each e-service.

3) Activities implemented

The Activities implemented are listed below:

a. Pilot Design, Specification and Detailing for four One Stop Shops in Public Administrations

June 2011 to October 2011

The objective of this project is to establish four One-Stop Shops (OSS) in four different Lebanese Ministries. This assignment includes the pilot design, specifications and detailing of those shops. The main role of the one stop shop in each ministry shall be to facilitate the processing of government transactions related to that ministry by reducing the overall transaction processing time and waiting time, while effectively utilizing the human resources at each ministry. This will eventually lead to overall citizen satisfaction and increased productivity in the public administrations.

b. Implementation of a One-Stop Shop at the Ministry of Tourism - Civil Infrastructure

April 2012 to July 2012

The One-Stop Shop project is an important project for the enhancement of public service delivery. The idea is to create a common model and follow a common procedure located at one place for government institutions to deal with a large number of citizens. It aims at improving the activities of the services dealing with the public by furnishing services in a single location. Transaction could then be tracked through the internet.

The project targets the internal organization of public services and favours the simplification of procedures, the use of the technology within the scope of the e-government portal and allows transparency and quality between the citizen and the public administration.

The civil works for this project have been completed

c. Government Data Center physical infrastructure – Portal

June 2012 to August 2012

The objective is to have a secure, a high-quality, rightly sized, high-available, efficient, reliable and operational data center ready to host the national Lebanese e-Government portal and the interoperability gateway.

The Data Center is expected to provide the following benefits:

– Resources are housed in a single location

– Optimal Management of resources

– Efficient Provisioning of applications

– Cost Reduction
– Ensuring guaranteed level of availability
– Standardization of computers and networking resources
– Sharing infrastructure services across all server platforms and storage systems and for all concerned stakeholders
– Setting common policies for all applications running in the data center room.
– Facilitating and streamlining maintenance operations

The overall project that is described in this document covers the supply, installation and integration of the various components for the physical infrastructure of the data center.

d. Phase I – Government Portal for Information, Forms, Tentative Payment and Pilot e-Services

December 2011 to present

OMSAR has decided to stage the implementation of the "e-government portal" services into multiple phases. This project (Phase I – Government Portal for Information, Forms, Tentative Payment and Pilot E-Services) is expected to develop a national portal as a single unified interface for all ministries, agencies, departments, boards and councils within the Lebanese government and public sector.

The primary purpose of this portal is to provide a gateway to the government of Lebanon and offer public services to the citizens, businesses, Diaspora, as well as international community.

This phase must provide a "Single-Window" or "One-Stop-Shop" model website portal that delivers comprehensive information, forms, procedures on all aspects and constituents of the government and present information and services in a standardized and efficient manner to improve communication and service delivery. This portal will be the beginning of a long-term strategy to move all government services online and to a full G2C solution.

The e-services include services from the Ministry of Agriculture, Ministry of Foreign Affairs and General Security.

e. Unique ID Number

A decision about the adoption of the identity card number as e unique ID number has been approved by the Council of Ministers.

This decision has been coordinated with different government entities as: Ministry of Interior, Ministry of Finance, Ministry of Public Health and Ministry of Labour.

4) Technologies and solutions deployed

The technical architecture relies on a set of integrated software solutions mainly open source technologies.

5) Lessons learned and next steps

The next step is to prepare different draft laws, decisions and technical projects that could be adopted by the Lebanese Government such as:

a. Project of Law – Electronic Transactions

This law is meant to address the following different elements:

– Banking Transactions
– Electronic Payments

– Electronic Contracts
– Electronic Transactions (E-Services)
– Electronic Signatures
– Internet Domains management
– Personal data protection

b. Draft Law – IT salaries scale law

This draft law integrates the following elements:

– Creation of IT units in each administration/organization, job descriptions, qualifications and related salaries scale

c. E-Transactions Law Adoption

This draft law integrates the coordination through PCM with committee: MOT, MOET, MOJ, ALSI and PCA.

d. Simplification of Procedures

This project includes the following activities:

– Review of legislation and corresponding procedures in view of their simplification, ease of control and predictable outcomes.
– Produce recommendations in terms of legislation, decisions to be taken, re-engineering of ICT processes.
– Develop a strategy and an action plan to streamline and simplify the existing business procedures, promoting the use of ICT.
– Develop a methodology, guidelines, manuals, templates and toolkits for business process re-engineering.

Implementation of the Action Plan

It will start beginning 2013 for four Ministries:

1) Public Health,
2) Tourism,
3) Social Affairs and
4) Industry

e. Reengineering of licenses at Ministry of Tourism

The implementation is on-going and expected to be complete by end of December 2012.

f. Framework Agreement for WMS/DMS/ Archiving for three years in order to:

The agreement with the awarded consultant of the selected product is to implement WMS/DMS/ Archiving across the Lebanese Government wherever there is an official request for a workflow/Document Management/Archive system. The expected starting date is June 2013.

g. The Assistance on Simplification of Administrative Procedure:

This project includes the Methodology, Guidelines, and templates for the simplification, the modelling and the automation of administrative procedures. The expected starting date is February 2013.

h. E-Government Interoperability Gateway – Government Service Bus

The Government Service Bus ― GSB will provide integration platform and access to shared government services, like shared data, security, payment services, and notification engine. Later phases of the GSB will provide advance services, like service orchestration, registry and e-Forms integration

Case 11: MWANA (Zambia)

1) Introduction

Information and communication has always been a very important part in human life. The role and influence of ICT in Zambia has rapidly increased due to social factors and vigorous advancement of ICT technologies. According to ZICTA survey on the ICT Usage, Zambia that has a population of 12 million; 7.8 million have access to mobile usage while 4 million have access to internet. The rise in community's evolving service demands and increased ICT usage has compelled both Government and Private sector to be more innovative and to heavily invest in the telecommunication backhaul.

Various telecommunications technologies such as optical fibre, wireless technologies, mobile hardware and electronic government applications, are being deployed, in order to make a fundamental improvement to ensure public safety and deliver services and to transform the way the government responds to citizen's needs and expectations.

It envisaged that the deployment and use of e-Governance services will transform citizen service, provide access to information to empower citizen, enable their participation in governance and will enhance citizen economic and social opportunities.

All e-Government Services will pass through one active portal, which will be an interface to bring together the services offered, by government and its agencies on this multi-tier architecture. The portal will be a seamless one-shop for a range of government services from a number of government departments.

Project Mwana is one of e-Government service that Ministry of Health has implemented with the help of the cooperating partners to improve early infant diagnostics services, post-natal follow up and care using mobile phones.

2) Country overview

Zambia has shown growth in attracting investment in the Information and Communication Technologies (ICT), Sector. The sector has recorded over 42 percent penetration rate growth compared to 0.02 per cent recorded 14 years ago. The ICT sector have continued to pour in since the country launched the policy in 2007 adding that the policy has created an environment for the growth of the sector. Mobile manufacturing company and various internet and mobile service providers are some of the investments that the country has attracted. The unfortunate scenario is that most of development are concentrated along the line of rail, leaving large areas in the rural and remote place unserviced or underserved.

In Zambia, large numbers of infants are infected with HIV either at delivery or when breastfeeding. If no interventions provided, most of these children who contract HIV from their mothers die before the age of two years. These deaths contribute to the high levels of national under-five mortality rate. The government made it mandatory to test every infant born and begin treatment within the first twelve weeks of life.

The challenge faced by the Ministry of Health in particular area was how to transmit infant diagnostics services results from the three (03) test centres (Laboratories) in the country to the respective remote places within the shortest possible time. The turn-around time under the courier systems available would take an average duration of forty-two (42) days to complete the process, a period too long for a mother wait without breastfeeding. This challenge led to the birth of Project Mwana in 2009.

3) Objectives and strategies

a. To strengthen early infant diagnosis with an aim both to increase the number of mothers receiving results and to reach mothers in a faster, more efficient manner using the SMS application (mHealth).

b. To improve the rate of postnatal follow-up, increasing the number of birth registrations for clinic and community births, while also raising the number of clinic visits for mothers through community-health worker tracing using the "RemindMi" application.

c. To enhance service delivery of government to its citizens.

d. To reduce bureaucracy, turn-around time in providing government services.

4) Activities implemented

a. Procurement of ICT Infrastructure (Servers and Connectivity) for the project.

b. Development of Project Mwana using RapidSMS, a free and open-source framework for building mobile application for dynamic data collection, logistics coordination and communication, leveraging the basic short message service mobile technology.

c. Piloted in the project 6 provinces across Zambia, servicing 31 clinics and the pilot evaluation showed that it had substantial positive health impacts.

d. Scaling the project nationally between 2011and 2015.

5) Technologies and solutions deployed

a. SMS technology - powerful innovation that in Zambia has reduced delays in receiving early infant diagnosis (EID) DBS HIV test results, improved communication among health care providers and community volunteers, and more important, encouraged patients to return to the clinic for their test results with greater confidence.

b. RapidSMS Technology - addresses Early Infant Diagnosis (EID) of HIV. SMS messages are used to send the HIV results from the labs where they are processed to clinic workers in facilities where the samples are collected. The results arrive on phones in smaller clinics and SMS printers in larger facilities. The system also tracks samples and provides real-time monitoring for the province and district officials.

c. RemindMI - RemindMi addresses Patient Tracing for post-natal care. SMS messages are sent to Community Based Agents who seek out caregivers and infants and ask them to return to the clinic for 6 day, 6 week and 6-month post-natal check-ups or special circumstances, such as results arriving at the facility.

6) Changes and outcomes achieved

Project Mwana RapidSMS pilot reduced delays in transmitting results from the HIV test laboratories to the rural health facilities via SMS message from the average of 42 days to an average of 4 days. To date, the project has been piloted in 31 predominantly rural districts of Zambia and has produced desired results, which has prompted the government to schedule a national scale up program.

7) Challenges and success factors

a. Challenges

– Ownership of the project prior to initiation, and coordination among the partners

– Sustainability of the project after scale up and when cooperating partners hands over the project

– Lack of investment in research and development in ICT
– Digital gap between the Urban and the rural areas
– Socio-economic disparities

b. Success Factors

– Leadership taken by government on the project
– Government beginning to fund the large component of the project

8) Lessons learned and next steps

a. Government leadership

– When undertaking a project in the government, Users should be involved from the beginning project. This step helps in understanding user requirements and processes involved to complete tasks.
– There is need to integrate the project into long-term planning.
– Integrate data into district reporting.

b. Locally sourcing

– Employ a permanent local software development team.
– Have a permanent project manager who can coordinate partners.
– Create government-led working groups.

c. Cost control

– Negotiate with telecom companies for scale, not pilots.
– Utilize the phones people have rather than purchasing and supporting a national phone system.
– Create district-level training teams.

d. Co-creation

– Make decisions based on identified needs of the end users.
– Create the tools with the people who are going to use them.
– Test early and often; don't worry about failing and stay adaptable.
– Use open source tools that can be customized to local needs

e. Next steps

A national scale-up plan has been developed, commencing with a preparation phase and then shifting to an iterative phase where clinics are trained and added to the system and the problems and successes of the additions are evaluated. The aim is to achieve national scale by 2015, with health facilities offering early infant diagnosis services. The preparation phase will focus on solidifying the technical, physical, monitoring and human infrastructure to allow the system to handle the stresses of scale. Throughout the scale-up process, the project will be closely monitored to ensure the systems are having a positive effect on the targeted health challenges.

Case 12: eGovernment Service in Montenegro

1) Introduction

There is more than one definition of eGovernment i.e. usage of Information – communication technologies in combination with organizational changes, and new know-hows, to increase cooperation with public, to increase democracy and involvement of public in decision making process.

This requires huge change in business processes of governments, both on national and local level and it tackles more than strategic vision and organizational sources. Huge efforts should be made, apart from using different technologies, to implement various solutions in public administration, which means a huge change in a way of thinking.

2) Country overview

Aware of the importance of development and application of ICT, Montenegro has made significant steps in this direction in the past. This is clearly recognized in the ranking of the World Economic Forum - the Network Readiness Index (ISM), where it is ranked in the 44th position out of 138 countries, far above other European countries in the region. With the penetration of mobile network users of nearly 200% and the penetration of internet users which is growing continuously, it is evident that the ICT sector in Montenegro is undergoing intensive growth. More information can be found in latest survey done by national statistics office.

3) Objectives and strategies

Amendments to the Strategy for Information Society Development (2009-2013).

Initially, we planned to make Amendments to the Strategy for Information Society Development 2009-2013. However, starting from the fact that in 2010 the EC adopted Digital Agenda for Europe, in order to comply with European requirements, the decision on creating a new document for the next five-year period was evaluated as more expedient.

In this context, in September we adopted the Draft Strategy for Information Society Development for the period 2012-2016 year, i.e. after the completion of the public hearing in December we also adopted the Proposal of Strategy for Information Society Development (2012-2016).

The Strategy for Information Society Development (2012-2016) relies on the five pillars of development associated with ten programmes with individual goals and objectives. For the purpose of complying with the Strategy projects in the Action Plan for the implementation of the Strategy are divided by areas:

ICT Sustainability - with the programmes: ICT basics (technological framework, a framework of the radio-frequency spectrum, a framework for consumer protection), ICT infrastructure, legal and regulatory framework, information security with the aim of improving broadband infrastructure, legal and regulatory framework designed to create competitive and sustainable ICT sector.

ICT for society - with the programs: e-education, e-health, e-inclusion, with the aim of encouraging all actors of society to use modern technology.

ICT in public administration - with the programme: e-government, which is focused on encouraging public administration to use information and communication technologies in an innovative manner to improve the quality of services provided by state authorities.

ICT for economic development - a program of R & D and innovation-ICT technologies in development of science and research in order to create a productive and sustainable ICT systems through the creation of a database of talent, encouragement of creativity and entrepreneurship.

Action plan for 2012 for implementation of the Strategy for Information Society Development 2012-2016 includes a total of 26 projects or activities, the implementation of which will, together with the implementation of obligations under the Government's Programme of work for the current year and the implementation of commitments and the Ministry's Programme of work contribute significantly to development of information society in Montenegro.

Analysis of eGovernment development

In Montenegro, the Ministry of Information Society predicted, in the Strategy of Development of Information Society for the period 2009-2013., the monitoring of degree of development of basic eGovernment services annually. The first survey was conducted in late 2009. Research concerning the measurements of eGovernment development is monitored and implemented over the network / the Internet, i.e. how many electronic services are already available to citizens and businesses. Along with all measurements of eGovernment, the existing websites are monitored and new sites, that will allow users to perform government services through a network or other communication channels, are searched. Research related to the assessment of the degree of development of 20 main e-government services, which are defined in the strategy documents both in EU countries and the countries of the region (and i2010 Plus eSEE Agenda) were conducted for the first time, internally, in late 2009. In order to clearly define in Montenegro the directions of further development of electronic services in public administration, according to all models, it is necessary to examine the current situation and according to that and following the trends in the region, to focus the development in the right direction.

EU cooperation

The Ministry of Information Society formally expressed interest in accession to the ICT Policy Support Programme - ICT PSP, which is part of the Competitiveness and Innovation Programme – CIP in October 2009 and Montenegro joined this programme in 2011.

Community ICT PSP programme, which operates under the CIP, aims to support innovation and competitiveness through the wider and better use of ICT services by citizens, governments and businesses, especially by small and medium-sized enterprises. This program is fully aligned with the priorities of the European i2010 strategy and is one of the main financial instruments for achievement of the goals of the i2010.

Within eSEE initiative Montenegro is a signatory to "eSEE Agenda" and "eSEE Agenda Plus", as well as to the Memorandum, between the countries of South East Europe on the development of a uniform broadband market related to European and global networks, and also has a representative in the Centre for eGovernance Development for South East Europe.

4) Technologies and solutions deployed

During the period since establishment of the Ministry, we have implemented a number of projects, but also we participated in number of projects that are implemented by other institutions. Below we gave an overview of some of the projects currently on-going or at latest stages.

eGovernment Portal

In order to implement the e-Government in Montenegro, Ministry for Information Society and telecommunications implement the project web portal eGovernment - www.euprava.me hereinafter referred to as: the portal, through which all institutions of public administration and local self-government units will provide services to individuals and corporate entities, and other institutions electronically.

The goal is that citizens and legal entities, meet their needs for certain information and documents do from anywhere, via the Internet and the Portal rather than over the counter. On the other hand, the portal is a platform and tools for government authorities to create electronic services, to handle requests more easily and communicate with the applicants of those requests electronically.

Under the Portal eParticipation citizens can actively participate in the creation of laws and other strategic documents, and they may express opinions and attitudes in the public debate. eParticipation is in full correlation with electronic democracy - eDemocracy and eGovernance.

The portal officially started to operate on 7th April 2011. and in cooperation with five state institutions, citizens and businesses were provided immediately with 12 e-services on the portal. Currently over 24 electronic services are provided over portals, within the jurisdiction of nine institutions.

The Ministry of Information Society and Telecommunications aims to involve as more authorities of state and local self-government units as possible, which will provide electronic services and information about them. Also, the goal is the motivation of citizens to use electronic services provided on the Portal to a greater extent.

Electronic Document Management System – eDMS

eDMS (Electronic Document Management System) is a project whose main goal is informatization and electronization of business office in the Government of Montenegro, in order to increase efficiency, save time, reduce costs and provide better quality management of documentation material. This project will create the conditions for the creation of a business solution that will ensure efficient operations in accordance with the legal documents that define this area of work, and it will cover the complete life cycle of all of the documents (since the emergence of registration, to digital archiving). The solution will provide the technological basis for improving business processes of Government and ministries and their integration into a unique information system that meets the highest standards in terms of flexibility, speed and security.

This system provides basis for future development of eGovernment. Also it is a basis for electronic Government session which started in 2010. Currently all government sessions are held electronically as well as councils and commissions.

5) Lessons learned and next steps

Future steps and efforts will be focused on Interoperability Framework, which by nature is not a technical document is intended for those who are involved in the definition, design and provision of public services.

Although the provision of public services, in almost all cases involves the exchange of data between information systems, interoperability is a broader concept and includes the possibility of organizing joint work on generally beneficial and commonly agreed goals.

Interoperability is a prerequisite and a facilitating factor for the efficient provision of public services, which meets the need of:

– Cooperation between public administration institutions;

– Exchange of information in order to fulfil legal conditions, or political obligations;

– Exchange and re-using of information to increase administrative efficiency and reduce administrative burdens on citizens and businesses;

and leads to:

– Better provision of public services to citizens and businesses on the principle of “one-stop shop” (one-stop government)

– Reducing costs for public administrations, businesses and citizens through the efficient and effective provision of public services.

Case 13: National Program of Accelerated Development of ICT Services in 2011-2015 (Belarus)

1) Introduction

[1] The Republic of Belarus is a landlocked country in Eastern Europe bordered by Russia to the northeast, Ukraine to the south, Poland to the west, and Lithuania and Latvia to the northwest. From the ITU perspective, Belarus represents the CIS region. According to ITU and UN reports on ICT infrastructure and e-government, Belarus occupies second place after Russia in CIS region on most indicators. Based on analysis it is evident that Belarus has well-developed ICT infrastructure, but still has much to do in implementing and promoting electronic services.

In order to get over these difficulties specialized Informatization Department was established under supervision of national telecom regulator. At present Informatization Department operates in scope of the National program of accelerated development of ICT services in 2011-2015. The National program was approved by the Council of Ministers on 28/03/2011.

2) Goal and objectives

The goal of the National program is to create conditions that promote faster ICT development, stimulate information society development on innovative basis and improve quality and effectiveness of G2C and G2B relationships, including creation of national e-services system.

Main objectives of the National program are:

– ICT infrastructure development with advance capabilities required to satisfy growing needs of citizens, business and state. Creation of environment for e-services implementation, development of e-government resources and providing universal access to such services;

– creation and development of state system of e-services;

– improving quality of health care services;

– improving quality of social and employment services;

– e-learning development and capacity building;

– e-commerce promotion in order to faster economic development;

– increasing government, business and civil society online presence;

– security systems development in order to provide safe ITC usage;

– providing appropriate conditions for IT-industry growth.

3) Subprograms

National program comprises 9 subprograms aimed to develop different aspects of information society:

1) ICT infrastructure development subprogram. Main ideas are broadband development in terms of speed and quality, implementation of IMS, LTE, PON, creating environment for new services.

2) E-government subprogram.

[1] See document: 2/INF/89-E.

3) E-health subprogram. Main ideas are improvement of health care quality and accessibility, increasing health tracking by citizens, telemedicine development, creating of specialized web-resources dedicated to health care and healthy living.

4) Electronic employment and social security subprogram. Main ideas are creation of unified information system for employment and social security purposes, provide complete implementation of digital signature in social security organizations, inform unemployment about employment and training possibilities through ICT.

5) E-learning and capacity building subprogram Main ideas are overall ICT training in schools, constant courses update in high schools and universities, creation of educational web-resources, academia integration into international education networks, creation of e-libraries, education for people with disabilities.

6) E-customs subprogram. Main ideas are development of national e-declaration system, development of customs information system in order to provide clear communication and data exchange with Russia and Kazakhstan as partners in Customs Union, improving quality and security of e-customs services.

7) National content subprogram. Main ideas are stimulating online presence of media, digitization of museum and library funds, rich accessibility of cultural information for foreigners.

8) Security and e-trust subprogram. Main ideas are creation of necessary legal acts, implementation of information security systems, creation of unified security monitoring system, development of typical security policies.

9) Export-oriented IT industry development. Main ideas are providing necessary support to IT companies, constant training for IT specialists, creating environment to attract investments in IT industry.

4) E-government subprogram

E-government subprogram aims on integrating development of specialized information systems and resources to provide e-government services for citizens and business. Long-term goal of this subprogram is to create integrated, user-friendly system to provide all possible e-government services with centralized access and with multi-channel delivery.

Subprogram includes almost 40 activities to be implemented till 2015. These activities cover all spheres of e-government and mostly directed to develop information systems, electronic registers, to make digital signature widespread, to make e-government services easily accessible and to develop monitoring systems to observe e-government implementation process. Each activity has responsible state authority as well as time frames and funding specified.

Subprogram uses the following KPIs to evaluate its progress:

– UN e-government readiness index;

– Percentage of organizations using digital signature;

– Percentage of organizations using Internet to perform information exchange with Government;

– Percentage of information systems, integrated into unified e-government system;

– Percentage of state authorities using outsourced professional services of information systems support and maintenance.

5) Challenges

– Informatization processes are still fragmented, and there is lack of proper coordination between state authorities;

– There are not enough e-services provided for citizens, services are decentralized. Exceptions are banks and cadastral agencies;

– Digital signature is not widely adopted and is not in demand. It needs to be improved;

– There is lack of process coordinator, who has enough experience and credentials to link involved authorities into singe productive team.

6) Lessons learned

– Changes should be overall, fearless but with prior active consulting with civil society and business;

– Changes must be implemented step by step. We should use positive experience from previous changes in future ones;

– Business likes changes and generally supports them;

– E-government implementation should be fully transparent and must be based on multi-stakeholder approach;

– Processes should be simplified prior to automation;

– Sometimes we should be able to implement changes one-sided instead of spending unlimited amount of time searching for mutual understanding.

Case 14: Creation of Government CIO (Chief Information Officer) (Iran, Islamic Republic of)

Introduction

[2] Creation of CIO is first goal to integrated planning, regulating and supporting of ICT projects & objects and CIO has come to be review in national level as the key contributor formulating strategic goals for the country. One of the reasons for not reaching the favourite outcome in Iran is: numerous institutions and decision makers, lack of unique authority, lack of necessary integration and Lack of supervision that the CIO structure can be help to manage the problem.

The Government CIO is a very important indicator in e-Government ranking. The CIO is expected to align management strategy with ICT investment in order to achieve harmonization between business strategy, organizational reform, and management reform; hence, the Government CIO is considered by many governments to be one of the key factors in the success of e-Government implementation as ICT leaders.

In this ranking, we split this indicator into four elements: firstly the presence of CIOs in government; secondly, the extent of their mandate; thirdly, the existence of organizations which fosters CIO development, and finally, the special development courses and the degree/quality which teaches CIO related curricula.

Most developing countries receive low score since there is no strong evidence on CIO mandate, CIO Presence as well as CIO development programs

[2] See document: 2/INF/91.

Country overview

A brief review of the situation in Iran about e-Government and E-government Development Index (EDGI):

Table 7: Waseda University Institute of e-Government rankings 2013

No	Final Rankings	Score
1	**Singapore**	**94.00**
2	**Finland**	**93.18**
3	**USA**	**93.12**
4	**Korea**	**92.29**
5	**UK**	**88.76**
6	**Japan**	**88.30**
7	**Sweden**	**87.80**
8	**Denmark**	**83.52**
8	**Taiwan**	**83.52**
10	**Netherlands**	**82.54**
11	**Australia**	**82.10**
12	Canada	81.78
13	Switzerland	81.33
14	Germany	80.08
15	Italy	79.11
16	New Zealand	77.29
17	Norway	75.53
18	Belgium	72.01
19	Estonia	71.76
20	France	69.49
20	Thailand	69.49
22	Portugal	69.11
23	Turkey	67.10
24	Malaysia	66.26
25	Hong Kong	66.12
26	Spain	65.89
27	China	65.69
28	Mexico	64.24
29	UAE	63.34
30	India	62.77
31	Brunei	60.89
32	Israel	60.25
33	Brazil	59.88
34	Russia	59.32
35	Macau	58.65
36	South Africa	57.77
37	Vietnam	55.42
38	Czech	55.06
39	Chile	54.87
40	Indonesia	53.05
41	Philippines	50.88
42	Romania	49.72
43	Argentina	49.23
44	Pakistan	47.25
45	Venezuela	47.20
46	Peru	46.56
47	Nigeria	45.20
48	Egypt	44.11
49	Kazakhstan	37.27
50	Georgia	34.98
51	Cambodia	33.52
52	Fuji	32.65
53	Tunisia	31.33
54	Iran	30.77
55	Uzbekistan	30.35

As per the e-Government Ranking 2013 shown in Table 1, Iran stands in the 54th place.

Unfortunately, in spite of having numerous experts and IT projects Iran could not have good rate in e-government ranking in the world. After many research about this, we concluded that the CIO structure definitely can be help us to solve our problem.

Technologies and solution deployed

Creation CIO will cause the integrated management strategy with investments in technology to achieve a balance between business strategy, organizational reform and administrative reform

That is useful to complete the CIO structure (controlling technology investments, etc.) at the national level for integration of e-government in implementation stronger master plan

Objectives and strategies

– Develop and implement information technology policy.

– Coordinate information technology investment strategy and capital planning.

– Develop and implement Enterprise Architecture.

– Implement Data Management program.

– Identify and oversee business process improvement opportunities.

– Develop and implement information technology performance measures.

– Oversee the Department's Reports Management Program, including the Information Collection Budget.

- Develop and implement electronic government in compliance
- Manage systems integration and design efficiency.
- Analyse information technology skills for all employees including executives, end-users, and IT professionals.
- Develop and execute IT Governance and Investment processes.
- Coordinate, develop, and implement IT Security computer policy and procedures.
- Manage information technology operations.

Annex 2: Toolkit to create the ICT-based services using the mobile communications for e-government services

Table of contents

0 Introduction

The Toolkit to create ICT-based services using mobile communications for e-government services, is an analysis of approaches for the creation of services based on mobile communication, such as e-government, e-health, e-learning, as well as mobile payments, mobile banking, authentication services and electronic signatures. The document reviews the ITU standards for security services based on mobile communications, shows achievements of a number of countries in the industry and provides guidance on the construction of such services. The Toolkit was launched by the Intervale (Russian Federation) and in addition to contributions from the Russian Federation, valuable input to the Toolkit was provided by the Ministry of Internal Affairs and Communications of Japan, the Bank-of-America and the Swedish company Accumulate. The Toolkit was analysed by ITU-T SG 17, and approved and supplemented by it complementary contributions. The approaches outlined in the Toolkit are in correlation with materials of the Mobey Forum, a non-profit organization specializing in development of mobile payment systems.

The authors are very happy to thank Ms Mayumi Yamauchi, Mr Abbie Barbir, Mr Lars Aase, Mr Vladimir Minkin, Mr Dmitry Kostrov, Mr Vladimir Soudovtsev, Mr Viacheslav Kostin, Mr Dmitry Markin and also Mr Hani Eskandar and Ms Christine Sund for their help and constructive recommendations.

The material in the Toolkit can be useful for developing countries building their secure e-government services based on mobile communications.

1 E-Government Delivery Models – Use of Mobile Terminals

While e-government is often considered as Internet web-based government, many non-Internet "electronic government" technologies can be used in this context, such as TV and radio-based delivery of government services, email, newsgroups, electronic mailing lists, online community facilities, chats and instant messaging technologies. Some non-Internet technologies also include telephone, fax and very important services based on wireless networks including SMS and MMS messaging. Mobile communication, beside its main purpose - voice communication and message transfer between users, has been found extremely useful for additional applications such as m-Commerce, m-Health and m-Government and so on, where “m” stands for “mobile”. However, one should understand that m-Government is only one of various means of electronic communication with the government and the same goes for m-Health, m-Education, m-Commerce and m-Payment.

In spite of the fact that mobile handsets have small displays and keyboards, they have a great deal of expectation to be used for e-government services. Today’s extremely fast evolution and important advantages of mobile communications made “e“ services, based on mobile terminals and named as “m“ services (*m-Government, m-Health, m-Payment, m-Learning and so on*), are very prospective, because:

– Not every citizen owns a personal computer, but usually almost everybody owns a mobile phone (According to the ITU report "Trends in Telecommunication Reform 2012", by the end of Y2011 there were 6 billion mobile subscribers and almost twice less Internet users all over the world);

– Mobile phones are always with their owners and always on-line;

– In some cases mobile communication may be the only available way of communication;

– Mobile communications are not less secure than the Internet.

Prospects for the use of mobile communication are so great, that in 2010 ITU’s fifth World Telecommunication Development Conference in Hyderabad has adopted the Resolution 72 "Increasing the efficiency of service mobile telecommunications". And at the World Telecom Conference 2012, held in October in Dubai, two new ITU initiatives on the use of mobile devices have been launched to provide ICT-based services:

– m-Powering Development

– m-Health for NCDs (jointly with WHO)

There are four primary delivery models of e-government which usually take place:

– Government-to-Government (G2G)

– Government-to-Business (G2B)

– Government-to-Employees (G2E)

– Government-to-Citizens (G2C)

– Obviously, G2C is the most widely used model and this model, in particular, can play an important role in world-wide spread of m-services.

2 G2C Activities

Government-to-Citizens is a delivery model, in which the government provides one-stop, on-line access to information and services for citizens. G2C applications enable citizens to ask questions to government agencies and receive answers; to file income taxes (federal, state, and local); to pay taxes (income, real estate); to renew driver's licences; to pay traffic tickets; to change their address information and to make appointments for vehicle emission and driving tests.

In addition, government may: provide information on WEB or WAP sites; provide downloadable forms online; conduct training (e.g., in California, drivers' education classes are offered online); help citizens to find employment; provide tourist and recreation information; provide health and safety advices; allow transfer of benefits like food coupons; file flood relief compensation (as it was after Hurricane Katrina aftermath in New Orleans, USA), and so on.

– Usually, four types of G2C activities take place: governance, e.g. online polling, voting, and campaigns.

– one-way communication, e.g. regulatory services, general holidays, public hearing schedules, issue briefs, notifications, etc.

– two-way communication between the Agency and the Citizen. In this model, users can engage in dialogue with agencies and post questions, comments, or requests to the Agency.

– financial transactions, e.g. payments, lodging tax returns, top-ups, fines.

No security required for the first and, probably, for the second types of activity. On the contrary, the third and the fourth types require strong user authentication and secure connection. In these cases when processing a service request, both parties, the Agency and the Citizen, should be authorised and data transfer should be executed in secure mode with the use of cryptography means. Below is the more closely study of these instances.

Two-way communication between the Agency and the Citizen

The Citizen may either seek an audience with the Agency or request information, for example, concerning his payments due, or to request such information in electronic form/paper form. The document requested electronically may be sent encrypted to Citizen's mobile device or to the Citizen's personal page on government's WEB site, access to which requires the submission of an electronic signature. If the document is requested in paper form, Citizen will be informed when the document will be ready and where it will be available.

Financial Transactions

The service of carrying out financial transactions should be universal. This will allow to process non-cash payments with state institutes, trading companies, service providers and between citizens, including cross-border payments, which means not only G2C, but also B2C and C2C transactions. Along with these services the option to initiate a payment by either party should be available. Sources of payment may be national or international bank cards, clients' bank accounts, and even personal accounts of mobile

network subscribers, or so-called “electronic money”. In this proposal Mobile Payment System (MPS) becomes a part of national Retail Payment System being under the government control. While processing cross-border transactions, it is important that national payment systems of various countries should be compatible with each other. That is impossible to fulfil without following common standards. ITU, as an international organisation and under aegis of UNO, should carry out coordination and standards settling.

One should note here that standardization is mandatory not only for financial transactions, but also for e-Health, e-Government and other similar services.

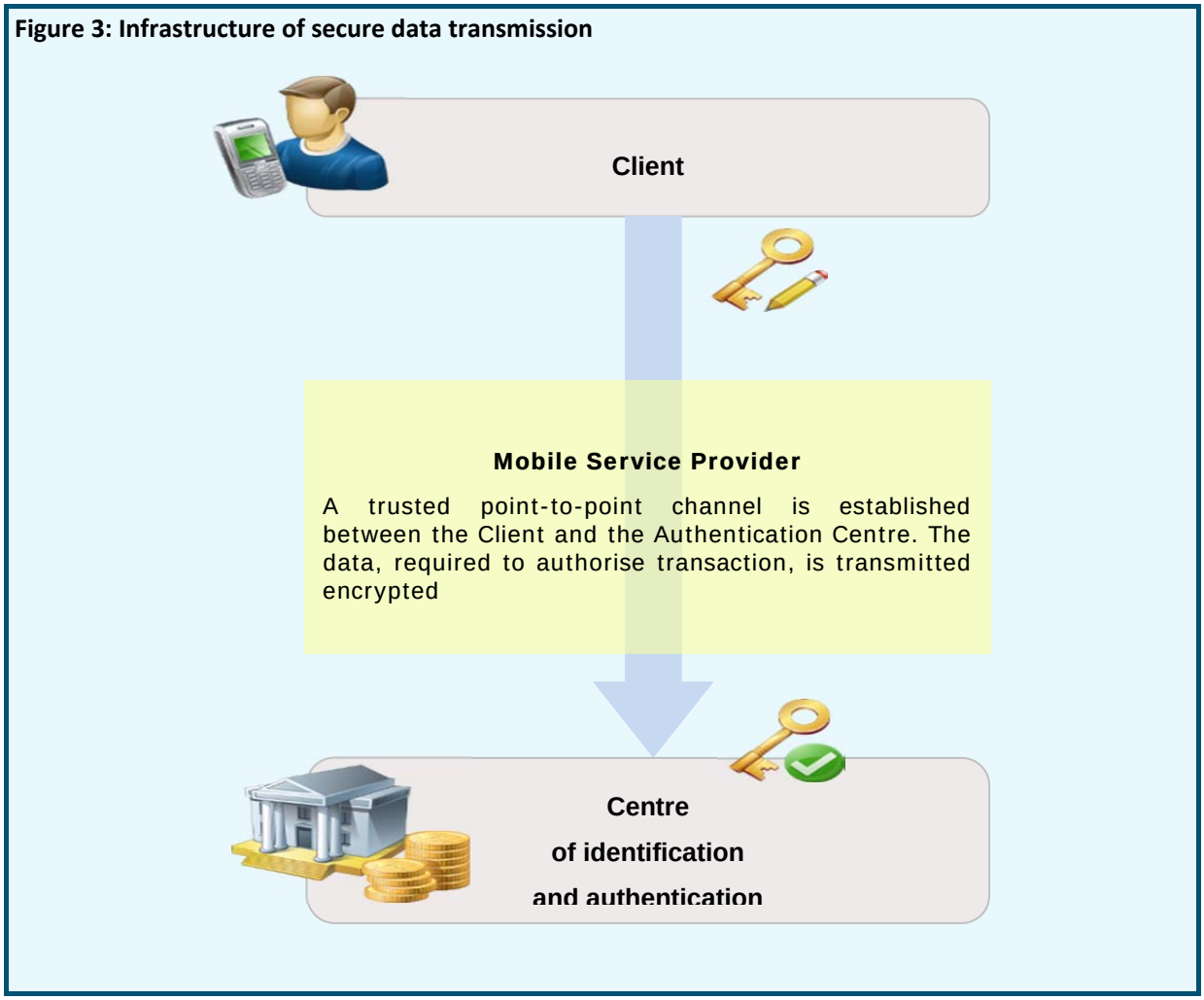
3 General Principles for Secure Mobile Services

Mobile system for providing secure remote services, whether it is mobile electronic government, mobile medicine or mobile commerce, in general should present an infrastructure with secure transmission of data blocks between mobile terminal users and service providers (Figure 3). To ensure the security, this structure must have an element that provides authentication and encryption. Transmitted blocks can contain confidential information requiring secured treatment. Data exchange should be carried out only between authorised users, not accessible to third parties and properly logged to avoid non-repudiation. User authentication shall be resulted from multi-factor authentication. In accordance with the ITU Recommendation Y.2740[1], which will be described below, means of authentication and encryption must meet the required service security level, determined by an agreement between the service provider and the Client, if it is not inconsistent with national legislation.

3.1 Identification and authentication

For identification purpose, it is required to validate Client’s identity and uniquely link Client mobile device to his account in the database of the service provider. After initial Client identification, he should be issued a "secret" that will authenticate the user during his future interactions with the service provider. This "secret", also known as “mobile signature”, appears as one of authentication factors. Practically, mobile signature is a unique cryptographic key, which may also be used to encrypt information. Thus, use of keys provides both data encryption and parties’ authentication. The second factor of multi-factor authentication can be specified by the user PIN or password, allowing access to applications installed on the handset. This PIN protects against unauthorized use of applications.

Figure 3: Infrastructure of secure data transmission



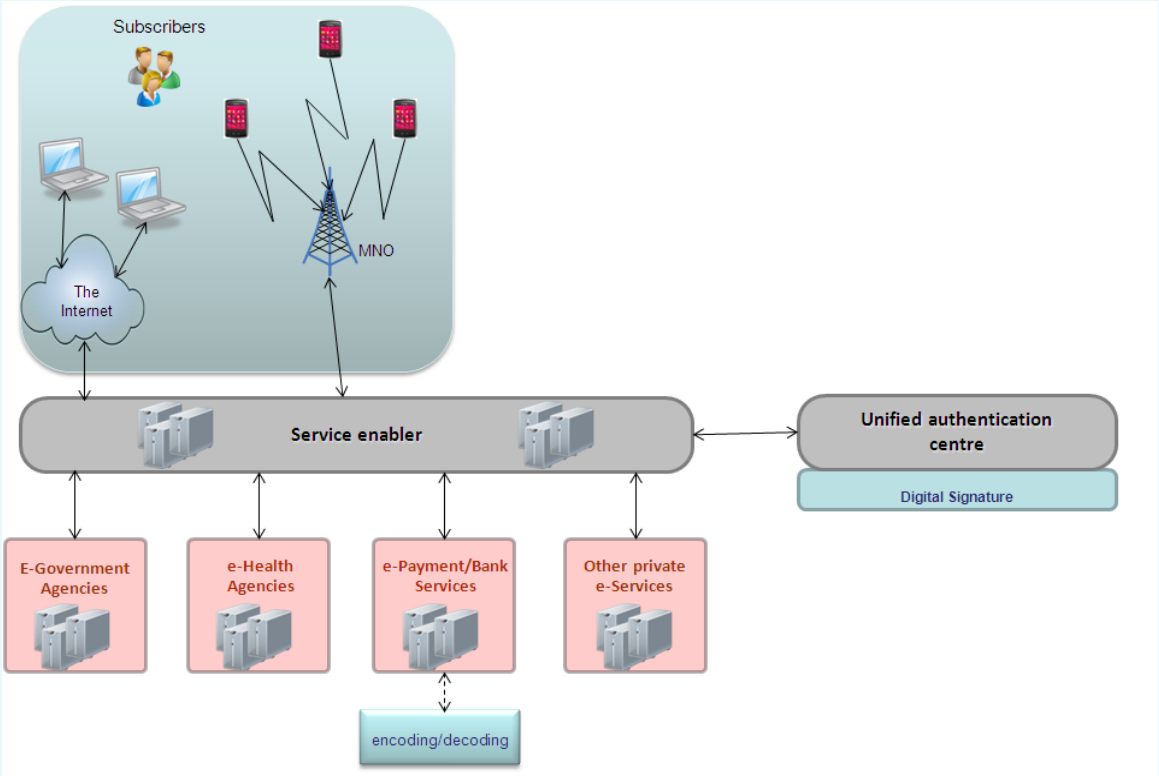
Existing mobile payment systems have already implemented their own security procedures, where security requirements are determined by agreements between service providers and their customers. Obviously, e-government requires a security system, controlled by the State and compliant with national law regulations concerning electronic signatures. The system should ensure secure transmission of confidential information between government agencies and authorised users, while providing electronic signatures. The same system can be used for e-health services and other newly created services that require data protection. And although private mobile payment systems will probably have their own means of protection, one shall not exclude complex solutions, which provide centralised authentication at a single centre, and some service providers (most likely, financial ones) additionally use their own encryption and verification procedures. Therefore, in mobile applications it appears reasonable to provide several independent blocks with different sets of keys. Figure 2 shows unified authentication model for mobile and Internet devices.

Despite the existence of multiple identification and authentication centres, all of them shall use unified rules to issue global customer mobile identities – mIDs, registered within the System Central Directory to ensure proper routeing of messages to Clients. The Client may have multiple mIDs, but they should be bound to the Client's MSISDN.

Service Enabler provides the technology support and plays a very important role in this structure. Beside integration of various access means, interoperability with service providers and authentication centre, Service Enabler also provides users with applications for access means (personal computers and mobile terminals).

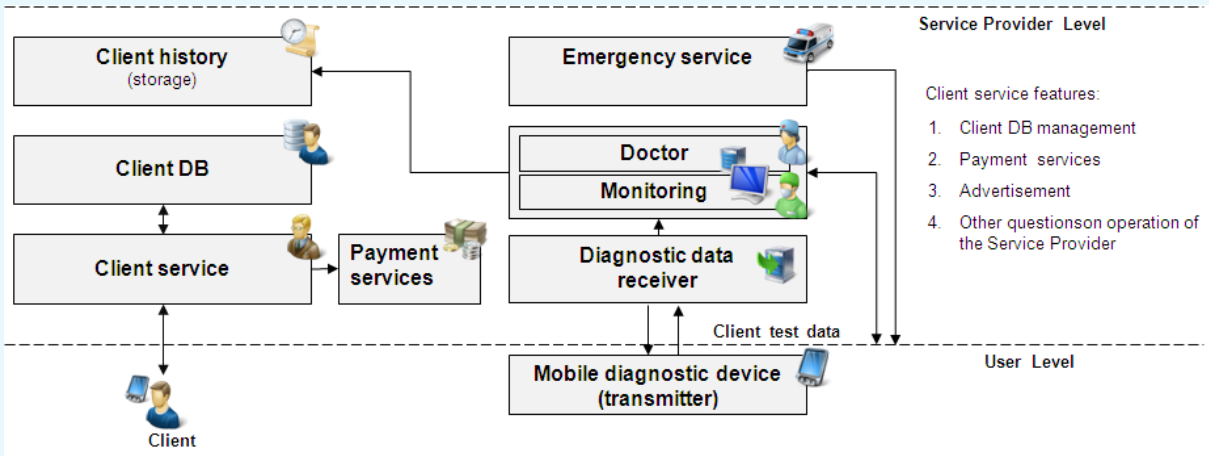
All identification and authentication centres must comply with the same allocation rules and regulations for global identifiers of mobile clients (mID), registered in a central System Directory to ensure message delivery to customers.

Figure 4: Unified authentication model with additional cryptography



As an example of usage of Unified Authentication Centre, proposed dynamic of development of Healthcare structure from several unrelated companies to a single National Healthcare System is provided below. Today many medical companies have been formed, holding their own technological know-how and trying with more or less success to implement ICT achievements in medicine, including mobile diagnostic devices.

Figure 5: The structure of a separate medical service provider



Some companies focused only on developing devices based on ICT technologies, others offer a full package including rendering medical services (see Figure 5). There are two levels of this structure: User level and the Service Provider level. Companies, using this two-level approach, supply their Clients with diagnostic devices which can take and transfer medical test results to the Centre. These companies perform monitoring of received data, data analysis, systematisation and storage of measured data, creating patients' records and providing emergency services, if necessary. Besides, each company provides a customer service, managing Client database and accepts payments for services. The shortcomings of such approach are described below:

1) Difficulty to present services to the Client (Advertising problem)

2) Difficulty for one service provider to use results obtained by another provider

3) If the client stops to pay, who will store his history?

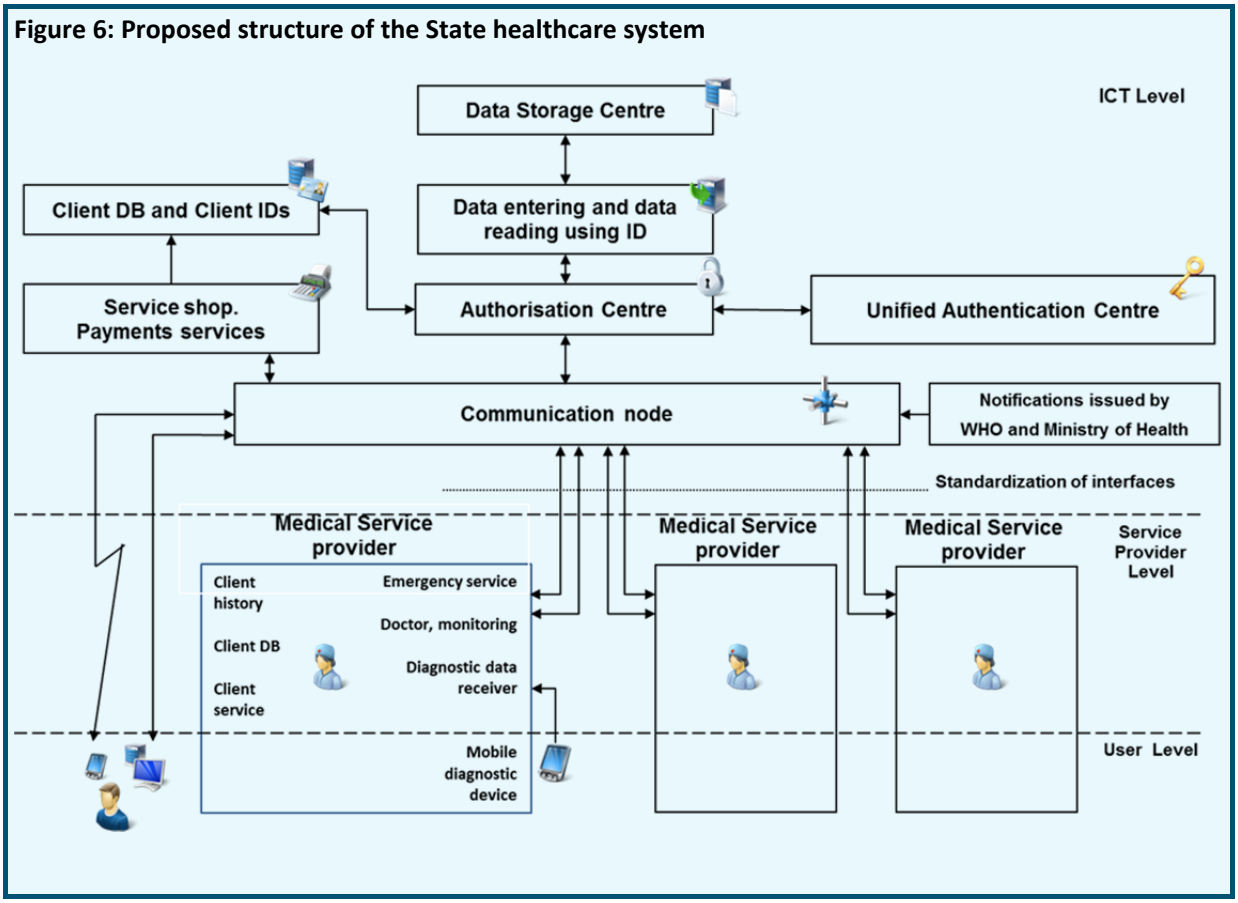
4) Insufficiency of authentication and protection of personal data

5)In case the Service Provider ends its activity, the Client history will be lost

Despite the fact that the use of ICT technologies in medicine is an explicit step towards the progress, such approach cannot be accepted as a base to implement a joint ITU-WHO initiative started at Telecom World-2012 in Dubai[2]. Therefore, three-level centralised scheme is suggested, integrating services of multiple service providers and implementing partnership between state and private sectors. In the structure shown in Figure 6 there are three logical levels: User level, Service Provider level and ICT level, which ensures secure data storage, multifactor authentication, multi-level access, remote payments and interactions with users. Communication node appears as the central device in the offered scheme, managing two-way communication between users (Clients or Service Providers) and the System, and providing information notifications. The node ensures operations with data for authorised users, which allows (depending on user rights) to read and/or enter data in the data storage. User authentication is performed by the Unified centre of authentication with the use of digital signature officially recognised as an analogue of manual signature. ICT provides the first line of communication with clients, conclusion of agreements and payments services last are performed, whenever possible, via remote means. The communication node uses all available means of communication with clients (mobile phones, e-mail, voice calls), dispatching and delivery of requests and responses, user authorisations and information notifications on behalf of public institutions (Ministry of Health, Ministry for Emergency Situations, etc.).

At the Service Provider level, there are different medical clinics, both state and private. They may have multiple specialisations and emergency services (if needed). These clinics may provide their clients with special mobile diagnostic devices, collecting and transmitting health parameters of clients to central devices.

Figure 6: Proposed structure of the State healthcare system



3.2 Keys administration

Cryptography can be used with both symmetric and asymmetric keys to encrypt transmitted data and to create mobile signatures. The advantage of symmetric encryption (Standards 3DES, AES) is to use algorithms that are easy to implement in low-cost computing devices. Symmetric key generation is a simple operation, which does not require any special means. However, by definition, use of the same key, shared between the user and service provider (provider's authentication centre), can cause a situation, when the user might dispute the completed transaction. It is fair to point out that mobile payment systems successfully use symmetric key cryptography, having learnt to create reliable transaction logging systems to deal with disputes.

Asymmetric key cryptography applies public-key infrastructure (PKI) to link two different keys which belong to one individual: "public" key, with publicly available identity, and "private" key that is securely stored and protected from unauthorized access (for example, in SIM card or specially protected smart card). Mathematical interaction between keys is managed in such a way that an action committed with one key can be "linked" to another key, without disclosing the private key data. This is particularly useful for creating an electronic signature, since the signing action completed by the private key identifies the private key owner only due to the relationship with the associated public key - the identity of the latter is known. The most important task of PKI technology is, on one hand, to ensure "privacy" of private keys, and on the other hand - to verify the relationship between open and private keys. This is achieved by

careful management of registration process when keys are issued, and certification process, confirming the identity of the public key. These elements are managed respectively by entities known as "Registration" and "Certification" Authorities, (i.e. RA and CA). In relation to mobile signature, their primary function is to acknowledge the unique relationship between private key usage and the registered identity of the Citizen by virtue of his/her ownership of the associated public key.

Asymmetric encryption methods require the use of more expensive computing devices, but they can be applied in numerous interaction patterns. Using the "dual key" provides opportunities for greater scalability and easier conflict resolution. This approach leads to more efficient trust model with simplified administrative management and services (for example, many different applications and interaction schemes can be supported by a single asymmetric key pair). As a result, documents describing global interoperability frameworks for electronic signature are almost entirely focused on asymmetric cryptographic encryption methods (e.g. eEurope "Blueprint" Smartcard Initiative[3]).

Currently, RSA-1024 is the most common asymmetric encryption system, but it is well known, that 512-bit key may be hacked with modern computing means in only 10 minutes and so for all newly designed secure systems NIST Special Publication 800-57[4] in 2012 required to use RSA-2048 encryption algorithm. Unfortunately, this will complicate the relevant calculations, and will scrutinise requirements for processor performance. That is why symmetric encryption is still often applied for non-powerful processors, used in mobile devices. In this case, asymmetric encryption may be utilised for secure distribution of a symmetric session key, which is used to encrypt subsequent communications. Scenario of such secure exchange of keys looks like sequence of steps outlined below:

– The application is loaded onto mobile device from an open source together with the public key of the System.
– During the activation process, the application generates a random symmetric session key.
– The application sends this session key encrypted using the public asymmetric key of the System.
– The System decrypts the session key using System's secret key and stores it at the Hardware Security Module.
– This session key is used by both the System and the Application for all subsequent activities.

4 Mobile Payment System (MPS)

Historically, mobile devices, for obvious reasons, were primarily used for remote financial transactions. To date, mobile payment service providers have gained great experience in various fields, including security. It is logical to extend this experience to other systems using mobile networks. In this regard, below we will consider mobile payment systems in more detail.

4.1 MPS participants and their Roles

To support transactions in MPS, following Roles must be present in the System:

– MPS Operator
– Mobile Operator
– Banks (for typical MPS)
  • Clients' Bank (bank issuer)
  • Acquiring bank, accepting payments and providing access to Clients' banks for merchants or service providers
  • Settlement Bank (interbank settlements)

– Clients (mobile Operator subscribers, using Mobile Payment System and owning payment card or bank account)

– Client application – a special program downloaded to a mobile terminal of the Client, or to special hardware security module, for example, SIM card, which allows to perform registration, select payment means, interact with authentication agent, perform financial transactions, and also to set up payment details.

– Issuers of Client applications

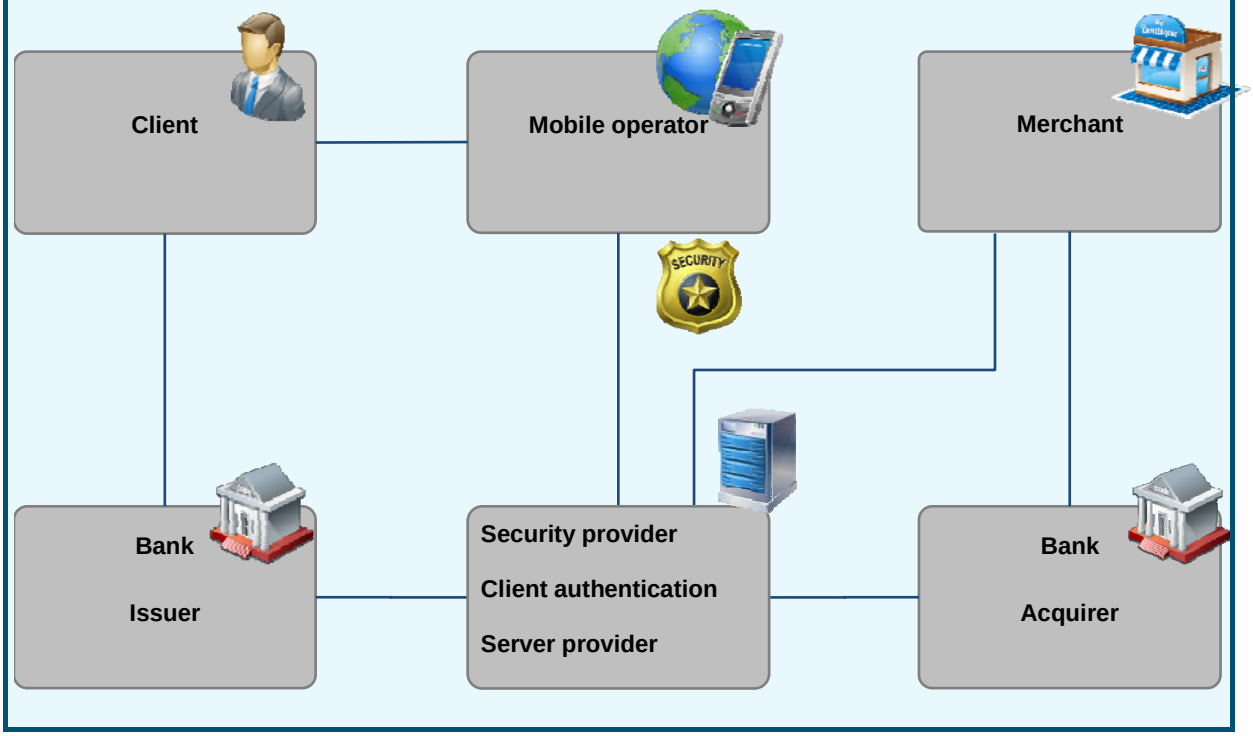
– Merchants (legal entities, clients of Acquiring Banks)

– Authentication agent (Client authentication)

4.2 Typical System Architecture

The following MPS architecture is suggested by the ITU-T Recommendation Y.2741[5] (Figure 5).
Such arrangement is recommended for implementation in local Mobile Payment System which handles payments within the same country.

Figure 7: (Y.2741) Secure Mobile Payment System Architecture

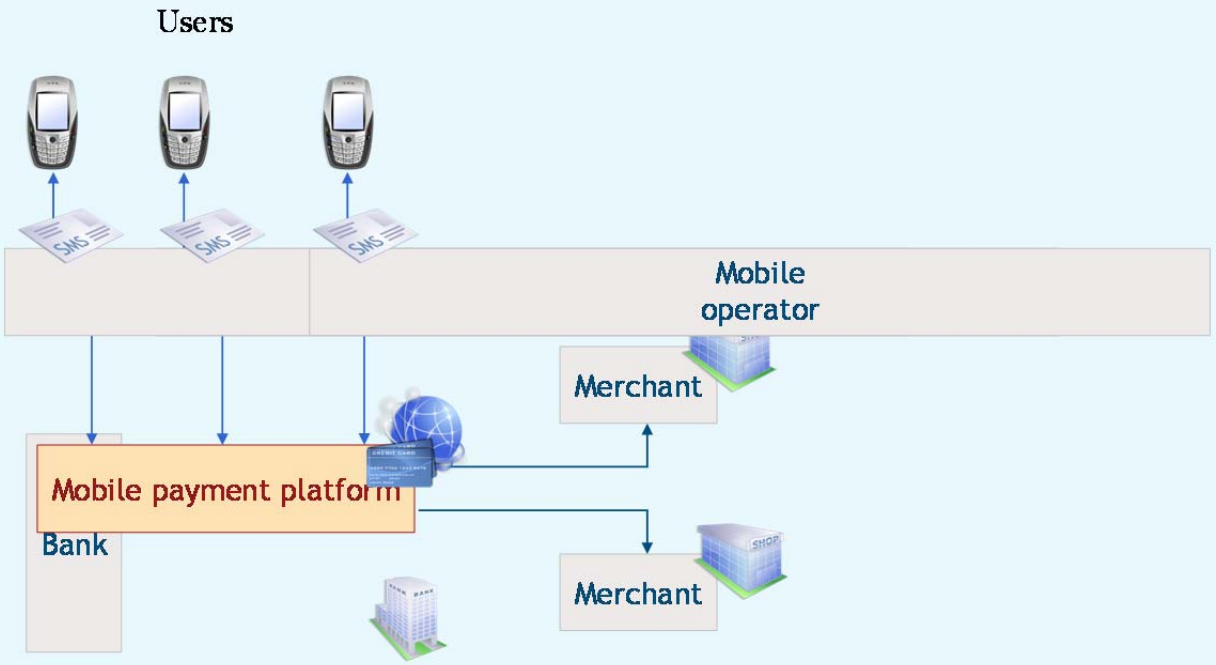


4.3 MPS Models

Different MPS models exist:

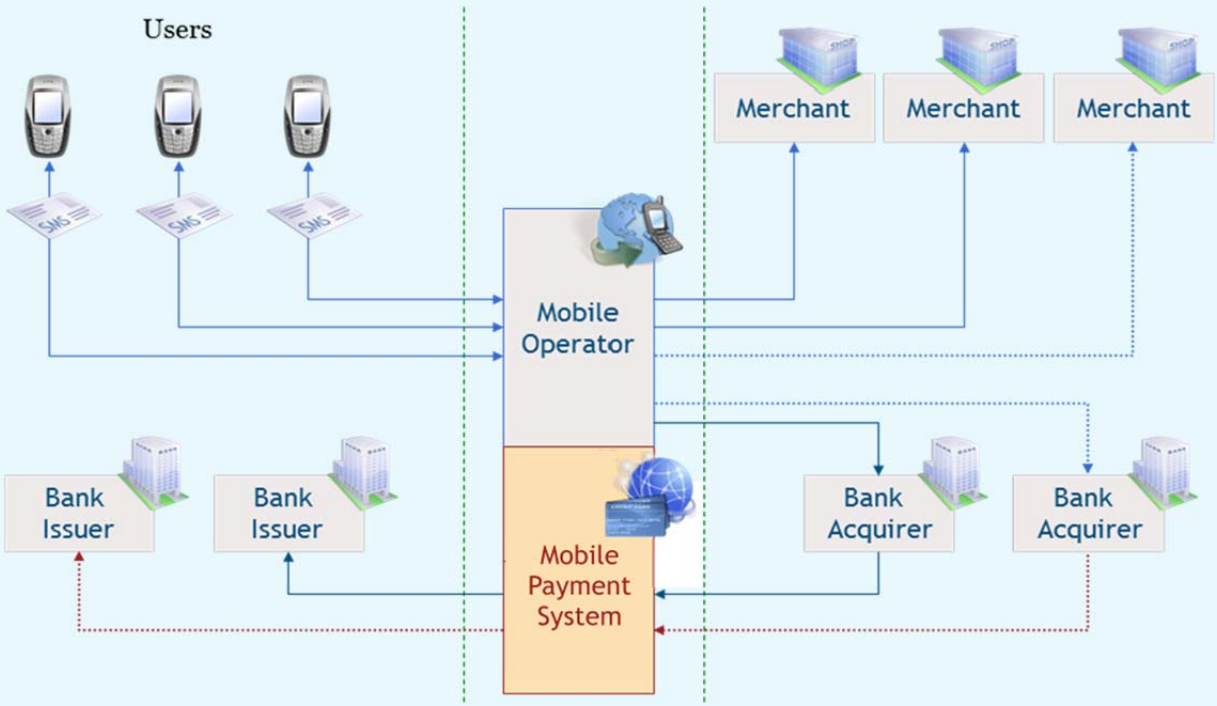
– Bank-oriented model (Figure 8), where bank offers mobile payment services with many mobile operators.

Figure 8: Bank-oriented MPS model



– Operator-oriented model (Figure 9), where mobile operator offers mobile payment service using payment cards as source of payment issued by multiple banks or using personal accounts of mobile subscribers.

Figure 9: Operator-oriented MPS model



– Mixed model (Figure 10) with multiple banks and multiple operators.

An example of such model can serve an MPS working with international payment cards, for example, MasterCard or VISA. However, most perspective model is the National Mobile Payment System, being a part of the National Payment System, integrating all national banks and working with all mobile operators.

Figure 10: Mobile Payment System as a part of the National Payment System

4.4 Available payment means

The following payment means may be used as a source in the Mobile Payment System:

– Bank account

– Bank cards issued by local or global payment systems

– MNO subscribers personal accounts

– E-money

4.5 Payment arrangement

Two operation types are available in MPS:

– Operations initiated by the Client

– Operations initiated by the Merchant

4.5.1 Operations initiated by the Client

Transactions initiated by the Client may contain the following steps:

1. By means of mobile device the Client generates a request containing parameters of the financial operation, payment instrument and secret PIN code
2. The request is transmitted via mobile operator channels
3. The MPS operator receives the request
4. The Client is authenticated
5. The required financial operation is performed using the Client's payment instrument details
6. The operation result is sent to the Client
7. The response is transmitted via the mobile operator channels
8. The Client receives the result of the financial operation

4.5.2 Operations initiated by the Merchant

Transactions initiated by Merchants may contain the following steps (it is assumed that the Client informed the Merchant on his unique identifier):

a) The merchant generates a payment offer and sends it to the MPS operator;

b) The MPS operator determines the Client and the way to deliver the payment offer to the Client;

c) The request is sent to the Client over the mobile operator channels;

d) The Client receives the request through his/her mobile device and generates the response that contains the financial operation parameters as well as the parameters of the payment instrument;

e) The request is transmitted via the mobile operator channels;

f) The MPS operator receives the Client's response;

g) Authentication of the Client;

h) The required financial operation (remittance/payment) of is performed using the Client's payment instrument details;

i) The operation result is sent to the Client;

j) The response is transmitted via the mobile operator channels;

k) The Client receives the result of the financial operation.

4.6 Near Field Communications (NFC)

NFC is evolving as a key technology for non-remote mobile payment services. This technology is positioned to enable user's handsets to communicate with card readers at the point of sale.

Mobile NFC business models are being developed to be integrated in any mobile security framework for financial transactions. Typically, mobile NFC system involves the following elements:

– Mobile Device with NFC Chipset or Secure Element of NFC Chipset containing the logic and interfaces to communicate with card readers.

– Mobile Network Operator (MNO)

– One or many Service Providers

– Trusted Service Manager or broker providing a point of contact between service providers and MO

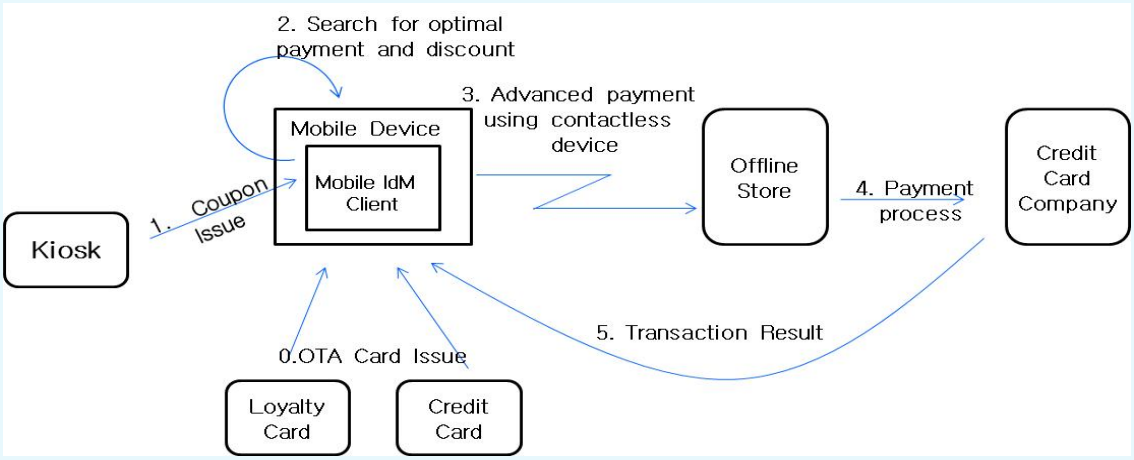
It is considered, that NFC payment systems can use credit cards as payment means for interactive shopping purchases via contactless NFC devices. After the payment transaction is processed successfully, result is stored in the system and sent to subscriber's handset. The use case is depicted in Figure 11 below. In order to actualise the scenario described above, following requirements are needed:

– User Authentication Communication security

– Protection of information stored, if mobile device is lost or stolen

– System storage to accumulate and process transaction records

Figure 11: Interactive shopping



NFC systems, due to its features, have become the most popular when carrying out the sale of consumer goods, and also within the transport sector, allowing for a reduction in the time spent to purchase tickets and significantly reducing lines for customers. Also, NFC-based systems can be successfully applied for authentication purposes instead of paper ID. Despite the differences, the main security methods for NFC operations remain the same as for remote services.

5 Security

The most important requirement for payment systems, as well as e-government and e-health, including their mobile variations, is security, which is provided by meeting recommendations of the ITU Telecommunication Standardization Sector, which issued a manual entitled "Security in telecommunications and information technologies[6]". This manual provides an overview of existing ITU-T Standards and their practical application in secure telecommunications. ITU-T Standards are required to follow, they stay as recommendations, but compliance with recommendations is essential to ensure compatibility and consistency of telecommunication systems of different countries.

Since these systems include many players, security considerations can be divided in multiple categories that include:

a) End-point Security

b) Mobile Application Security

c) Mobile Network Security

d) Identification of the requesting party that includes proper identification of the individual that is requesting the financial transaction.

Prior to the era of smart phones, management of mobile applications by operators on mobile phones was relatively easy. Basically, operators used to control which application can be downloaded onto device and their security characteristics. Management of mobile applications becomes more complicated with the advent of smart phones and ability to freely download third party applications. Nowadays, it is almost impossible to be completely certain that every application that is executing on a mobile device originated from a trusted source. As a result, mobile users are subject to additional threats such as identity theft, phishing, and loss of personal data.

The term "security" is used in the sense of minimising vulnerabilities of assets and resources. An asset is anything of value. Vulnerability is any weakness that could be exploited to violate a system or information it contains. A threat is a potential violation of security. The ITU-T Recommendation X.805 "Security Architecture for Systems Providing End-to-End Communications[7]" (Figure 10) of defines set of eight so-called "Security dimensions" – set of means that protect against all major security threats, described in the ITU-T Recommendation X.800 "Security architecture for Open Systems Interconnection for CCITT applications"[3]*:*

– destruction of information and/or other resources;

– corruption or modification of information;

– theft, removal or loss of information and/or other resources;

– information disclosure;

– service interruption.

Security dimensions are not limited to the network, but extend to applications and end user information as well. In addition, security dimensions apply to service providers or enterprises offering security services to their customers. The security dimensions are:

1) Access control;

2) Authentication;

3) Non-repudiation;

4) Data confidentiality;

5) Communication security;

6) Data integrity;

7) Availability;

8) Privacy.

Properly designed and implemented security dimensions support security policy that is defined for a particular network and facilitate the rules set by the security management.

The access control security dimension protects against unauthorized use of network resources. Access control ensures that only authorised personnel or devices are allowed to access network elements, stored information, information flows, services and applications. In addition, Role-Based Access Control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to, and perform operations on, network elements, stored information, and information flows that they are authorised for.

[3] ITU-T Recommendation X.800 "Security architecture for Open Systems Interconnection for CCITT applications (page 12).

The authentication security dimension serves to confirm identities of communicating entities. Authentication ensures validity of claimed identities of entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication.

The non-repudiation security dimension provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It provides evidence that can be presented to a third party and used to prove that an event or action has taken place.

The data confidentiality security dimension protects data from unauthorized disclosure. Data confidentiality ensures that the data content cannot be understood by unauthorized entities. Encryption, access control lists and file permissions are methods often used to provide data confidentiality.

The communication security dimension ensures information flows exchange only between the authorised end points (information is not diverted or intercepted as it flows between these end points).

The data integrity security dimension ensures correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.

The availability security dimension ensures that there is no denial of authorised access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category.

The privacy security dimension provides protection of information that might be derived from the observation of network activities. Examples of this information include web sites visited by a user, user geographic location, and IP addresses and DNS names of devices within service provider network.

In order to provide an end-to-end security solution, security dimensions must be applied to a hierarchy of network equipment and facility groupings, which are referred to as security Layers and security Planes. The Recommendation X.805 defines three security layers build on one another to provide network-based solutions:

– Infrastructure security Layer, consisting of network communication means and individual network elements (routers, switches, servers, communication lines);

– Services security Layer to protect service providers and their clients (both basic services – connection to resources, DNS, and additional services – VPN, QoS, etc.);

– Applications security Layer, includes 4 potential targets: application user, service provider, application provider, bounding software.

Security layers represent a series of interrelated factors that contribute to ensure network security: Infrastructure security layer allows to use Services security layer and Services security layer allows to use Applications security layer. Security architecture takes into account that each layer has different security vulnerabilities, and provides flexibility in reflexion of potential threats in the most appropriate way for a particular security layer.

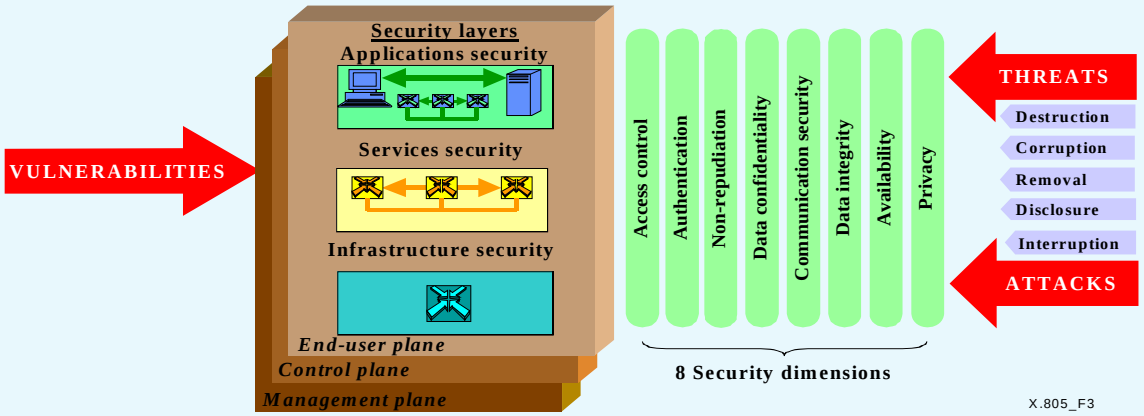
Each of these security Layers consists of three security Planes, representing a specific type of network operation, protected by Security dimensions:

– End-User Plane;

– Control Plane;

– Management Plane.

Figure 12: X.805 – Security architecture for end-to-end network security



According to this Recommendation the security architecture logically divides the System in question into separate architectural components. This separation assumes a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing solutions. The security architecture addresses three essential questions with regard to the end-to-end security:

1) What kind of protection is needed and against what threats?

2) What are the distinct types of system equipment and facility groupings that need to be protected?

3) What are the distinct types of system activities that need to be protected?

These questions are addressed by three architectural components: security dimensions, security layers and security planes.

– Required security should be based on the use of:

– Means of identification and authentication of participants;

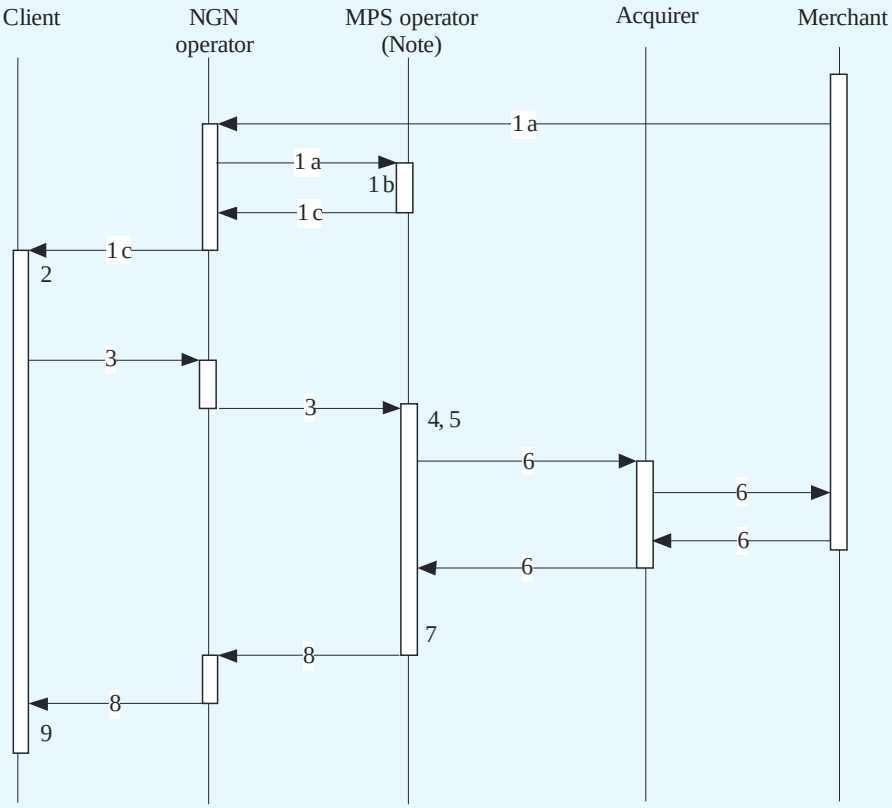
– Encryption of data transmitted through communication channels;

– Physical and administrative means to ensure the safety of information transmission and storage.

The ITU Recommendation X.1122[9] applies when using asymmetric cryptography, and provides guidelines for creation of secure mobile systems based on Public Key Infrastructure (PKI). This standard describes generation of public and private keys, certificate applications, as well as issuance, activation, use, revocation and renewal of the certificate.

The ITU Recommendations Y.2740 and Y.2741 describe security requirements and architecture of secured mobile financial transactions. These recommendations, though made for mobile remote financial transactions in NGN, are fully applicable to ensure security for m-Payment, m-Health and m-Government Systems in 2G, 3G and 4G mobile networks. The Recommendation Y.2741 describes the system architecture (Figure 5) and possible interaction scenarios. The example of such scenario for Merchant initiated payment is shown in Figure 11.

Figure 13: Performing payments initiated by merchant



NOTE – Security provider, client authentication provider, service provider.

ITU-T Y.2741(11)_F04

The basic steps of the scenario are as follows:

1. a) the Merchant generates a payment offer and sends it to the MPS operator;
   b) the MPS operator determines the client and the way to deliver the payment offer to the client;
   c) the request is sent to the client over the mobile operator channels.
2. The client receives the request through his/her mobile device and generates the response that contains the financial operation parameters as well as the parameters of the payment instrument;
3. The request is transmitted via the mobile operator channels;
4. The MPS operator receives the client's response;
5. Authentication of the client;
6. The required financial operation (remittance/payment) is performed using the client's payment instrument details;
7. The operation result is sent to the client;
8. The response is transmitted via the mobile operator channels;

9. The client receives the result of the financial operation.

The Recommendation Y.2740 defines four levels of system security and its provision. Security Level is determined by the extent to which security dimensions are implemented in the System. According to this Recommendation system participants should be aware of the Security Level, which should be stipulated in the participants' agreement if it is not contrary to the law. Service providers can further reduce the risks by organizational means - to restrict the transfer of some information, to limit service for users with a low level of loyalty, etc. The System security is entrusted upon every participant of the System and is achieved by the physical and administrative facilities of security assurance at data transfer, processing and storage. Implementation of security dimensions are required to be executed by all the participants in respect of data involved in information exchange. Thus the subscribers are responsible for maintaining the secrecy of their PIN codes, for the safe storage of their mobile terminals, as well as for confidential information related to a bank account or plastic payment card secure parameters. In turn, service providers are liable for the logging of performed transactions, security of transmitted and stored sensitive information, user authentication, etc.

Security Levels defined in the ITU-T Recommendation Y.2740 "Security requirements for mobile remote financial transactions in next generation networks":

Security Level 1

System can rely on authentication provided by the NGN operator. Data confidentiality and integrity at their transfer are ensured by the data transfer environment (communications security), and at their storage and processing – by the data storage mechanism and System access control facilities. The privacy is ensured by the absence of sensitive data in the messages being transferred as well as by the implementation of the required mechanisms of data storage and the System access control facilities. The System components must not have latent possibilities of unauthorized data acquisition and transfer.

Security Level 2

Authentication when using the System services can be executed by using only one authentication factor and thus can be implemented without the application of cryptographic protocols. One-Time Password is used for authentication. One-Time Password is generated by means of various tokens (Single Factor OTP Device, Single Factor Cryptographic Device, etc.). Data confidentiality, integrity and privacy are ensured similarly to Level 1.

Security Level 3

Multifactor client authentication must be used to access System services. The Client shall use more than one authentication factor. Data confidentiality, integrity and privacy at message transmission must be ensured by using additional message encryption together with data transfer protocols that ensure the security of the data being transferred by the interoperation participants (including data integrity verification); at data storage and processing their confidentiality, integrity and privacy are ensured by additional mechanisms of encryption and masking, together with well-defined distribution of access in accordance with privileges and permissions.

To meet security requirements at this level, System shall use software modules installed in Clients' handsets. These modules shall implement at least two-factor authentication and ensure both encryption and decryption of transferred data. Each authentication shall require entry of the password or other activation data to activate the authentication key and the unencrypted copy of the authentication key shall be erased after each authentication (Multi-factor Software Cryptographic Token).

All System interoperation participants shall use security facilities that ensure the System against break-in. In the Level 3 solutions the security of data transferred over the communications channels shall be ensured by means of strong cryptography. The strength of a cryptographic method depends on the cryptographic key being used. Effective key size shall meet minimal length recommendations to suffice protection.

Security Level 4

This is the highest System security assurance level. To meet security requirements at this level, clients' mobile terminals shall be equipped with hardware security modules. Implementation of other security dimensions shall fully correspond to level 3. Both symmetric and asymmetric cryptographic algorithms may be applied to message encryption. To prevent interception or corruption of information between mobile terminal elements (e.g. CPU and display, CPU and keyboard), some security measures shall be taken to ensure the integrity of data exchange on the Client's device (Trusted Execution Environment).

Security dimensions that are equally implemented at all Security Levels:

– access control,

– non-repudiation,

– communication security,

– availability

The following security dimensions have different implementation at different Security Levels:

– authentication,

– data confidentiality,

– data integrity,

– privacy

From Table 1 it follows that the implementation of the first and second levels of security can be achieved without installation of any special applications on the mobile device or special security element of mobile device; but to implement the third and fourth security levels, it is necessary to install custom applications that provide client authentication, encryption and decryption of data transmitted.

Table 8: Security implementation degree - (Y.2740) subject to Security Level

Security Dimension	Security Level			
	Level 1	Level 2	Level 3	Level 4
Access Control	The access to every system component shall be granted only as provided by the System personnel or end-user access level.			
Authentication	Authentication in the System is ensured by the NGN data transfer environment	Single-factor authentication at the System services usage	Multi-factor authentication at the System services usage	In-person connection to services where personal data with obligatory identification is used. Multi-factor authentication at the System services usage. Obligatory usage of Hardware Cryptographic Module.
Non-repudiation	The impossibility of a transaction initiator or participant to deny his or her actions upon their completion is ensured by legally stated or reserved in mutual contracts means and accepted authentication mechanisms. All system personnel and end-user actions shall be logged. Event logs shall be change-proof and hold all actions of all users.			

Table 8: Security implementation degree - (Y.2740) subject to Security Level

<table>
<tr><th rowspan="2">Security Dimension</th><th colspan="4">Security Level</th></tr>
<tr><th colspan="2">Level 1</th><th>Level 2</th><th>Level 3</th><th>Level 4</th></tr>
<tr><td>Data confidentiality</td><td colspan="2" rowspan="2">Data confidentiality during the data transfer, is ensured by the data transfer environment (communications security), and by the mechanism of data storage together with the means of system access control – at data storage and processing.</td><td rowspan="3">Data confidentiality during the data transfer is ensured by additional message encryption together with data transfer protocols that ensure the security of the data being transferred by the interoperation participants (including data integrity verification); at data storage and processing their confidentiality, integrity and privacy are ensured by additional mechanisms of encryption and masking together with well-defined distribution of access in concordance with privileges and permissions.</td><td rowspan="3">The implementation of the Level 3 requirements with the obligatory usage of hardware cryptographic and data security facilities on the Client’s side (Hardware Cryptographic module).</td></tr>
<tr><td>Data integrity</td></tr>
<tr><td>Privacy</td><td colspan="2">Privacy is ensured by the absence of sensitive data in the messages being transferred as well as by the implementation of the required mechanisms of data storage and the System access control facilities.
The System components must not have latent possibilities of unauthorized data acquisition and transfer.</td></tr>
<tr><td>Communication</td><td colspan="4">The delivery of a message to the addressee is ensured as well as the security against unauthorized disclosure at time of transfer over the communications channels. It is ensured by the NGN communications providers.</td></tr>
<tr><td>Availability</td><td colspan="4">It ensures that there is no denial of authorised access to the System data and services. Availability is assured by the NGN communications providers as well as the service providers</td></tr>
</table>

6 Mobile Technology

To date, the term "mobile communication" is most often associated with the GSM Standard of the second and the third generations. These mobile communication systems use different subsystems for voice and data transfer (with the use of time-division switching and packet switching technology) and this is an intermediate step in evolution of mobile communications. Next Generation Networks (NGN), which has already come to replace existing networks, provides subscribers with broadband access and use only packet switching channels technology.

NGN perform voice, images, text and multimedia messages transmission services, as various applications of universal process of Batch Data Transmissions. As a result, SMS and MMS data transmission technologies, widely used at the present time, may yield to other technologies. Users may not even notice these changes. However, technological solutions developed for m-services should be prepared for the process of evolution of mobile communications.

Today's mobile terminals are widely used, but originally they were not designed for systems with strong authentication. Therefore, terminals of different manufacturers and even different models of terminals made by the same manufacturer may use different algorithms, which lead to greater complexity, and in some cases – to inability to create Applications which perform all required System functionalities. For instance, an application should be able to be activated automatically upon receiving a message from

Mobile Payment System (Operations initiated by Merchant). Unfortunately, it cannot be implemented in every mobile terminal.

To unify operation of such systems, some additional protocols should be standardised and ITU, together with equipment manufacturers, can perform this task. Another important challenge is the location of crypto-application and administration of access to this application. As it is shown in the chapter "Security", in order to achieve the highest level of security, these applications should be located in a special module (hardware security element), which protects stored information from unauthorized access. Thus, SIM/UICC card can be successfully used as a module, provided that the problem of delegation of administrative rights to access SIM card, belonging to the mobile operator, will be solved. This problem is easily solved when both of these functions are performed by the same entity, otherwise it becomes difficult. Creation of mobile terminals equipped with an additional hardware security element can be considered as a solution to resolve issues resulted from SIM card co-management. This may be reached by an embedded security module or specially installed tamper-resistant memory card.

There are different ways of data transfer available in mobile networks, such as CSD, SMS, USSD, GPRS, EDGE, LTE. Each of them has its advantages and disadvantages. For example, SMS is very reliable and easily implementable way, but limited by message length. On the contrary, GPRS is not limited by message length, but less reliable and requires correct adjustments for mobile terminal, especially in roaming, which is also very expensive.

The success of technology progress has led to wide implementation of geo-location services in smartphones based on GPS or GLONASS systems. Geo-location essentially expands functional capabilities of mobile terminals. Therefore, lately geo-location services are widely used in applications for mobile devices (where the share of smartphones grows rapidly).

7 M-Government in the European Union

According to "Mobile Signatures Whitepaper: Best Practices[10]", issued on 25th April 2010, the most advanced national m-Government services, based on Digital Identity systems using cryptography techniques are implemented in Turkey and Estonia. Also, Finland is a top-ranked leader in the field of e-ID, including mobile PKI, which is seen as a great alternative for strong and flexible user authentication and electronic signature service.

Mobile PKI offers a very strong security framework for all parties. The security related operations are done in the SIM card, tamper resistant environment, making it almost impossible to misuse the user identity. Software that tries to steal the user identity, passwords or other credentials cannot penetrate into SIM content. Authentication and signature information are transmitted via SMS and back-end channels to the service provider and are verified by the operator, so even if the user is attacked at the browser level, or the computer is infected, it does not matter. The data never goes through the Internet channel. To be successful, attacker should also gain access to the mobile operator network to attack/infect the encrypted SMS messages.

All of these services are using asymmetric cryptography techniques and based on European Parliament and Council Directive on Electronic Signature and ETSI Mobile Signature Requirements and Specifications:

– ETCI TR 102 203[4]
"Mobile Commerce (M-COMM); Mobile Signature; Business & Functional Requirements"

[4] ETCI TR 102 203 "Mobile Commerce (M-COMM); Mobile Signature; Business & Functional Requirements" (page 19).

– ETCI TS 102 204[5]
"Mobile Commerce (M-COMM); Mobile Signature; Web Service Interface".

– ETCI TR 102 206[6]
"Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework".

– ETCI TS 102 207[7]
"Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services".

Mobile signature is *"A universal method for using a mobile device to confirm the intention of a citizen to proceed with a transaction."* It is an enabling technology that allows remote or present authorisation of electronic events using a mobile phone. Mobile Signature can carry legally valid identity information (qualified digital certificates) of over a GSM network and provide that information to any authorised application. According to documents, mentioned above, mobile signatures are digital signatures that are created using private key data that is stored on the UICC; so it can be used to provide legal and ultimately secured transactions. Essentially, Mobile Signatures extend the concept of Digital Identity and encompass the mobile phone as main device for authentication. Mobile Signatures can, in principle, be applied to any electronic event that requires authorisation by a nominated individual or by a member of a defined group of individuals. Mobile Signature is an important building block for secure services, which helps service providers to identify and authenticate users, and also may be used to sign secure transactions.

Figure 14: Typical mobile smartcard implementation

Modern communications and e-commerce are largely built on a solution, i.e. Internet that was built without an identity layer that would allow each party to identify their communicators. 'Identity' leads to the development of trust models that are so important to the functioning of current societies. By establishing a Public Key Infrastructure (PKI) and providing digital certificates and keys to end users on a mobile phone UICC (Wireless PKI), digital identity can be established thus enabling the delivery of new and enhanced features and services For example, virtual access to Internet resources, financial transaction authorisation or electronic document signing. It should be noted that Digital Identities are not necessarily unique as one identity may be used by more than one person as in the case of joint signatories

[5] ETCI TS 102 204 "Mobile Commerce (M-COMM); Mobile Signature; Web Service Interface" (page 19).

[6] ETCI TR 102 206 "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework" (page 19).

[7] ETCI TS 102 207 "Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services" (page 19).

or members of shared groups with equal authority to access a resource or service. Also one person may have multiple digital identities for different services. Identity Management System (IDM) not only provides a structure for storing identity but also provides assurance that the right people have the right access at the right time. Essentially the systems provide authentication, authorisation and administration. Authentication ensure that the requesting application or individual is who they say they are; authorisation determines what they are allowed to access; and administration deals with the routine maintenance, ensuring that the system works and that integrity is ensured.

Security is greatly increased due to the use of UICC in secure chain of events and also due the nature of services which will typically require two “points of presence” in the transaction chain, i.e. Internet portal access from the computer will also require the user to authorise the event from his mobile phone. If the mobile phone user, phone (UICC) and the originating event are not all present, the activity will not be possible. Further, information required to perform an event, for example, account information, can be transmitted over different channels thus disassociating it from the originating service and reducing the risk of fraud.

Mobile signature creation is achieved using a crypto-processor on a smartcard, such as Subscriber identity module (i.e. SIM card) found inside GSM mobile handsets or the Universal Integrated Circuit Card (UICC) that has been adopted for 3rd Generation mobile devices (Figure 12). The use of SIM or UICC smartcards in mobile operator business model effectively gives mobile operators the role of "Smartcard Issuer".

Signature requests, received on citizen’s mobile device, trigger a "signing" application on a smartcard. This allows the display of the transaction text on the mobile device screen and provides an option for the citizen to enter his/her signing PIN. The fact of entering the correct PIN initiates creation of the mobile signature in the smartcard and transmission of the signature to the mobile signature service. By entering the correct signing-PIN, citizen is deemed to have confirmed his/her intention to proceed with transaction details displayed on his/her mobile device screen.

In the solution described above, Mobile Signature extends PKI authentication technology to the Mobile Phone environment (WPKI) and positions the SIM/UICC card along with the mobile phone as the main device in the service chain. Below a simplified process flow for the User to access a Service Provider is described (see Figure 13):

– The User shall access the service via the Internet browser.

– Internet service requests the User to input the account name or a similar account identifier.

– Internet service identifies that the User has the Mobile Signature and initiates an authorisation request to the relevant Mobile Signature service provider (MSSP).

– MSSP sends an SMS to the SIM Client on the User’s mobile phone, which requests a Mobile Signature from the User.

– The User enters the signature PIN code.

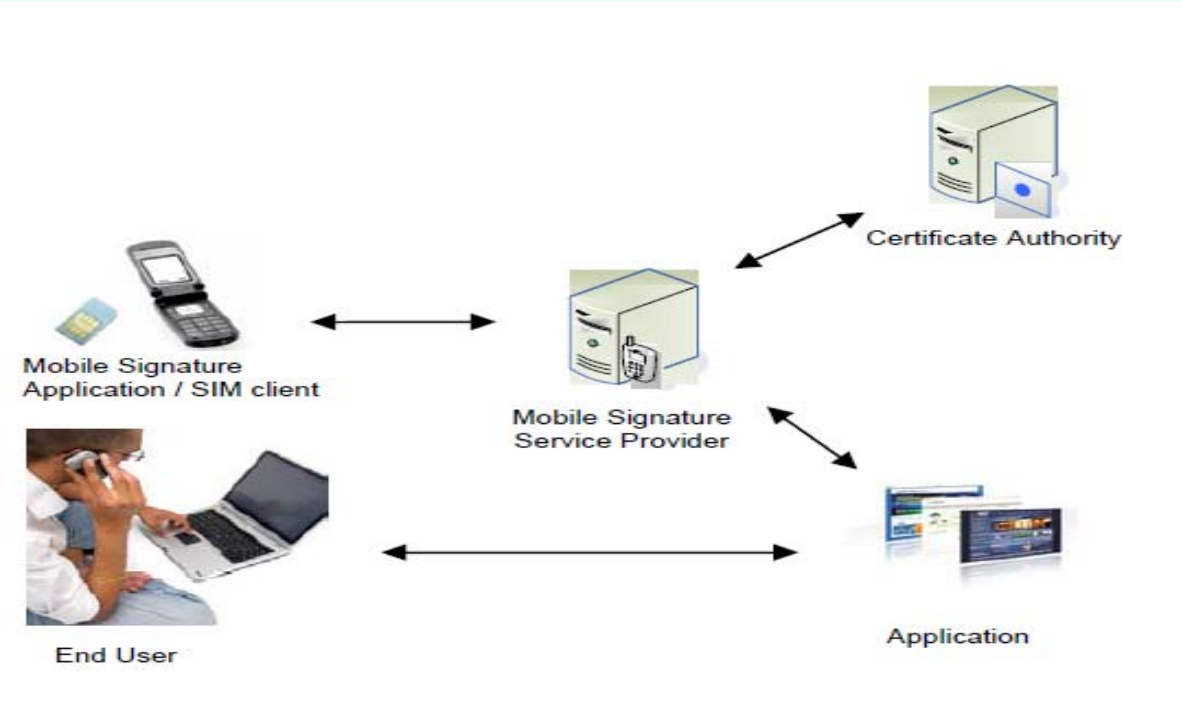
– Mobile application sends Mobile Signature to MSSP.

– MSSP sends a request to the Certification Authority, which shall verify the Mobile Signature.

– MSSP returns a positive confirmation to the Application.

– The User is authorised to enter the service menu at the Internet site.

Figure 15: Use of the 2nd "Point of Presence"



Roles

The following describes the roles of MSSP, Registration Authority and Certification authority.

These are described in greater detail in ETSI TS 102 203.

Role of MSSP

MSSP is in charge for service facilities it provides. MSSP may be required to demonstrate compliance to contractual agreements (where they exist), including active management of:

– Preparation of a documented security policy.

– Prevention of unauthorized Access to databases, etc.

– Detection of unauthorized access to databases, etc.

– Implementation of processes to monitor vulnerabilities.

– Actual monitoring for system vulnerabilities.

– To record and retain system information sufficient to perform security audits and investigations.

– To record and retain security audit reports.

MSSP may also be in charge for physical elements used in the delivery of services they provide (e.g. mobile equipment). This may include (but not be limited to) of the following elements:

– Provide assurance that "what the user sees is what the user signs …"

– The PIN should be erased from all memory after being transmitted to the card.

– A card with which no interaction occurring should be powered off after a prescribed timeout.

– No application capable of mimicking user screens should be installable in the mobile handset.

– No application capable of disclosing the PIN (e.g., Capturing it and sending it via SMS) should be installable in the mobile handset.

– The keying in of the PIN should not generate DTMF signals (a malicious party eavesdropping on the communication could then determine the PIN even if the PIN itself is not transmitted out of the mobile handset!).

– Users may have the ability to customise the screens displayed by the mobile handset goal being to avoid confusing the user with a fake mobile handset whose sole function is to capture the PIN).

– The signature and the signed message should be erased from all memory after use.

– Entering the PIN may result in display of a sequence of characters unrelated to the PIN's value or length.

– The human interface should be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

– All software running on the mobile device should be immune to buffer overrun attacks.

– Citizens may have the ability to terminate the mobile signature service from the mobile device (e.g. in emergency/distress situations).

Role of the Registration Authority (RA)

The RA is responsible for acquiring and validating personal information provided by potential users. The process of acquiring this information is called the Registration Process (RP).

Role of the Certification Authority (CA)

The CA is responsible for processing information from the RA and certifying public keys of citizens who intend to use the mobile signature service. In addition, CA will provide a certificate revocation service (i.e. to manage mobile signature lifecycle and permit audit transaction investigations).

Benefits for the service provider

One of the biggest advantages for the service provider is cost efficiency. According to the Tax Administration in Finland, the cost for a single transaction went down from of €10 - €50 to of €0.20 - €0.50 per transaction, when they adopted on-line services. Cost savings for the service provider, even in a small nation such as Finland, can be huge.

These on-line services are under constant threat. On-line crime has turned into highly professional business. The service provider needs to protect its own assets and give users the assurance their information is also protected. User’s trust is a key for the service provider. Today, passwords to protect customers and their data are not enough to establish trust with the customer. They may even discourage potential customers, slow down adoption and eventually kill the service. More and more services are going into the cloud, and the normal authentication is “username + password”. Security breaches in these kinds of services are not breaking news any longer. Online services that offer alternatives gain competitive advantages over others.

Strong authentication is one way of mitigating some of the risks related to on-line services and Mobile PKI offers one of the strongest and easiest ways to authenticate the end user. Another aspect in on-line business is transaction protection.

There are several potential threats when a high-level transaction is performed in on-line service. Mobile PKI offers two distinctive advantages over other methods:

– Transactions are signed using a method that complies with the EU electronic signature directive and making signatures legally binding;

– The transaction and the identity of the user are protected against even the most sophisticated attacks. Pretending to be someone else requires access to both the service and the operator network. This is not an easy task to do. New on-line services can be delivered in a favourable environment with minimal risks as they will be protected from fraud from the start.

Benefits for mobile network operators

Mobile network operators have to get the best ROI from their investments. They have to create new opportunities and generate revenue. Mobile PKI enables both. One of the issues service providers are struggling with is the mobilisation of the user base. Users crave for services that are available 24/7, reachable from almost anywhere and at the same time they need security. Mobile PKI offers both. For the MNO it creates new opportunities in several ways:

– adds value to current services;

– can secure new products and services to attract new customers;

– can stimulate new business models;

– can strengthen customer loyalty.

For revenue opportunities the MNO can investigate these different options:

– Negotiate high volume, special priced authentication transactions for e-Government, corporate or financial services;

– Produce new services and integration options for the end user organisations;

– Offer trust centre-type of services to other organisations;

– Generate transaction revenue in services requiring transaction verification (electronic signing).

Mobile PKI creates a wealth of new opportunities. For the MNO, it means offering new and innovative services to its existing customer base, targeting completely new customer segments and use cases where MNO presence was previously only through the subscriber base.

A micro loaning service and a pension fund provide Mobile ID authentication for their users. The Lahti municipality uses Mobile ID to authenticate people accessing several different online services. The National Board of Patents and Registration of Finland allow users to access the services using Mobile ID.

Every week new service providers join mobile PKI revolution and create more value for the stakeholders in the mobile PKI ecosystem. The main beneficiary being is the end user.

Benefits for the Government

Mobile ID enables governments to put the citizen electronic ID into every pocket that can hold a mobile phone. Complementing the national eID card the mobile PKI SIM card adds a true mobility factor into the e-Government services. Now citizens can access services from all over the world, only thing needed is a working SMS connection.

One of the biggest challenges in the market has always been the threshold in user acceptance. If the solution is too complex, citizens may shy away from it. Using the mobile phone as a signing and authentication device is natural for almost all users, and when it is done using a SIM card one can also see it as the most democratic method of all – it can be available to anyone who has a mobile phone. Mobile PKI truly brings power to people's fingertips!

Mobile ID provides also the capability to digitally sign documents. When using the EU directive as an example Mobile ID can be used to produce advanced electronic signatures.

Benefits for the End User

Extreme mobility is the most obvious benefit for the user. As Mobile ID is managed in the SIM card on the client side, it can be used within almost any mobile phone out in the market.

Mobility is one of the key features that the MNO and service provider also see as a great benefit for the end user. Due to Mobile ID, the end user has a strong authentication method available in his/her mobile phone. An easy-to-use PIN is required to use the keys stored on the card for authentication or signing. This is extremely important as mobile phones have been part of daily lives for many people all around the globe.

With Mobile ID, value of the mobile phone increases even more. Besides games, entertainment, web access or banking applications, it offers remote electronic identity tool, that always available for the user, strong authentication, and consent through secure electronic signature, secure banking access, age verification, and much more.

Mobile ID can open up a multitude of new possibilities for the benefits of users, mobile operators and service providers.

Recently, European system that serves to provide mobile signatures was adopted by non-EU countries, such as the Republic of Moldova. Long-term experience of successful operation of the system and its global penetration show real attraction of this solution, however, most likely, in the long term the encryption algorithm RSA-1024 will not meet tamper resistance requirements and probably will be replaced with some more complicated algorithm, which will require, as it was stated above, to use more powerful processors. However, most likely, progress of mass production technology will allow not to increase costs of UICCs.

8 Case Study in Japan

In Japan, number of domestic subscribers of mobile phones, having been increasing year by year, was 128.21 million (up of 7.3 % of from last year) by the end of FY2011[15]. The mobile phone is an important infrastructure to support economic and social activities and the daily lives of the people.

In addition, spread of smartphones has been progressing rapidly. Smartphone shipments in Japan in FY 2011 amounted to 23.4 million units (2.7 times increase year-on-year), accounting for 55.8 % of total shipments of mobile phone terminals[16]. Furthermore, since FY 2012, mobile phone terminals with NFC (Near Field Communication) functions have been introduced into the market.

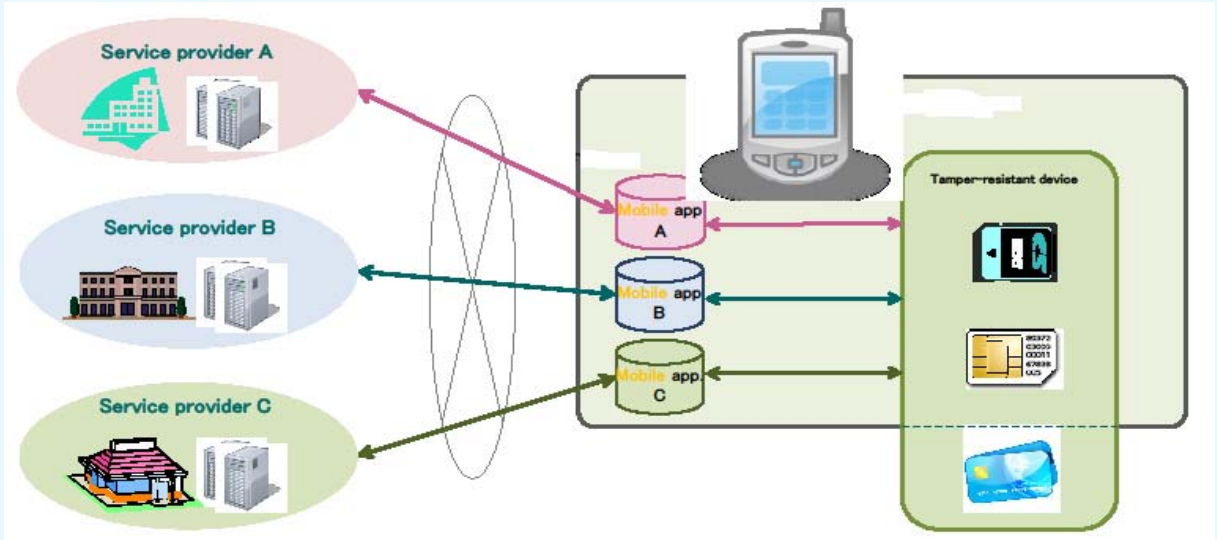
The government of Japan, in “The New Strategy in Information and Communications Technologies (IT) Roadmaps” (suggested in June 2010, revised in August 2011 and in July 2012) made by The Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (director-general: prime minister), presents the following goals regarding programs to diversify methods to access administration services, concerning the renovation of the government portal, and to encourage people to access the governmental service: in 2011, deliberation, verification, and demonstration of methods for mobile access to administrative services with authentication from mobile phones; from 2012 to 2013, based on demonstration, to introduce, develop and promote services partially in testing areas based on the demonstration above, and gradual nationwide deployment; by 2020, realisation of highly convenient electronic administration services, namely a 'one-stop service'.

Based on the roadmap, for the purpose of technical specification review and technical verification toward the realisation of the underlying mobile access system for using Web services through mobile phones in the field of public administration, ministry of Internal Affairs and Communications conducted the “Project Promoting Cooperative Business Administration Systems (Verification of Ways of Improving User-Friendliness for Mobile Phones as Means of Access)” in 2011, based on survey and research results from

the (Commissioned) "research and study of the diversification of means of access to electronic administrative services, etc. (research and study of technology for mobile phones to access electronic administrative services, etc.)" conducted in 2009 (Contracted).

As discussed above, mobile terminals with NFC functions are going to be commercialised from FY 2012. They realise both offline and online enclosure, into tamper-resistant devices (Devices equipped with an IC chip having a function to protect internal of physical or theoretical information), of service users' personal information, in the form of authentication information such as ID/passwords, points and coupons, and enable the information to be read. However, at present, in order to store and use ID information or users information in tamper-resistant devices, it was necessary to develop and operate an application for mobile phones (hereinafter, "mobile app") for each service provider. Also, users need to download and install separate mobile apps provided by service providers. In other words, both service providers and users face inconvenience when a tamper-resistant service is provided (Figure 16). For the purpose of creating an environment convenient for users, in which it is easy for service providers to provide and operate, we examined technical specifications to realise the mobile access system.

Figure 16: Separate application for each service provider in a tamper-resistant device



In order to resolve the difficulties mentioned above, system, that users and service providers alike could commonly utilise, was studied. In other words, it was studied the technical specifications of a mobile access system consisting of servers for storage and safe reading instead of each service provider and a mobile app utilised commonly for every service to store and use ID information in tamper-resistant devices (Figures 17 and 18).

Figure 17: Common application and unified mobile access server for all service providers

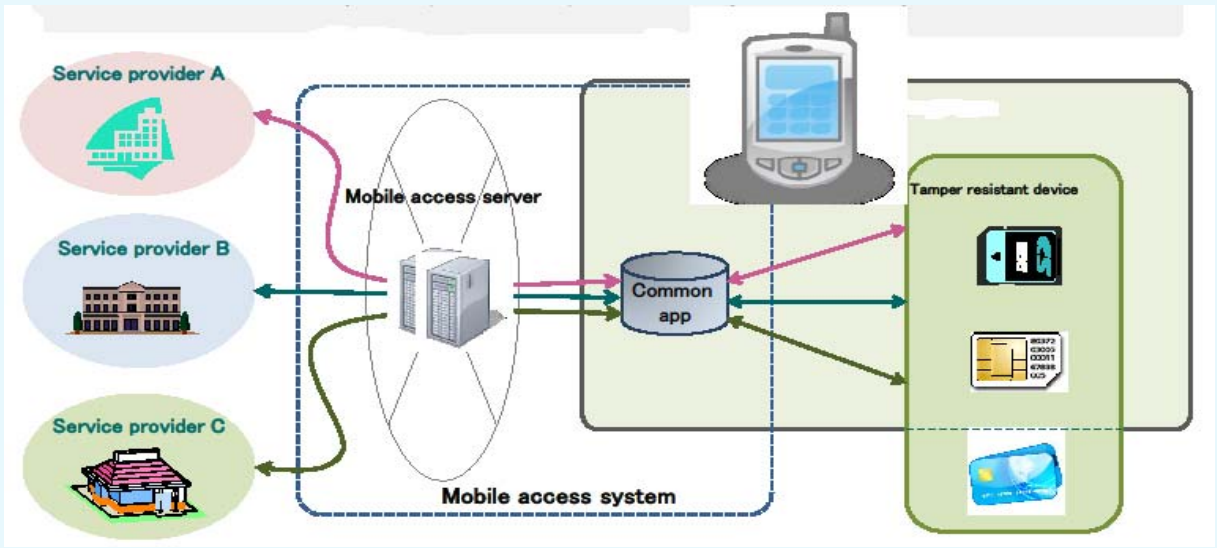
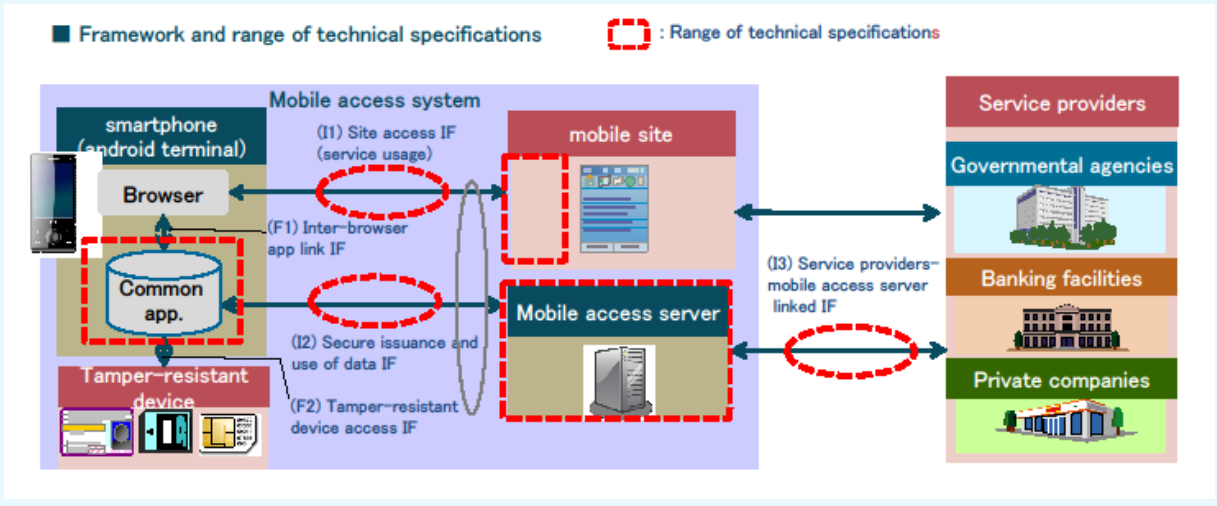


Figure 17: Common application and unified mobile access server for all service providers. Further, verification by experimentation with technical specifications etc. was studied. In other words, **A:** Examination of technical specifications for a mobile access system realising online storage and use of ID information and **B:** Based on the examination results of issue A, construction of an experimental environment, inspection of operability and user-friendliness from the viewpoint of both service providers and users, and verification of technologies.

Figure 18: Technical specifications for structure with common application



The outcomes on the difficulties mentioned above, A and B, are listed below.

A: Multiple service providers which perform writing and reading of ID information into and from tamper-resistant devices have established technical specifications for a mobile access system composed of a common app by integrating a mobile access server that securely sends and receives ID information with a browser. With respect to ID information, established technical specifications for handling are not only e-certificates but optional information, such as other members' IDs, ticket information, etc. with a common method. To be compatible with various access methods depending on service providers, established the technical specifications that permit a common method (common protocol/API) of applicable to any of the public IC card system (IC card), public card system for mobile phones (flash memory type device) or Universal Integrated Circuit Card (UICC).

B: Used a mobile access server and common app within mobile terminals examined in issue A, constructed a demonstrative environment assuming virtual service operated on them, conducted function evaluation, performance evaluation, and evaluation by the users. The function evaluation revealed that the system examined in issue A had sufficient functions. The performance evaluation achieved performance measurement of the operation of the system using mobile terminals and confirmed that writing of ID information and point information in about 6 seconds was possible. The evaluation by the users consulted with service providers and users and confirmed the operability, effectiveness, and usability of the mobile access system.

Examples of the utilisation image of mobile access systems are: (1) writing ID information for certificates to mobile terminal-tamper resistant devices, (2) applying the administration for a certificate through a mobile terminal online, (3) holding a mobile terminal over the ministerial kiosk terminal (multi-copy machine) of installed at convenience stores and administrative bodies to receive a printed certificate. Another example is (1) holding the user's mobile terminal over the mobile terminal of healthcare personnel, (2) after authentication, user's information (history of diagnosis and prescription) of is enabled to be displayed on the mobile terminal of the healthcare personnel.

In order to realise the services above, further experimental studies for overcoming technical difficulties will be conducted. The main topics for consideration in the future in light of the technology are methodologies of authentication of the issuing terminal when storing the ID information, such as an e certificate, etc. and scheme such as a mobile access system, considering the way of exchanging ID information between mobile phones and outer terminals, through local communication.

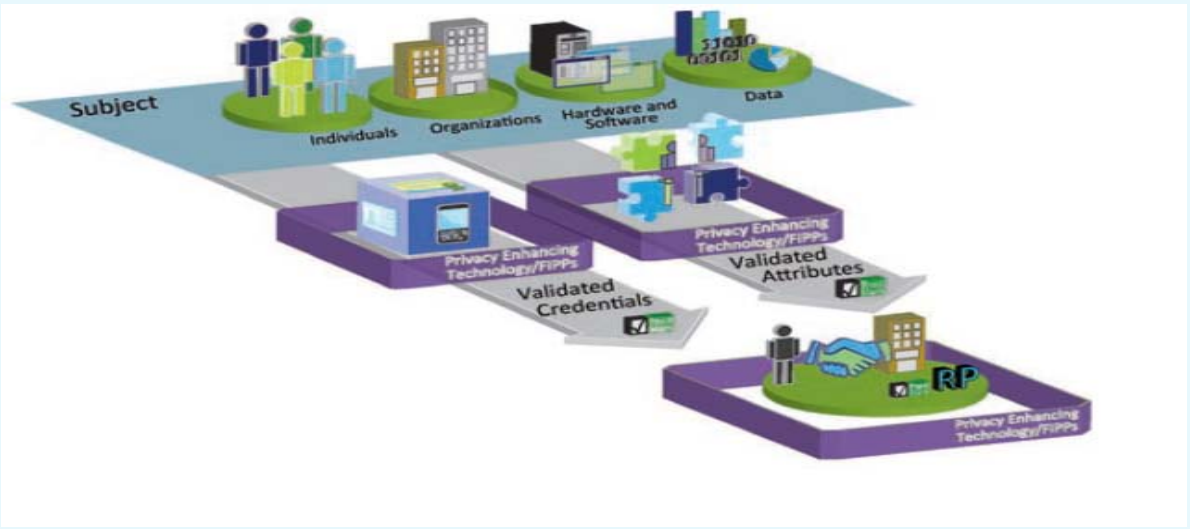
9 United States of America National Strategy for Trusted Identities in Cyberspace (NSTIC)

Individuals have limited ability to use strong digital identities across multiple applications, because applications and service providers do not use a common framework. Instead, they face the increasing complexity and inconvenience associated with managing the large number of usernames, passwords, and other identity credentials required to conduct services online with disparate organisations. Finally, collection of identity-related information across multiple providers, coupled with the sharing of personal information through the growth of social media, increases the opportunity for data compromise. For example, personal data that individuals use as "prompts" to recover lost passwords (mother's maiden name, name of a first pet, etc.) is often publicly available or easily obtained.

That is why the US National Strategy for Trusted Identities in Cyberspace (NSTIC) of was created by the White House in April 2011. The strategy's vision consists of the following: individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice and innovation. It offers the idea of the Identity ecosystem (Figure 19), where users can authenticate themselves at any service provider (relying party)f by their IDP using strong digital identities (for example: digital signature in a SIM card). In some cases relying party needs to confirm some characteristic inherent to the subject (for example, "this individual's age is at least 21 years"), retaining anonymity of the User. Such information can be asserted by the Attribute

provider – an organisation, responsible for the processes associated with establishing and maintaining attributes of the subject.

Figure 19: NSTIC ecosystem



The Identity Ecosystem will increase the following:

– Privacy protection for individuals, who will be assured that their personal data is handled fairly and transparently;

– Convenience for individuals, who may choose to manage fewer passwords or accounts than they do today;

– Efficiency for organizations, which will benefit from a reduction of paper-based and account management processes;

– Ease-of-use, by automating identity solutions whenever possible and basing them on technology that is simple to operate;

– Security, by making it more difficult for criminals to compromise online transactions;

– Confidence that digital identities are adequately protected, thereby promoting the use of online services;

– Innovation, by lowering the risk associated with sensitive services and by enabling service providers to develop or expand their online presence;

– Choice, as service providers offer individuals different—yet interoperable—identity credentials and media.

The logical step in the development of this ecosystem is the presence of the Authentication Provider Agregators that connect to many attribute providers and identity providers and provide a single interface to all of them.

10 Case study mobile payment in Poland

Today many equal mobile payments with NFC payment, this is not really right though NFC is one of many pairing methods to get information from the payer to the payee. Also a payment using NFC is covering one payment situation, pay at POS. A Polish bank has commercially launched a mobile payment service that includes all payment situations. The solution is unique in that it covers all payment situations, doesn't need any new hardware (ex. no need for a Secure Element), is operator independent, use the existing payment eco-system without the need of adding new players and can be used with any pairing technology (ex. NFC, RFID, QR-codes and barcodes). The roll-out includes all the bank's ATMs and very many POS-terminals. From start the mobile payment service supports:

– Point of Sale (POS) - pay in store, at restaurants, etc. (including future support for NFC)

– Online - pay at online stores

– P2P - real-time money transfer person-to-person to beneficiaries identified only by their telephone number

– Cardless cash withdrawal from ATMs

– Money vouchers – offline timed vouchers for shopping payments and ATM cash withdrawals

– Information services

Later on more payment situations can easily be added, though the same method and processes are used:

– Person-to-machine (ex. vending, parking, petrol, etc.)

– inApp payment

– mCommerce

– mPOS

More services like mobile ticketing, loyalty, coupons and gift cards can easily be added to mobile service and based on the same technology.

The Mobile payment service is available on all mobile platforms; Android, iOS, BlackBerry, Java (feature phones) and Windows Mobile/Phone.

The service uses a connected mobile device and the user is online authenticated to the issuer of the payment service. At the authentication a number of checks are performed; exchange of key's (PKI implementation), right unique application number and tied with IMEI (serial number of mobile), MSISDN (telephone number) and approved by user PIN. After successful authentication the payment transaction is performed by user pressing "pay" in his/her mobile app. No sensitive information are stored on the mobile nor transmitted during the payment transaction.

The user process step-by-step, example (POS)

1. Open mobile payment app (can be set with or without PIN)
2. Choose pay and for example swipe mobile at POS-terminal (an OTT is shown on the mobile and transferred to the merchant)
3. Approve payment in app with PIN (can be set without need of OK or OK+PIN for low value transactions)
4. Receipt printed

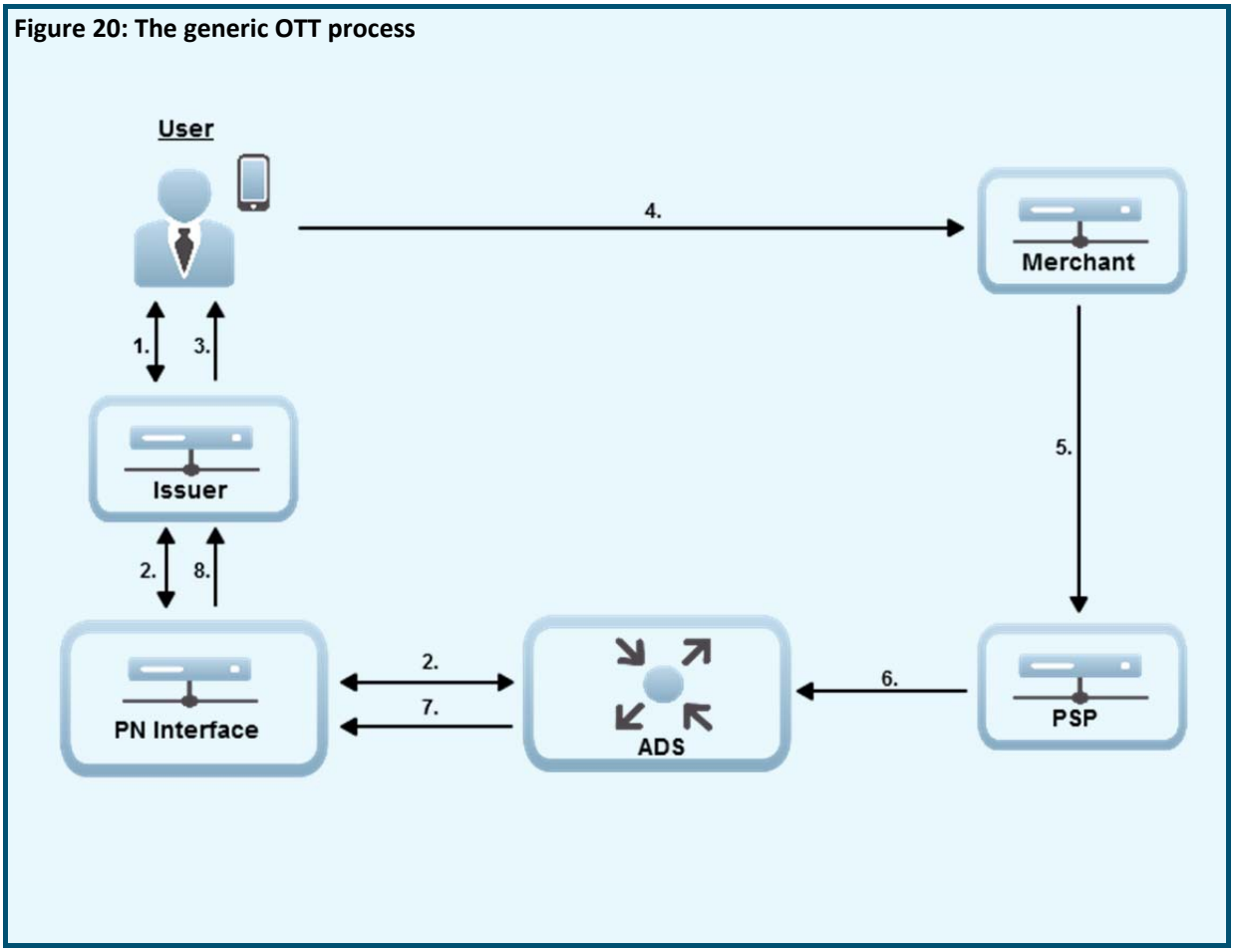
The payment generic process step-by-step (technical)

In the Polish bank case the ADS (active discovery service) is at the bank in a closed loop system, where the bank also act as Payment Network (PN) and Payment Service Provider (PSP). Figure 20 below shows an ADS outside the bank and that give the opportunity for an open technology standard for mobile payment

in for example a country or region. The different players in the payment eco-system (issuers, payment networks, payment service providers/merchants) are connected once and can then use different mobile payment services from different issuers only by adding a commercial agreement.

An OTT is a One-Time Ticket that is generated by the ADS upon request from the issuer inside a payment network. The OTT is transferred by the user from the mobile device to the merchant's system. By having the security aspects regarding authentication between the issuer and the user instead of between the user and the merchant, the OTT is simply a nonsense code that does not hide any sensitive information. The OTT is matched in the ADS with any active OTTs and tied together with the specific user.

Figure 20: The generic OTT process



1. The user starts the application and initial authentication is made between the issuer system and the user's application.
2. An OTT is generated by the issuer through the ADS.
3. The issuer presents the OTT to the user through the mobile application.
4. The user transfers the OTT in the appropriate way (ex. swiping using NFC or NFC-tags, QR- or barcode or just typing it into the POS-terminal or cashier system) to the merchant.
5. The merchant sends the user-provided OTT to the PSP and its back-end system.
6. The PSP receives the OTT and forwards it to the ADS.
7. The ADS matches the OTT with any valid OTTs in the database and routes the status to the appropriate payment network.
8. The necessary details are forwarded to the appropriate issuer inside the payment network.

Lessons learned

– Easy (but secure) registration/enrolment process.

– It must be easy and fast to use and the trick is to get merchants where the service can be used.

– Simple for merchants to sign up and not higher fee's than for a card solution/transaction.

– Adding simple services like receipts, transaction history and balance in the mobile application will gain adoption.

11 Case study in the Russian Federation

Various mobile payment systems have become very popular in the Russian Federation. Some of them, while having minimum functionality limited to top-up the balance of previously registered mobile phone, do not require security and, respectively, do not provide it, the others (for example, mobile payment systems "Easy payment" and "MasterCard Mobile"), have wide functionality and meet the highest security level requirements, set forward by ITU standards to secure systems. Thus, and this is very important, security means do not invoke any additional inconveniences for users. All the diversity of means presented by modern mobile communication standards is used as transport environment. SMS and USSD have become quite wide spread, however, due to wide circulation of smartphones and development of standards for mobile telecommunication systems, increased the use of GPRS, UMTS, WiMax and LTE.

It is interesting to note, that in the market under equal conditions are present both applications with "sensitive information" stored on tamper resistance devices, and applications with the data stored in the phone's memory. Nevertheless, the latter have become more popular, yet they are potentially less secure. Obviously, the consumer benefit of the latter is that he does not need to change his SIM/UICC card. Yet, risk of reading the confidential data from phone's memory is a shortcoming. With respect thereto, it is interesting to compare these two types of applications from the point of security.

According to statistics, fraud usually takes place not when applications on stolen phones are hacked, but either because of the "human factor", or virus programs penetrated into clients' phones. And this is the least protected system elements that require further increase of security of mobile applications only in case of very high risks of being hacked, for example, for the official digital signature recognized by state entities. Unlike it, risks of payment systems can be limited by the maximum amount of financial transaction per transaction and/or a time period. Therefore, the most important role in secure usage of devices working in open networks consists of training clients to use these devices, and to use anti-virus programs. Thus, certainly, the service provider should take all measures to protect confidential information, defined by ISO 27001 and other similar standards. In particular, it is necessary to minimize amount of employees operating the system, who have access to "sensitive data", to assign different access levels to the system, and to provide mandatory authentication and login registration.

In Russia, as well as in other countries, all three MPS models, described in Section 4.3 above, have become popular and all sources of payment described in Section 4.4 are used, namely: clients bank accounts, international and local payment cards, personal accounts of subscribers of cellular communication, and e-money.

Use of mobile devices for providing legally recognized digital signature in Russia is aggravated by Russian requirements to its cryptographic protection and is not introduced yet; however, Rostelecom has been dealing with this issue for a long time and intends to implement it in nearest time.

12 Findings

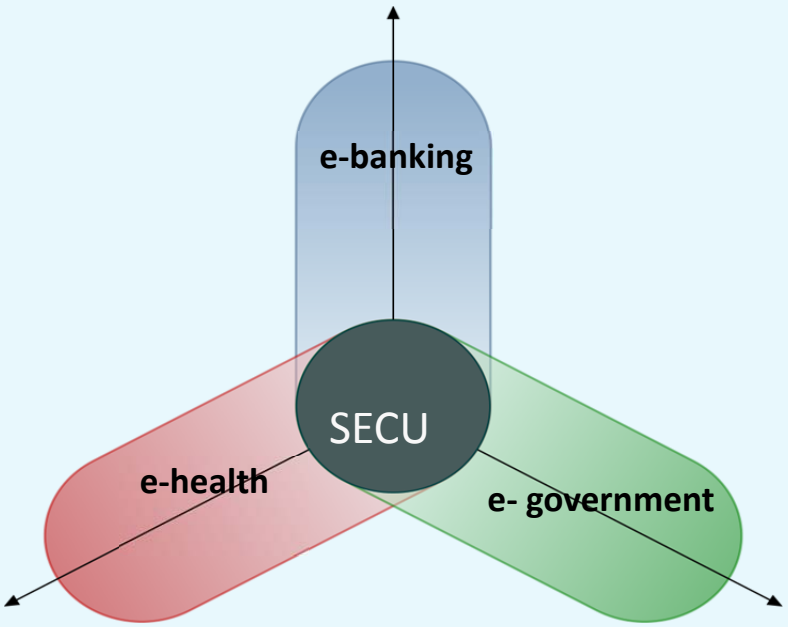
As shown in implementation cases described in chapters 6-9 above, development and usage of mobile devices for *m-Government, m-Health, m-Payment, m-Learning and so on* are at different levels in various countries, however, in today's global world the penetration of technology innovations increases drastically, that leads to step-by-step convergence of technological development levels and reduces digital gap between developed and developing countries. Today the developed countries already have fully functional electronic payment systems and mobile government, and in some developing countries even simple use of SMS to transfer the data between medical offices brings real results, reducing delays in receiving early infant diagnosis (EID) DBS HIV test results as it was described in the Project MWANA implemented in the Republic of Zambiya[17]. This proves that very soon this technological gap will be decreased. The most advanced today's systems which are based on mobile devices offer the whole range of services which is continuously extended. So, beside mobile payments and mobile banking services, wide application was received by services based on geo-location. Besides, it is stated at White Parer Mobile Payments[18], issued by European Payments Council in 2012, the mobile terminal should represent a "digital wallet" which will provide authentication and digital signature to replace multiple passwords, IDs and loyalty cards of merchants (Figure 21).

Figure 21: The wallet shall be digital, not leather

As a normal wallet, the "digital" wallet, in effect, contains identification data of the owner, data on means of payment available to the owner, and in certain cases - personal data of the owner (images, documents, etc.). It may include ID information, digital signatures and certificates, login information, addresses for drawing of scores and transmission, and also information on means of payment. Besides, it can also include other applications, for example bonus points, tickets or travel documents. After having passed authentication in Unified Centre, one may enter personal merchant accounts or social networks, such as Facebook, LinkedIn, etc., which is very convenient and relieves from the need to remember or to store securely numerous passwords of multiple accounts. In the short term, one can expect active distribution of mobile devices as terminals for e-government and healthcare. Recent initiatives in the use of mobile devices, launched at Telecom-2012 by the ITU and WHO, are to prove this statement.

So rapid development of systems based on mobile devices is due to security measures applied to services. Security is a common task for e-government, financial services and e-health (Figure 20) and is provided with observance of ITU-T recommendations for security.

Figure 22: Security – touchstone for all e-services



Due to these recommendations, cryptography has been implemented to use for authentication and encoding of transferred data instead of one-time passwords used in previous systems, that considerably increased security of mobile devices and at the same time increased convenience of their use and, as a result, led to growth of popularity of services based on mobile devices.

13 Recommendations

– Since mobile phones have achieved full market penetration and high service levels, they are the ideal payment terminals and secure communication instruments.

– It is important to provide easy-to-use mobile phone interfaces with consistent user experience across all supported mobile phone implementations, even if the most advanced smart phones boast "great" colour displays and touch-based interfaces. The user experience remains strongly challenged by necessarily small form factor. For example, the mobile phone form factor effectively limits the amount of information that can be displayed at any given time and the ability of the user to enter complex text.

– Mobile device is a "digital wallet", to store identification information on the wallet holder, on payment instruments – accessible to the wallet holder and optional personal information items belonging to the holder (e.g., pictures, documents, etc.). This may include information related to ID cards, digital signatures and certificates, logon information, billing and delivery addresses as well as payment instrument related information. Furthermore, it may also include other applications such as loyalty, transport or ticketing.

– It is advised that the Customers should not be bound to a specific MNO or Bank, and should retain their current ability to choose service providers.

– Parties of electronic dialog should be authorised with the use of at least two-factor authentication, and data transfer should be executed in secure mode using cryptography means.

– It is advised to use Security Lelel 4 or 3 according to Y.2740 ITU-T Recommendation.

- Customers should be aware of the Security Level of the System, which should be stipulated in the participants' agreement. User authentication may be performed by the Unified centre of authentication.
- To ensure the security, the mobile device must have a special Mobile Application, which provides authentication and encryption.
- The most realistic vision is one of a market where multiple Mobile Applications co-exist, combining services on a single mobile device.19
- The registration and provisioning of a Mobile Application needs to be executed in secure environment. Access to a Mobile Application would be easier for customers, if they could use existing trusted relationship between them and their service providers.
- To reach the highest security level, Mobile Application should be located on the hardware Security Element.
- The choice of Security Element has a major impact on the service model and roles of various stakeholders. There are three types of SEs used until now: UICC, embedded SE and removable SE, such as micro SD card.
- Service Enabler provides the technology support and integration of various access means, interoperability with service providers and authentication centre.
- It is recommended to use Mobile Applications with several independent blocks with different sets of keys.
- The Client may have multiple customer mobile identities – mIDs, bounded to the Client's MSISDN. Unified rules to issue mIDs, registered within the System Central Directory, should be introduced to ensure proper routing of messages to Clients.
- All identification and authentication centres must comply with the same allocation rules and regulations for mobile identifiers of mobile clients (mID), registered in a central System Directory to ensure message delivery to customers.
- Mobile systems should, as much as possible, use technologies and infrastructure which have been already widely deployed.

14 Terms and abbreviations

ADS	Active Discovery Services
CA	Certification Authority
CPU	Central Processor Unit
CSD	Circuit Switched Data
DNS	Domain Name System
DTMF	Dual-Tone Multi-Frequency
EDGE	Enhanced Data for GSM Evolution
EU	European Union
G2B	Government-to-Business
G2C	Government-to-Citizens
G2E	Government-to-Employees
G2G	Government-to-Government
GLONASS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
ICT	Information and Communication Technology
IDM	Identity Management
IP	Internet Protocol
ITU	International Telecommunication Union
LTE	Long Term Evolution
mID	mobile Identificator
MNO	Mobile Network Operator
MPS	Mobile Payment System
MSISDN	Mobile Subscriber Integrated Services Digital Number
MSSP	Mobile Signature Service Provider
NCD	Non-communicable disease
NFC	Near Field Communications
NGN	Next Generation Networks
NIST	National Institute of Standards and Technology (USA)
NSTIC	National Strategy for Trusted Identities in Cyberspace (USA)
OTA	Over-The-Air
OTP	One Time Password
OTT	One Time Ticket
PIN	Personal Identification Number
PKI	Public Key Infrastructure

PN	Payment Network
PSP	Payment Service Provider
QoS	Quality of Service
RA	Registration Authority
ROI	Return On Investment
RSA	an algorithm for public-key encryption
SIM	Subscriber Identification Module
SMS	Short Message Service
TEE	Trusted Execution Environment
UICC	Universal Integrated Circuit Card
UNO	United Nations Organisations
USA	United States of America
USSD	Unstructured Supplementary Service Data
VPN	Virtual Private Network
WHO	World Health Organisation
WiMAX	Worldwide Interoperability for Microwave Access
WPKI	Wireless Public Key Infrastructure

15 List of References

1. ITU-T Recommendation Y.2740 (page 3)
2. Joint ITU-WHO initiative on NCD(page 6)
3. eEurope "Blueprint" Smartcard Initiative (page 7)
4. NIST Special Publication 800-57 (page 7)
5. ITU-T Recommendation Y.2741 (page 8)
6. Security in telecommunications and information technologies (page 12)
7. ITU-T Recommendation X.805 "Security Architecture for Systems Providing End-to-End Communications (page 12)
8. ITU-T Recommendation X.800 "Security architecture for Open Systems Interconnection for CCITT applications (page 12)
9. ITU Recommendation X.1122 (page 14)
10. Mobile Signatures Whitepaper: Best Practices (page 18)
11. ETCI TR 102 203 "Mobile Commerce (M-COMM); Mobile Signature; Business & Functional Requirements" (page 19)
12. ETCI TS 102 204 "Mobile Commerce (M-COMM); Mobile Signature; Web Service Interface" (page 19)
13. ETCI TR 102 206 "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework" (page 19)
14. ETCI TS 102 207 "Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services" (page 19)
15. Ministry of Internal Affairs and Communications (2012) “Information and communications in Japan, White Paper 2012,” p333 (page 23)
16. Ministry of Internal Affairs and Communications (2012) “Final Report from ‘Study Group on Information Security Issues of Smartphone and Cloud Computing,’” June 29,2012 http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/120629_03.html (page 23)
17. Project MWANA, Zambia D10-SG02-C-0215 http://www.itu.int/md/meetingdoc.asp?lang=en&parent=D10-SG02-C&question=Q17-3/2
18. “White paper. Mobile payments”, 2012. http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=564
19. A Series of White Papers on Mobile Wallets
20. http://vanha.mobeyforum.org/Knowledge-Center/Mobey-White-Papers
21 PKO Project brief http://www.mynewsdesk.com/se/pressroom/accumulate/document/view/mobile-payment-systems-brief-iko-mobile-payment-service-28292
22. PKO Bank Polski mobile payment use case http://www.youtube.com/playlist?list=PL5xZmvvYELkUOr2a2BuIorS7NPXa17tuY
23. http://www.accumulate.se

_____

Union internationale des telecommunications (UIT)
Bureau de développement des télécommunications (BDT)
Bureau du Directeur
Place des Nations
CH-1211 Genève 20 – Suisse
Courriel: bdtdirector@itu.int
Tél.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Adjoint au directeur et
Chef du Département de
l'administration et de la
coordination des opérations (DDR)
Courriel: bdtdeputydir@itu.int
Tél.: +41 22 730 5784
Fax: +41 22 730 5484

Département de l'environnement
propice aux infrastructures et
aux cyberapplications (IEE)
Courriel: bdtiee@itu.int
Tél.: +41 22 730 5421
Fax: +41 22 730 5484

Département de l'innovation et des
partenariats (IP)
Courriel: bdtip@itu.int
Tél.: +41 22 730 5900
Fax: +41 22 730 5484

Département de l'appui aux projets et
de la gestion des connaissances (PKM)
Courriel: bdtpkm@itu.int
Tél.: +41 22 730 5447
Fax: +41 22 730 5484

Afrique

Ethiopie

International Telecommunication
Union (ITU)
Bureau régional
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopie

Courriel: itu-addis@itu.int
Tél.: +251 11 551 4977
Tél.: +251 11 551 4855
Tél.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroun

Union internationale des
telecommunications (UIT)
Bureau de zone de l'UIT
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

Courriel: itu-yaounde@itu.int
Tél.: + 237 22 22 9292
Tél.: + 237 22 22 9291
Fax: + 237 22 22 9297

Sénégal

Union internationale des
telecommunications (UIT)
Bureau de zone de l'UIT
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Sénégal

Courriel: itu-dakar@itu.int
Tél.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe

International Telecommunication
Union (ITU)
Bureau de zone
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

Courriel: itu-harare@itu.int
Tél.: +263 4 77 5939
Tél.: +263 4 77 5941
Fax: +263 4 77 1257

Amériques

Brésil

União Internacional de
Telecomunicações (UIT)
Bureau régional
SAUS Quadra 06, Bloco "E"
11º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Courriel: itubrasilia@itu.int
Tél.: +55 61 2312 2730-1
Tél.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

La Barbade

International Telecommunication
Union (ITU)
Bureau de zone
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Courriel: itubridgetown@itu.int
Tél.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chili

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484 – Plaza de Armas
Santiago de Chile – Chili

Courriel: itusantiago@itu.int
Tél.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

Courriel: ituteguciglapa@itu.int
Tél.: +504 22 201 074
Fax: +504 22 201 075

Etats arabes

Egypte

International Telecommunication
Union (ITU)
Bureau régional
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypte

Courriel: itucairo@itu.int
Tél.: +202 3537 1777
Fax: +202 3537 1888

Asie-Pacifique

Thaïlande

International Telecommunication
Union (ITU)
Bureau régional
Thailand Post Training
Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thaïlande

Adresse postale:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thaïlande

Courriel: itubangkok@itu.int
Tél.: +66 2 575 0055
Fax: +66 2 575 3507

Indonésie

International Telecommunication
Union (ITU)
Bureau de zone
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonésie

Adresse postale:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonésie

Courriel: itujakarta@itu.int
Tél.: +62 21 381 3572
Tél.: +62 21 380 2322
Tél.: +62 21 380 2324
Fax: +62 21 389 05521

Pays de la CEI

Fédération de Russie

International Telecommunication
Union (ITU)
Bureau de zone
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Fédération de Russie

Adresse postale:
P.O. Box 25 – Moscow 105120
Fédération de Russie

Courriel: itumoskow@itu.int
Tél.: +7 495 926 6070
Fax: +7 495 926 6073

Europe

Suisse

Union internationale des
télécommunications (UIT)
Bureau de développement des
télécommunications (BDT)
Unité Europe (EUR)
Place des Nations
CH-1211 Genève 20 – Suisse
Courriel: eurregion@itu.int
Tél.: +41 22 730 5111

Union internationale des télécommunications
Bureau de Développement des Télécommunications
Place des Nations
CH-1211 Genève 20
Suisse
www.itu.int

Imprimé en Suisse
Genève, 2014

01/2014