INFORME FINAL

UIT-D COMISIÓN DE ESTUDIO 2

CUESTIÓN 17-3/2

ADELANTOS DE LAS ACTIVIDADES DE CIBERGOBIERNO E IDENTIFICACIÓN DE ESFERAS DE CIBERGOBIERNO EN BENEFICIO DE LOS PAÍSES EN DESARROLLO

5.° PERIODO DE ESTUDIOS 2010-2014
Sector de Desarrollo de las Telecomunicaciones

CONTACTO

Sitio web:	www.itu.int/ITU-D/study_groups
Librería electrónica de la UIT:	www.itu.int/pub/D-STG/
Correo electrónico:	devsg@itu.int
Teléfono:	+41 22 730 5999

CUESTIÓN 17-3/2:

Adelantos de las actividades de cibergobierno e identificación de esferas de cibergobierno en beneficio de los países en desarrollo

Comisiones de Estudio del UIT-D

Para apoyar el programa de divulgación de conocimientos y creación de capacidades de la Oficina de Desarrollo de las Telecomunicaciones, las Comisiones de Estudio del UIT-D ayudan a los países a alcanzar sus objetivos de desarrollo. Las Comisiones de Estudio del UIT-D, que actúan de catalizador creando, compartiendo y aplicando conocimientos de las TIC para reducir la pobreza y propiciar el desarrollo socioeconómico, contribuyen a crear condiciones propicias para que los Estados Miembros utilicen los conocimientos y alcancen más fácilmente sus objetivos de desarrollo.

Plataforma de conocimientos

Los resultados aprobados en las Comisiones de Estudio del UIT-D, así como el material de referencia conexo, se utilizan para implementar políticas, estrategias, proyectos e iniciativas especiales en los 193 Estados Miembros de la UIT. Esas actividades también permiten aumentar el acervo de conocimientos compartidos entre los Miembros.

Centro de intercambio de información y divulgación de conocimientos

Los temas de interés colectivo se comparten en reuniones físicas, foros electrónicos y reuniones con participación a distancia en una atmósfera propicia al debate abierto y el intercambio de información.

Acervo de información

Los Informes, directrices, prácticas idóneas y Recomendaciones se elaboran a partir de las contribuciones sometidas por los miembros de los Grupos. La información se reúne en encuestas, contribuciones y estudios de casos, y se divulga para que los miembros la puedan consultar fácilmente con instrumentos de gestión de contenido y publicación web.

Comisión de Estudio 2

La CMDT-10 encargó a la Comisión de Estudio 2 que estudiara nueve Cuestiones en los ámbitos de desarrollo tecnológico y de infraestructura de la información y la comunicación, telecomunicaciones de emergencia y adaptación al cambio climático. La labor se concentró en métodos y planteamientos más adecuados y satisfactorios para la prestación de servicios en los ámbitos de planificación, desarrollo, aplicación, explotación, mantenimiento y sostenibilidad de servicios de telecomunicaciones/TIC que optimizan su valor para los usuarios. Esta labor se concentraba especialmente en las redes de banda ancha, las radiocomunicaciones y telecomunicaciones/TIC móviles para las zonas rurales y distantes, las necesidades de los países en desarrollo en materia de gestión del espectro, la utilización de las telecomunicaciones/TIC para mitigar las consecuencias del cambio climático en los países en desarrollo, las telecomunicaciones/TIC para la mitigación de catástrofes naturales y para operaciones de socorro, la realización de pruebas de conformidad y compatibilidad y las ciberaplicaciones, con enfoque y acento particulares en las aplicaciones basadas en las telecomunicaciones/TIC. También se estudió la aplicación de la tecnología de la información y la comunicación, teniendo en cuenta los resultados de los estudios realizados por el UIT-T y el UIT-R y las prioridades de los países en desarrollo.

La Comisión de Estudio 2, junto con la Comisión de Estudio 1 del UIT-R, también se ocupan de la Resolución 9 (Rev.CMDT-10) relativa a la "participación de los países, en particular los países en desarrollo, en la gestión del espectro".

En la elaboración del presente informe han participado muchos voluntarios, provenientes de diversas administraciones y empresas. Cualquier mención de empresas o productos concretos no implica en ningún caso un apoyo o recomendación por parte de la UIT.

Índice

Página

1 Introducción 1

1.1 Revolución de la TIC y desarrollo de las aplicaciones de Internet 1

1.2 Cibergobierno y la CE 2 de la UIT 1

1.3 Estudios comparativos sobre cibergobierno en las organizaciones internacionales 2

2 Principios de cibergobierno 3

2.1 ¿Qué se entiende por cibergobierno? 3

2.2 Tendencias de la evolución de las TIC aplicadas al cibergobierno 3

2.2.1 Características de las TIC aplicadas al cibergobierno 3

2.2.2 Comparación entre sistemas fijos y sistemas móviles 4

2.2.3 Dispositivos móviles y tecnologías sociales 4

2.2.4 Datos públicos abiertos como tendencia para una administración pública centrada en los principios de transparencia, responsabilidad, participación y colaboración 5

2.3 Componentes del cibergobierno 6

2.3.1 Portal, intercambio de información, seguridad 6

2.3.2 Redes, capacidades humanas 7

2.4 Categorías de actividades relativas al cibergobierno 7

2.4.1 Aplicaciones: servicios G2G, G2C y G2B 7

2.4.2 Financiación 8

2.4.3 Disposiciones jurídicas e institucionales 8

3 Prácticas óptimas aplicados por los Estados Miembros (contribuciones a los trabajos del UIT-D) 9

3.1 Proyecto INV (Information Network Village, *Aldeas de la red de información*) (República de Corea) 9

3.2 Sistema coreano de compras del sector público en línea (KONEPS) (República de Corea) 10

3.3 En camino del cibergobierno (Uganda) 11

3.4 Implantación de la conectividad de banda ancha en zonas desfavorecidas en Uganda (Uganda) 12

3.5 Sistema de información del gobierno local (LGIN) 14

3.6 Panorama general de los servicios TIC en Bangladesh 15

3.7 Implantación del cibergobierno en la República Kirguisa – Experiencia y próximas etapas 16

3.8 Actividades encaminadas a facilitar el acceso a sistemas administrativos con terminales móviles gracias a la cooperación entre servicios en Japón 17

3.9 Cibergobierno en el Líbano 18

3.10 MWANA (Zambia) 19

3.11 Servicio de cibergobierno en Montenegro 20

Página

4 Herramientas para prácticas óptimas 21

4.1 Conjunto de herramientas para servicios TIC utilizando comunicaciones móviles 21
4.1.1 Principios aplicados a la seguridad de los servicios móviles 22
4.1.2 Identificación y autenticación 22
4.1.3 Administración de claves 23
4.1.4 Seguridad 23
4.1.5 Tecnología móvil 25
4.1.6 Conclusiones 26
4.1.7 Recomendaciones 26

4.2 Evaluación de la eficacia del cibergobierno y su incidencia en Corea (República de Corea) 28
4.2.1 Introducción 28
4.2.2 Organigrama de la gestión de la eficacia del cibergobierno 28
4.2.3 Orientaciones futuras 29

4.3 eGovFrame: Plataforma de innovación abierta 29
4.3.1 Panorama general 29
4.3.2 Antecedentes del marco informático eGovFrame 30
4.3.3 Estrategia de innovación abierta 30
4.3.4 Cambios y ventajas de eGovFrame 33
4.3.5 Futura expansión de eGovFrame móvil 34
4.3.6 Oportunidades para otros países 34

5 Ámbitos de aplicación en beneficio de países en desarrollo 35

5.1 Directrices relativas a la identificación de ámbitos de aplicación 35

5.2 Infrastructuras 36

5.3 Servicios G2G 36

5.4 Servicios G2C y G2B 36

6 Factores que garantizan el éxito de las actividades de cibergobierno 36

6.1 Liderazgo presidencial (Apoyo político) 36

6.2 Equilibrio entre la oferta y la demanda de servicios de cibergobierno 37

6.3 Comprensión clara del concepto de cibergobierno 37

6.4 Aliento al compromiso y la participación de los ciudadanos 38

6.5 Innovación en la gestión de recursos de información 38

6.6 Protección de la vida privada y seguridad de los sistemas 39

6.7 Estrategias para la adopción de servicios electrónicos 39

7 Directrices relativas a la promoción de las actividades de cibergobierno y a la identificación de los ámbitos de aplicación del cibergobierno en los países en desarrollo 39

7.1 Esfera de acción 39

7.2 Objetivo de las Directrices 39

Página

7.3 Directrices para la identificación de los ámbitos de aplicación en beneficio de los países en desarrollo 40

7.4 Directrices para asegurar el buen avance de las actividades de cibergobierno 40

Annexes

Annex 1: Full Transcripts of contributed cases 45

Annex 2: Toolkit to create the ICT-based services using the mobile communications for e-government services 94

Figuras y cuadros

Figure 1: Workflow of e-government Performance Management 28

Figure 2: Open Innovation Strategy Open sourcing 31

Figure 3: To-be image of eGovFrame 31

Figure 4: Evaluation and final selection of open source Open processes 32

Figure 5: Many stakeholders of eGovFrame 32

Figure 6: Vision and strategies of eGovframe 33

Figure 7: eGovFrame 2.0 34

Cuadro 1: Países que han adoptado eGovFrame 35

CUESTIÓN 17-3/2

Adelantos de las actividades de cibergobierno e identificación de esferas de cibergobierno en beneficio de los países en desarrollo

1 Introducción

1.1 Revolución de la TIC y desarrollo de las aplicaciones de Internet

"Todo cambia con Internet." Esta expresión sintetiza en líneas generales los cambios fundamentales que han aportado las TIC, en particular la tecnología Internet. El avance de las TIC, su difusión y su aplicación a gran escala han influido en todos los aspectos de la sociedad. Se habla de revolución de las TIC. Una sociedad que ha cambiado a raíz de la revolución de las TIC recibe el nombre de sociedad de la información. Concretamente, la revolución de las TIC consiste en el proceso de transformación, el surgimiento de la sociedad de la información y la influencia en diversos ámbitos, en particular los servicios públicos y las empresas. Internet ha transformado totalmente la manera en que las administraciones públicas prestan servicios al público y a las empresas en general. El interés acordado a las aplicaciones TIC en numerosos países refleja la convicción de las autoridades gubernamentales y los ciudadanos de que las tecnologías que sirven de base al cibergobierno constituirán fuerzas poderosas para mejorar la eficacia de la administración y facilitar la prestación de servicios al público, dando lugar a una ventaja en el plano de la competitividad en el contexto de la sociedad de la información.

1.2 Cibergobierno y la CE 2 de la UIT

En el marco del Programa 3 del UIT-D se han llevado a cabo estudios relativos a aplicaciones de cibergobierno, en especial sistemas modernos para el acceso y pago de servicios, en colaboración y asociación con el sector privado y otras organizaciones del sistema de las Naciones Unidas. Para sacar partido de los posibles beneficios de las aplicaciones de cibergobierno, los países en desarrollo necesitan información sobre estrategias, prácticas óptimas, fuentes de conocimientos especializados y apoyo financiero, así como sobre el tipo de aplicaciones de cibergobierno y plataformas tecnológicas que serán más útiles para sus ciudadanos, teniendo en cuenta las necesidades y capacidades actuales de cada país.
La UIT decidió crear una nueva Comisión de Estudio para las cuestiones relativas al cibergobierno que se refieren principalmente a la evaluación de los avances en las actividades de cibergobierno en el mundo entero y a la identificación de los ámbitos de mayor interés para los países en desarrollo, por ejemplo la utilización de plataformas móviles e inalámbricas para la prestación y el pago de servicios en zonas rurales y aisladas.

El origen de las contribuciones al estudio de la Cuestión es el siguiente: avances en el examen de las Cuestiones que guardan relación con este tema (autenticación, confidencialidad, etc.) realizado por las correspondientes Comisiones de Estudio del UIT-T (CE 13 y 17); progreso de las iniciativas de la BDT con otras organizaciones de las Naciones Unidas y el sector privado relativas a los servicios y aplicaciones de cibergobierno, haciendo hincapié en la participación de los países en desarrollo; avances en todas las demás actividades importantes llevadas a cabo por la Secretaría General de la UIT o la BDT; Informes y estudios de casos presentados por los Estados Miembros y Miembros de Sector sobre iniciativas en materia de aplicaciones o tecnologías elaboradas que podrían ser de utilidad para la prestación de aplicaciones de cibergobierno.

La UIT publicó *e-Government Implementation Toolkit, the e-Government Readiness Assessment Framework* (Conjunto de herramientas para la implantación del cibergobierno: Marco de evaluación de la

preparación para el cibergobierno) (2009). Se examinan en él las dimensiones fundamentales del entorno de cibergobierno con objeto de ayudar a los encargados de adoptar decisiones a identificar las esferas de acción prioritarias, en función de su grado de preparación y de sus estrategias nacionales de desarrollo. La UIT llevó a cabo también un estudio sobre las tecnologías móviles y sus consecuencias para gobiernos con capacidad de respuesta y sociedades conectadas con miras a publicar un informe, "*M-Government*", junto con el Departamento de Asuntos Económicos y Sociales de las Naciones Unidas (UNDESA) y la OCDE (2011). El Informe, que destaca las posibilidades esenciales de las tecnologías móviles para mejorar la gestión pública, analiza en profundidad los requisitos previos de un gobierno móvil, sus principales ventajas y dificultades, describe la cadena de valores y los principales interesados, y enumera una lista de medidas concretas para ayudar a los responsables de definir políticas generales a evaluar y poner al día sus conocimientos en materia de gobierno móvil.

1.3 Estudios comparativos sobre cibergobierno en las organizaciones internacionales

La mayoría de organizaciones internacionales, en especial las Naciones Unidas, la OCDE, la UIT, el Banco Mundial y los bancos regionales de desarrollo, como el BAD y BAfD, consideran que los asuntos relativos al cibergobierno constituyen un tema importante en el programa de desarrollo sostenible de los países en desarrollo. Desde 2002, el Departamento de Asuntos Económicos y Sociales de las Naciones Unidas ha llevado a cabo con regularidad una encuesta sobre cibergobierno que trata de evaluar globalmente su nivel de desarrollo y clasificar a los países miembros según el grado de preparación en materia de cibergobierno. Con esa finalidad, las Naciones Unidas han elaborado un modelo de desarrollo de cibergobierno formado por cinco etapas muy claras, destacada cada una de ellas por importantes indicadores.

A principios de 2000, la OCDE estableció un grupo de trabajo sobre cibergobierno, y publicó dos libros, uno en 2003 (*La administración electrónica: un imperativo*) y otro en 2004 (*e-Gobierno para un mejor gobierno*), que tratan temas fundamentales al respecto. Ambos libros han sido acompañados por una serie de estudios nacionales sobre cibergobierno, entre ellos los de Finlandia (2003), México (2004), Noruega (2005), Hungría (2007), Países Bajos (2007) y Turquía (2007), donde se han examinado el nivel de desarrollo del cibergobierno y los esfuerzos desplegados para su instauración con objeto de formular recomendaciones en materia de política. El estudio de la OCDE sobre cibergobierno prosiguió con la realización de investigaciones temáticas que dieron lugar a publicaciones como las siguientes: "*Benefits Realization Management*" y "*E-Government as a Tool for Transformation*" en 2007, y "*An Economic Framework to Assess the Costs and Benefits of Digital Identity Management Systems for E-Government Service*" en 2009.

Las actividades del Banco Mundial sobre cibergobierno dan prioridad a la prestación de ayuda a los países clientes destinada a crear las capacidades institucionales necesarias para la elaboración de aplicaciones de cibergobierno con objeto de mejorar el desempeño y la rendición de cuentas de las autoridades gubernamentales, en particular en lo que concierne a la prestación de servicios públicos. El Departamento Mundial de las TIC del Banco Mundial proporciona asesoramiento técnico y apoyo a la inversión para la concepción y puesta en marcha de soluciones y aplicaciones de cibergobierno. Entre ellas pueden mencionarse estrategias, políticas, aspectos reglamentarios y jurídicos, marcos institucionales, arquitecturas de empresa y normas de interfuncionamiento, infraestructuras y servicios de uso común, gestión de la formación y del cambio, aplicaciones de cibergobierno y mecanismos de financiación innovadores, como las asociaciones público-privadas. Reciben ayuda del Banco Mundial países como Túnez, Mongolia, Ghana y Rwanda.

2 Principios de cibergobierno

2.1 ¿Qué se entiende por cibergobierno?

Creado a principios de 1990, el concepto de cibergobierno combina dos términos muy heterogéneos. Uno de ellos es sumamente técnico y el otro se utiliza desde hace mucho para referirse al sistema de gobernanza. Aunque al principio el nuevo término no fue fácilmente aceptado, pronto constituyó el objetivo inevitable de la mayoría de los países que tratan de transformar la administración pública en una estructura moderna e innovadora. Según los futurólogos, la transformación de la administración pública dará lugar a un sistema de gobernanza revolucionario.

Organizaciones internacionales como la OCDE y las Naciones Unidas dan una definición de cibergobierno. La OCDE lo define como "la utilización de las tecnologías de la información y la comunicación (TIC), en particular Internet, en tanto que herramienta para lograr una administración de mejor calidad" (OCDE, 2003). Para las Naciones Unidas se trata de una administración pública que aplica las TIC para transformar las relaciones internas y externas. El objetivo final del cibergobierno es establecer una "buena gobernanza", es decir, lograr que la administración pública sea lo más eficaz y práctica posible desde el punto de vista del público en general. Su perspectiva es definir el marco de las TIC para que estas tecnologías constituyan un factor esencial en la adopción acertada de una administración pública clara, transparente y eficaz.

Este concepto apunta esencialmente a transformar la administración pública para que modernice sus relaciones internas y externas con la ayuda de tecnologías electrónicas, lo que indica que se debe poner más el acento en "gobierno" que en "ciber", como señala la OCDE (2003). En este sentido, los asuntos en materia de cibergobierno deben situarse en el contexto de las iniciativas relativas a la reforma de la administración pública y a la buena gobernanza. El cibergobierno no es sólo innovación técnica sino también reforma de la administración pública, centrada en las necesidades del sector público, por una parte, y en los ciudadanos y las empresas, por la otra, asegurando de esa forma que la explotación de las TIC transforma las actividades internas de los órganos gubernamentales y la modalidad de interacción entre el sector público y el sector privado.

Dado que se propone transformar los procesos internos y las relaciones externas con los ciudadanos, el cibergobierno debe ser reconocido como un proceso sometido permanentemente a modificaciones a medida que las funciones de la administración pública evolucionan de acuerdo con los cambios sociales.

2.2 Tendencias de la evolución de las TIC aplicadas al cibergobierno

2.2.1 Características de las TIC aplicadas al cibergobierno

En el mundo de hoy, impulsado por la tecnología, las TIC constituyen el eje central del proceso de transformación de la administración pública. La utilización de las TIC está plenamente instaurada en las administraciones públicas y forma parte de la manera en que realiza sus actividades. La infraestructura de la información y, en particular, la tecnología Internet, se han destacado por su naturaleza, es decir apertura, conexiones, accesibilidad, etc. Por ese motivo, se ha tenido en cuenta en el plano nacional como elemento de esencial importancia para la transformación. Se considera que los asuntos de cibergobierno propician la transformación de las estructuras de la administración pública, y determinan la forma de interacción entre los organismos gubernamentales y los ciudadanos. Por otra parte, las TIC son una herramienta poderosa para lograr una mayor participación de los ciudadanos en la formulación de políticas públicas. La eliminación de las fronteras entre los organismos facilitada por las aplicaciones TIC es fundamental para transformar las estructuras de gobernanza, con el fin de agilizar y simplificar las administraciones públicas y, en ocasiones, suprimir la duplicación de tareas. Asimismo, las TIC mejoran la accesibilidad de la población a los organismos gubernamentales, dando lugar a la participación de los ciudadanos en el proceso de adopción de decisiones.

2.2.2 Comparación entre sistemas fijos y sistemas móviles

En un principio, cuando las TIC fueron aplicadas a la transformación de la administración pública, la mayoría de las iniciativas de cibergobierno se basaban en tecnologías de Internet fijas. Las transacciones por Internet se realizaban en redes de comunicación fijas, que correspondían a una infraestructura nacional de información instalada bajo tierra. El acceso a los servicios de cibergobierno sólo era posible en muy pocos lugares (ciertos domicilios u oficinas) a través de líneas de telecomunicación por cable. Sin embargo, con la gran difusión de las tecnologías móviles[1], el acceso móvil a Internet y el acceso inalámbrico a las administraciones públicas han empezado a tener una considerable repercusión en el entorno del cibergobierno. Las tecnologías móviles refuerzan la capacidad del sector público de aprovechar la utilización de las TIC para mejorar sus operaciones internas, así como su interacción con los ciudadanos y las empresas. Como resultado de ello, el cibergobierno se extiende al gobierno móvil, o evoluciona hacia un nuevo tipo de gobernanza, indicando el surgimiento de aplicaciones TIC de la próxima generación en el sector público.

En los países en desarrollo, el nivel de acceso a la banda ancha fija es más bajo que el nivel de acceso a las tecnologías móviles. Esto se debe al costo elevado de las tecnologías alámbricas y a la infraestructura necesaria para la instalación de Internet de banda ancha fija. Mediante la creación de canales de comunicación nuevos y ampliados, las tecnologías móviles ofrecen acceso en zonas donde la infraestructura necesaria para Internet y el servicio telefónico por cable no es una opción viable (OCDE y UIT, 2011). Dispositivos móvil baratos y listos para ser utilizados están eliminando los obstáculos que afrontan los ciudadanos en zonas donde los servicios de Internet de línea fija solían ser muy limitados.
Pese a que cuando empezaron a utilizarse las redes 2G, se estimaba que la tecnología móvil era un medio insuficiente para acceder a una amplia variedad de información y servicios, los teléfonos inteligentes, gracias a la implantación de redes 3G y 4G, ofrecen oportunidades sin precedentes en materia de servicios públicos facilitados a ciudadanos y empresas. Por otra parte, las tecnologías móviles están mejorando las posibilidades de comunicación en tiempo real entre las administraciones públicas y los ciudadanos, logrando que de esa manera los funcionarios públicos comprendan mejor las necesidades de los ciudadanos y ofrezcan opciones convenientes con gran capacidad de respuesta. Al mismo tiempo, las comunicaciones en tiempo real permiten a los ciudadanos comprender mejor a las administraciones públicas, lo cual aumenta sus posibilidades de participar en el proceso de elaboración de políticas.

2.2.3 Dispositivos móviles y tecnologías sociales

En la evolución de las TIC en relación con las iniciativas de cibergobierno, hay que tener en cuenta las tecnologías sociales, que permiten a las administraciones públicas solicitar a los ciudadanos que formulen comentarios sobre las políticas públicas con objeto de perfeccionarlas. Utilizando medios en línea, como Facebook, Twitter u otros, que los ciudadanos visitan con regularidad, las administraciones públicas toman contacto directo con los ciudadanos y verifican además qué opinan con respecto a las actividades públicas y a los servicios prestados. Cuando las tecnologías sociales se combinan con los dispositivos móviles, sus repercusiones favorecen a las administraciones públicas.

En lugar de responder pasivamente a las peticiones de los ciudadanos, las autoridades públicas pueden participar en las conversaciones que se mantienen en numerosos sitios de contacto social para saber qué dice la gente sobre la calidad de los programas gubernamentales. Si bien al principio el cibergobierno consistía simplemente en suministrar información y responder a demandas de los ciudadanos sobre los servicios públicos a través de las páginas web oficiales, ya no puede limitarse ahora a esperar

[1] El 90% de la población mundial y el 80% de los habitantes de zonas rurales tienen acceso a redes móviles; entre los países de la OCDE, el número de abonados a la banda ancha móvil aumentó, registrándose una tasa de crecimiento anual acumulada del 20% entre 2007 y 2009 (OCDE y UIT, 2011).

pasivamente la formulación de preguntas y reclamaciones de los ciudadanos. El nuevo avance de las TIC hacia las tecnologías sociales ofrece nuevas perspectivas para las iniciativas de cibergobierno.

2.2.4 Datos públicos abiertos como tendencia para una administración pública centrada en los principios de transparencia, responsabilidad, participación y colaboración[2]

En los últimos años, se observa en numerosos países una tendencia a los datos públicos abiertos, cuyo objetivo es la creación conjunta de valor público entre el sector privado, la sociedad civil y los ciudadanos. Este paradigma político se basa en los principios de transparencia, participación y colaboración. Se trata de un cambio cultural que convierte en socios a los poderes públicos, los ciudadanos y otras partes interesadas de la sociedad. Los valores esenciales de los datos públicos abiertos pueden resumirse de la siguiente manera: i) Transparencia: Las administraciones públicas deben ofrecer a los ciudadanos información sobre las actividades que realizan, para garantizar una gobernanza responsable; ii) Participación: Las administraciones públicas deben solicitar asistencia y consultar con todos los sectores de la sociedad para formular políticas teniendo en cuenta las informaciones más óptimas, iii) Colaboración: Los funcionarios públicos deben colaborar con los ciudadanos y el sector privado en el marco de su labor de resolución de problemas a nivel local y nacional.

La sociedad de la información modifica los puntos de vista sobre las instituciones sociales y sus esferas de responsabilidad. Cada vez más en todo el mundo, las administraciones públicas ponen su información a disposición de los ciudadanos, los medios y otras partes interesadas, y la comparten con ellos, en respuesta a su adhesión a los principios de buena gobernanza, que son los fundamentos que permiten alcanzar los objetivos de paz y desarrollo.

Los datos públicos abiertos son un pilar en la elaboración de una estrategia de gobernanza transparente. El término supone que los organismos gubernamentales publican sus datos en línea de forma que puedan ser leídos por personas y procesados por computadoras (preferentemente, como datos en bruto o datos estructurados en formatos abiertos que pueden ser procesados por máquinas, y con arreglo a una licencia libre para que puedan ser reutilizados por terceros). El público puede examinar y descargar los datos, e incluso crear nuevos análisis y aplicaciones basándose en ellos.

Por otra parte, los datos públicos abiertos propician niveles enteramente nuevos de participación cívica y de responsabilidad y transparencia gubernamentales que, a su vez, mejoran la prestación de servicios públicos y la utilización de recursos públicos. A pesar de las diversas dificultades que plantea la brecha digital entre "países con diferentes niveles de desarrollo, que afecta numerosas aplicaciones útiles desde el punto de vista económico y social en esferas como la administración pública, las empresas, la salud y la educación", los gobiernos del mundo entero utilizan e intercambian cada vez más datos por la web a escala nacional, regional y local.

El valor intrínseco y los posibles beneficios de los datos públicos abiertos parecen bastante claros, aunque es posible ampliar nuestro imaginario colectivo gracias al intercambio activo de ideas y experiencias. Es una tarea difícil para las autoridades gubernamentales a todos los niveles (nacional, regional, local) iniciar y sostener iniciativas en materia de datos abiertos debido a la falta de comprensión de sus ventajas por parte de responsables políticos y partes interesadas, así como de conocimientos técnicos.

Para ello es necesario reforzar la capacidad de los funcionarios públicos, y también de las partes interesadas en representación de las empresas, la comunidad científica y la sociedad civil, para iniciar, implantar y evaluar formas innovadoras y sostenibles de iniciativas en materia de publicación de datos. Aunque se ha logrado un amplio consenso sobre los beneficios generales que puede tener para la sociedad y la democracia mejorar la transparencia, la responsabilidad, la dimensión participativa y la eficacia de la administración pública, algunos estudios recientes indican también que los datos públicos

[2] Según un documento de la BDT.

abiertos tienen igualmente consecuencias positivas para la economía puesto que permiten crear nuevos productos y servicios basados en su reutilización.

En la actualidad se utiliza una amplia gama de indicadores para evaluar el desempeño de la administración pública, especialmente en el ámbito del cibergobierno. Uno de los retos de las futuras administraciones públicas será diseñar y poner en práctica nuevos parámetros de medición para comparar su desempeño y procurar la supervisión y mejora de las iniciativas en materia de participación ciudadana y datos públicos abiertos. Se debe hacer un análisis comparativo de la "voluntad de transformación" de los gobiernos e introducir mejoras en el "valor público" desde el punto de vista de los ciudadanos. Las iniciativas sobre datos públicos abiertos formuladas en el mundo entero durante los últimos años muestran con claridad que los interesados carecen aún de una comprensión clara de los posibles beneficios de esta herramienta, ya sea con respecto a la transparencia y responsabilidad de las administraciones públicas o a la obtención de mayores resultados sociales y económicos.

2.3 Componentes del cibergobierno

2.3.1 Portal, intercambio de información, seguridad

El portal de la administración pública es un elemento central del cibergobierno destinado a ofrecer a ciudadanos y empresas un fácil acceso a la información y a los servicios públicos. La idea fundamental que explica su importancia es que reagrupa información y servicios de todos los organismos y crea un punto de acceso único a cada información y a cada servicio. Los ciudadanos y las empresas están mejor informados y pueden saber qué funcionario en qué departamento y a qué nivel es responsable de ciertas informaciones o de un cierto programa público. Mediante una fácil interacción con las autoridades gubernamentales y el acceso a documentos oficiales y procedimientos administrativos, los ciudadanos estarán más dispuestos a participar en las cuestiones públicas, lo cual reforzará la dimensión participativa de los modelos de gobernanza haciendo que los ciudadanos intervengan más activamente en los procesos vinculados a la adopción de decisiones. El portal es una herramienta poderosa para la selección e integración de la enorme cantidad de información que posee la administración pública.

Dada la evolución de las tecnologías de cibergobierno hacia tecnologías móviles y sociales, se está llevando a cabo una reformulación del portal para convertirlo en un lugar donde las autoridades públicas solicitan la opinión de los ciudadanos y consultan a todos los sectores de la sociedad, con miras a adoptar decisiones que aporten los mejores beneficios a todos. Los funcionarios públicos pueden obtener información sobre lo que piensan los ciudadanos con respecto a las políticas gubernamentales. En vez de responder pasivamente a las demandas procedentes del exterior, los organismos gubernamentales perciben las necesidades de la población y tratan de dar respuesta a sus exigencias.

El intercambio de información es un elemento esencial en la implantación del cibergobierno puesto que propicia la reestructuración e integración de las actividades de la administración pública. La idea básica del intercambio de información consiste en almacenar la información una sola vez, y no de repetir varias veces la operación, de modo que los ciudadanos y las empresas no tengan que dar la misma información a diferentes departamentos públicos. Los ciudadanos no tendrán que presentarse tantas veces en oficinas públicas, y deberán entregar menos justificativos al solicitar un determinado servicio.

Por otra parte, el intercambio de información abarca el concepto según el cual los poderes públicos recopilan una sola vez información de los ciudadanos y las empresas, de tal manera que todos los departamentos gubernamentales pueden luego utilizarla. La información es un recurso vital para la gestión eficaz de la administración pública. Es frecuente que la información relativa a la identificación de los ciudadanos sea solicitada por numerosos organismos, por ejemplo, para el pago de impuestos o para la renovación de un permiso de conducir. Sería menos engorroso para los ciudadanos y las empresas que, al interactuar con el nuevo departamento para solicitar un determinado servicio, sólo tengan que facilitar datos suplementarios. El intercambio de información contempla cuestiones vinculadas a las tecnologías más propicias, a los acuerdos jurídicos e institucionales y a la cultura institucional, entre las cuales esta última ha merecido una atención particular puesto que se estima que el fracaso del intercambio de

información se debe al egoísmo de la institución, que considera la información como una fuente de poder y, por ese motivo, está menos dispuesta a compartirla.

Una de las cuestiones más delicadas en relación con el intercambio de información es la posibilidad de intrusión en los datos personales y la poca seguridad de las redes. Nunca se insistirá demasiado en la importancia de proteger la privacidad y la seguridad en la promoción del cibergobierno. Por más conveniente y eficaz que sea, si la privacidad no está protegida, el sistema encontrará la resistencia de los usuarios y será difícil recobrar su confianza. La protección de la información personal puede lograrse con la aplicación de medidas técnicas, jurídicas, institucionales y culturales. Si bien el intercambio de información es un elemento central del cibergobierno y una condición previa para promover aplicaciones TIC, la protección de la información es una medida de prevención contra la filtración de datos personales que puede tener lugar en el marco del intercambio de información.

2.3.2 Redes, capacidades humanas

Las redes de alta velocidad son la infraestructura básica que permite el acceso de los funcionarios gubernamentales a bases de datos y a diversas aplicaciones. Son condiciones previas no sólo de la interconexión entre organismos gubernamentales, es decir, entre gobiernos centrales y locales y entre ministerios, sino también de la interacción de los ciudadanos y las empresas con el gobierno para obtener información y servicios. El cibergobierno puede prestar servicios públicos, como la atención de la salud y la educación, a través de redes de banda ancha. Los sistemas de cibersalud proponen servicios a distancia a habitantes de zonas rurales, y con los sistemas de ciberaprendizaje los estudiantes pueden recibir materiales extraescolares no disponibles en las escuelas.

La capacidad de los usuarios para utilizar los sistemas implantados es fundamental para lograr los máximos beneficios del cibergobierno. En la primera etapa de la implantación del cibergobierno suele ocurrir que el nivel de utilización del sistema ha sido tan bajo que la inversión en él se considera un despilfarro. De los numerosos motivos que originan esta crítica, el señalado con mayor frecuencia es la incapacidad de los ciudadanos para utilizar el sistema. Durante la primera etapa de implantación de este sistema, es sumamente importante impartir conocimientos básicos de Internet, especialmente a personas que viven en zonas aisladas. Este asunto ha sido abordado en el debate sobre la brecha digital. Aunque la disparidad en la utilización de los servicios de cibergobierno está a veces vinculada a las instalaciones técnicas, en particular a la falta de equipos asequibles o de conexiones a Internet de banda ancha, la ausencia de capacidades humanas representa el principal obstáculo contra el aprovechamiento máximo de los sistemas implantados. Se recomienda resueltamente, al elaborar un plan nacional de las TIC que contemple servicios de cibergobierno, el establecimiento de programas de capacitación en las TIC para funcionarios públicos y ciudadanos, especialmente en las zonas rurales.

2.4 Categorías de actividades relativas al cibergobierno

2.4.1 Aplicaciones: servicios G2G, G2C y G2B

Las siglas G2G y G2C designan respectivamente los servicios prestados dentro de las administraciones públicas (“government to government”) y por las administraciones públicas a los ciudadanos (“government to citizens”). La sigla G2B alude a los servicios prestados por las administraciones públicas a las empresas (“government to business”), categoría de servicios muy cercana a la categoría G2C desde el punto de vista de las características de las aplicaciones de cibergobierno. Los servicios G2G se refieren a las iniciativas de cibergobierno relativas a las tareas administrativas, en tanto que los servicios G2C y G2B indican la interacción entre los gobiernos y los ciudadanos y las empresas, es decir, las actividades de atención al cliente.

La categoría G2G incluye las iniciativas, cuyo objetivo principal es la innovación de los métodos de trabajo, como el establecimiento de métodos de trabajo electrónicos, un mayor intercambio de información administrativa y la reorganización de las actividades centradas en los servicios. Por ejemplo, los sistemas

electrónicos de documentos, los sistemas de financiación de gobiernos locales y centrales, los sistemas de auditoría electrónica, etc., pertenecen a la categoría G2G.

Las categorías G2C y G2B comprenden las aplicaciones que se ocupan de la innovación de los servicios prestados a ciudadanos y empresas. En Corea, el servicio G4C (government for citizens) representa la categoría de aplicaciones G2C. Además, el sistema de bienestar nacional, el sistema de información sobre alimentos y medicamentos, y el sistema de información sobre el empleo y de búsqueda de empleo constituyen ejemplos de servicios G2C. La categoría G2B, relativa a la innovación de servicios a las empresas, incluye el servicio de portal de empresas relativo a las tareas administrativas de las entidades, la información industrial y otros servicios adicionales vinculados a diversas actividades durante todo el ciclo de vida de una empresa, desde su creación hasta el cese de sus actividades. Asimismo, el sistema de información sobre los flujos logísticos, las empresas extranjeras, etc., también pertenecen a esta categoría. La categoría de aplicaciones G2C comprende otro sistema concebido para fomentar la participación de los ciudadanos en el proceso de adopción de decisiones públicas, que tiene una incidencia importante en el marco de la ciberdemocracia. La finalidad del sistema es reforzar los medios que disponen los ciudadanos para expresar sus opiniones sobre determinadas políticas e interactuar con las autoridades gubernamentales en sus diferentes niveles.

2.4.2 Financiación

Los fondos requeridos por las iniciativas de cibergobierno son de tal magnitud que conviene elaborar con sumo cuidado un plan de financiación. Con el fin de facilitar la movilización de los recursos necesarios para la ejecución de proyectos de cibergobierno, muchos países en desarrollo se apoyan en dirigentes políticos que reconocen la importancia decisiva del cibergobierno. Es la estrategia utilizada por Corea en la primera etapa de los proyectos nacionales de tecnologías de la información. Dada la dificultad que planteaba poner de relieve las ventajas de las inversiones en las TIC, debido a la naturaleza de esas tecnologías, el gobierno de Corea decidió destinar una cierta cantidad de dinero para uso exclusivo de los proyectos de tecnologías de la información sobre la base de decretos promulgados por el Presidente del país.

El problema de la financiación de proyectos de tecnologías de la información estimula el debate sobre la oferta y la demanda. En los círculos académicos ha quedado muy claro que, al estimular la innovación de la tecnología y la creación de nuevas aplicaciones, se considera que políticamente es mucho más eficaz intervenir con respecto a la demanda que a la oferta. El riesgo de una mala asignación de los fondos públicos es elevado cuando no se comprende la demanda. Cuando se hace especial hincapié en la cuestión de la demanda de un proyecto, la pregunta fundamental es la siguiente: ¿qué tipo de servicios justifican la enorme inversión requerida para los proyectos de cibergobierno? Esta pregunta se plantea debido a la posibilidad de crear una solución costosa para un problema que en realidad no existe.

Lamentablemente, estamos frente a un dilema. Un cierto número de proyectos vinculados a las tecnologías de la información han creado un tipo de demanda que es imposible prever antes de que la oferta esté disponible. A raíz de este dilema, se han autorizado los primeros proyectos de cibergobierno con arreglo a la teoría de la oferta. La estrategia de los partidarios de esta teoría responde al mecanismo de financiación utilizado en la etapa inicial del cibergobierno en países como Corea. Sin embargo, dar prioridad a la oferta no debe descartar la importancia de tener en cuenta la posible demanda de un servicio particular de cibergobierno. Por ejemplo, al decidir qué servicios incluir en las iniciativas de cibergobierno, se pueden abordar aspectos relativos a la demanda examinando las transacciones fuera de línea entre las administraciones públicas y los ciudadanos.

2.4.3 Disposiciones jurídicas e institucionales

Durante la elaboración de las actividades de cibergobierno, el establecimiento de disposiciones jurídicas y reglamentarias es una condición necesaria de éxito dado que los métodos de trabajo de la administración pública deben ajustarse estrictamente a la legislación. Por ejemplo, si bien en el pasado los documentos impresos tenían valor de prueba jurídica de la gestión gubernamental, la instauración de sistemas de

cibergobierno ha dado lugar a la creación de documentos electrónicos para llevar a cabo las tareas de la administración pública, lo cual requiere el establecimiento de disposiciones jurídicas para ese tipo de documentos. Las disposiciones relativas al valor de prueba jurídica se cumplen mediante la agrupación y coordinación de funciones públicas análogas que, anteriormente, correspondían a diferentes organismos gubernamentales.
Con objeto de establecer una base institucional para el cibergobierno, las leyes y los decretos ejecutivos relacionados con asuntos civiles que se habían promulgado durante el entorno fuera de línea deben modificarse para tener en cuenta la tramitación electrónica de asuntos civiles. Incluso después de la implantación técnica de los sistemas de cibergobierno, la forma de trabajar y de razonar de funcionarios públicos y ciudadanos no cambiará a menos que se preparen para ellos leyes y reglamentaciones relativas al funcionamiento de los sistemas de cibergobierno.

La utilización de un sistema de gobernanza informático para llevar a cabo las actividades de cibergobierno de forma eficaz es una parte fundamental de las disposiciones institucionales dado que permitirá asegurar la solidez de la estructura orgánica. Puesto que en su mayoría suelen afectar a un cierto número de organismos, los proyectos de cibergobierno están muy expuestos a los conflictos que pueden perturbar el proceso normal de implantación del cibergobierno. Con el fin de garantizar la coordinación entre los organismos correspondientes, se ha formado un Comité ad hoc para resolver las diferencias planteadas entre ellos. Los miembros del Comité no sólo pertenecen a las organizaciones interesadas, sino también a profesiones independientes, de los que se espera que adopten una posición neutral en el proceso de coordinación.

3 Prácticas óptimas aplicados por los Estados Miembros (contribuciones a los trabajos del UIT-D)

Durante los últimos tres años del tercer Período de Estudios (2010-2013), se presentaron 12 casos de iniciativas de cibergobierno en la Comisión de Estudio en su reunión de septiembre. Los dos casos de Bangladesh se han reducido a uno debido a la similitud de contenidos. Se presenta una versión resumida de cada contribución respetando el orden de presentación. Los textos completos de cada contribución figuran en Anexo al final del presente Informe.

3.1 Proyecto INV (Information Network Village, *Aldeas de la red de información*) (República de Corea)

Este proyecto tiene por finalidad procurar el acceso de habitantes de zonas aisladas a importantes contenidos sobre, por ejemplo, educación, información médica y técnicas agrícolas, que reduzcan la brecha digital entre zonas urbanas y rurales. También prevé proporcionar capacidades que permitan vender directamente especialidades locales a los consumidores, lo cual aumentará las ganancias obtenidas por la producción local. De esta forma, el proyecto contribuye a impulsar la economía local y equilibra el desarrollo regional en todo el país. Se espera que la capacitación de los habitantes de zonas aisladas para que adquieran conocimientos básicos de Internet aumente la demanda de servicios de cibergobierno[3].

- Se aspiraba a crear una infraestructura Internet de banda ancha en aldeas de agricultores y pescadores, en zonas aisladas y en otros lugares en los que no tuvo lugar la revolución de la información, con la intención de resolver las disparidades en materia de información entre zonas urbanas y rurales. También se esperaba que sentaran las bases del cibergobierno y la democracia electrónica.

[3] Presentado en la primera reunión de la CE 2 el 14 de septiembre de 2010.

- El proyecto apuntaba también a la creación de contenido de la información, en especial un mercado en línea para productos locales, con objeto de generar beneficios prácticos y reactivar las economías locales para lograr un desarrollo nacional equilibrado.
- Debía facilitar a la población local el acceso cotidiano a la información sobre educación, medicina, cultura y conocimientos agrícolas a través de Internet.
- Para cada aldea se estableció un Comité de gestión del proyecto INV. El Comité determinaba las cuestiones esenciales relacionadas con las actividades informáticas de la aldea. Se alentó asimismo la creación de un modelo económico para que el Comité pudiera desempeñarse como órgano autónomo, incluso en ausencia de ayudas públicas. Teniendo en cuenta la singularidad de las características locales, se diseñaron con sumo cuidado modelos INV en armonía con las necesidades locales y, tras una evaluación estricta, se difundieron en todo el país.
- Aprender de qué manera utilizar los sistemas de información a través del proyecto INV es un factor decisivo para el éxito del proyecto.
- Este programa consiste en la celebración de diversos eventos para que el público en general conozca mejor el proyecto INV.
- El proyecto INV da prioridad al fomento de capacidades en materia de tecnologías de la información con objeto de que la población local logre hacer frente a la sociedad de la información en permanente evolución. Por ejemplo, uno de los objetivos es ofrecer servicios públicos en línea a la población local a través en el marco del proyecto de cibergobierno local.
- El proyecto INV ha logrado los siguientes resultados. En primer lugar, la aplicación de las iniciativas antes mencionadas contribuyó a reducir la brecha digital gracias a una mayor utilización de Internet por parte de quienes no tienen acceso a la información, como los habitantes de zonas rurales.
- Los habitantes de zonas aisladas han podido aprovechar los servicios de cibergobierno gracias a la capacitación que recibieron en el marco del proyecto INV.
- Asimismo, se crearon diversos incentivos para incentivar el interés en el proyecto, por ejemplo, incorporar en él el programa de comercio electrónico para aumentar las ganancias de quienes venden sus productos a través del cibercomercio.
- Otros países toman como referencia el proyecto INV, concebido para reducir la brecha digital de zonas con acceso limitado a la información, como las aldeas de agricultores y pescadores.
- Se invita a las aldeas participantes a establecer alianzas con empresas privadas interesadas en el desarrollo de aldeas a través del proyecto INV.
- En la visita a una aldea de la red de información, por ejemplo, un ejecutivo de Intel (el fabricante de circuitos integrados más importante del mundo) elogió el proyecto INV coreano considerándolo un ejemplo sin precedentes en la digitalización de aldeas de agricultores y pescadores.

3.2 Sistema coreano de compras del sector público en línea (KONEPS) (República de Corea)

El sistema KONEPS trata en línea la totalidad de las operaciones relativas a las compras del sector público, desde el anuncio para la presentación de ofertas y la adjudicación hasta el establecimiento de contratos y el pago. Al estar conectado a equipos de intercambio de datos públicos, el sistema eliminó la necesidad de presentar documentos en papel, como certificados de inscripción de las empresas y recibos fiscales. Por otra parte, permite tener acceso a una versión digitalizada de más de 160 formularios oficiales (licitaciones, contratos, pedidos de inspección y solicitudes de pago) que pueden ser tratados de forma electrónica. En la medida en que prevé los pagos en línea, los informes de prestaciones, la inspección y las solicitudes de pago, se pueden reducir efectivamente las demoras de pago, puesto que cada unidad

encargada de las contrataciones, la inspección y los pagos, incorpora respectivamente en el sistema común las tareas realizadas, racionalizando de esa forma los procedimientos de pago.
Se decidió que los diferentes organismos no debían elaborar su propio sistema de compras electrónico. En su lugar, se propuso elaborar un sistema tipo introduciendo ciertas adaptaciones. Para no malgastar el presupuesto, en junio de 2001 se anunciaron "directrices destinadas a evitar duplicaciones". Al llevar a cabo proyectos de cibergobierno, la revisión de la legislación y la reglamentación no son menos importantes que la creación del propio sistema.[4]

- La tecnología de infraestructura utilizada por el sistema KONEPS comprende una firma electrónica basada en la infraestructura de clave pública (PKI), una tecnología de seguridad de los documentos, normas para el intercambio electrónico de datos y servicios web a gran escala.
- El sistema KONEPS prevé la publicación electrónica de información relativa a la presentación de ofertas facilitada por todos los organismos públicos, procurando un servicio de ventanilla única para las compras del sector público.
- El sistema KONEPS también está conectado al sistema de contabilidad pública, con lo cual las instituciones que efectúan las compras pueden administrar los pagos mediante la transferencia electrónica de fondos.
- El PPS (servicio público de compras) prosiguió con el desarrollo del servicio móvil de compras por teléfono móvil; debido a la impresionante difusión de teléfonos inteligentes, los servicios móviles serán cada vez más populares en el mercado relativo a las compras.
- El sistema KONEPS ha mejorado considerablemente la transparencia del procedimiento de compras del sector público.
- En el Congreso Mundial de Tecnologías de la Información (WCIT), el PPS fue designado como el organismo público más innovador en servicios que utilizan las tecnologías de la información.
- Con miras a elaborar la forma integrada del sistema de compras, el sistema KONEPS ha sido examinado según tres diferentes puntos de vista, esto es, los servicios, los datos y la arquitectura técnica.
- Asimismo, KONEPS se integrará al sistema laboral del PPS con objeto de que los funcionarios públicos de este último servicio saquen pleno partido de las iniciativas de cibergobierno.
- Actualmente, los datos son administrados de forma separada según el tipo de elementos de servicio y de métodos de trabajo en el marco de las estructuras PPS.
- Por último, teniendo en cuenta la integración de los servicios de compras y la reestructuración de los datos resultantes del funcionamiento del sistema KONEPS, se analizará la estructura del sistema, y éste se rediseñará conforme a eGovFrame, el marco de elaboración de normas de cibergobierno.

3.3 En camino del cibergobierno (Uganda)

El Gobierno de Uganda está plenamente convencido de que las TIC no sólo pueden revolucionar el modo de funcionamiento del gobierno sino también mejorar la relación que éste mantiene con los ciudadanos, las empresas y sus propios organismos. El programa *En camino del cibergobierno* se inició en Uganda con la política de las TIC en 2003, que destacaba principalmente la necesidad de crear una infraestructura para esas tecnologías en todo el país. En el marco de esa política, en 2004 se llevó a cabo una encuesta

[4] Presentado en la segunda reunión de la CE 2 el 11 de septiembre de 2011.

sobre el grado de preparación del país en la esfera electrónica. En 2005, las autoridades gubernamentales estaban preparadas a utilizar métodos de trabajo electrónicos.

En 2006, con la ayuda del Gobierno de China, Uganda comenzó a poner en marcha una infraestructura de cibergobierno en todo el país. La primera fase abarcó todos los ministerios centrales situados en Kampala y Entebbe, y también las ciudades de Bombo, Jinja y Mukono. La red ofrece servicios básicos de telefonía, videoconferencia y datos.

Los servicios entre ministerios funcionan actualmente sin costo alguno. Se está realizando una experiencia de colaboración entre cuatro ministerios que les permitirá utilizar la misma plataforma informática. La segunda fase, que abarca las regiones orientales, septentrionales y occidentales de Uganda, comenzó a finales de 2011. El sector privado también ha puesto en marcha una infraestructura TIC en todo el país, que puede ser utilizada para el cibergobierno[5].

- Se ha adoptado una legislación aplicable al ámbito electrónico (por ejemplo, la Ley de transacciones electrónicas, la Ley de firmas digitales y la Ley sobre utilización abusiva de la informática), que entrará en vigor a finales del año.
- Disponiendo de la infraestructura necesaria, Uganda ha elaborado un marco de cibergobierno que orientará su puesta en marcha. Todos los gobiernos de distrito del país tienen a su disposición páginas web elaboradas en el marco del Programa de desarrollo de comunicaciones rurales (RCDP). Se publican en ellas información relativa a servicios públicos, inversiones y empresas, pese a las dificultades que plantean la actualización periódica de los datos y el pago por parte de los distritos de las tasas de Internet y de almacenamiento de páginas web.
- El portal web del Gobierno de Uganda sirve de plataforma de acceso a los servicios públicos. Está en curso de elaboración el enlace con las empresas del sector privado.
- En colaboración con la ONUDI, el Ministerio de las TIC ha establecido centros piloto de información empresarial en seis distritos (Mityana, Iganga, Lira, Rukungiri, Kamwenge y Busia) para mejorar el acceso de los ciudadanos a los servicios TIC.
- Un Centro nacional de datos facilita el almacenamiento, la utilización, el intercambio y la protección de datos públicos.
- La mayoría de las iniciativas formuladas por el sector privado contemplan la telefonía móvil teniendo en cuenta que la tasa de utilización de sistemas móviles es superior a la correspondiente a la informática/Internet en Uganda.

3.4 Implantación de la conectividad de banda ancha en zonas desfavorecidas en Uganda (Uganda)

La Comisión de Comunicaciones de Uganda (UCC) ha creado el Fondo para el desarrollo de las comunicaciones rurales (RCDF) con el fin de estimular la prestación de servicios de telecomunicaciones en zonas rurales desfavorecidas. El RCDF es pues un mecanismo que permite aprovechar las inversiones en infraestructura y servicios de comunicaciones en las zonas rurales desfavorecidas del país.

Se reconoció que, aunque el sector se ha liberalizado y fue abierto a la competencia, algunas regiones del país que no eran comercialmente viables no lograban atraer la inversión de capitales privados en infraestructura y servicios. Los objetivos principales del RCDF son proporcionar acceso a servicios básicos de comunicación a una distancia razonable, garantizar una inversión eficaz en el desarrollo de las comunicaciones rurales y promover la utilización de las TIC en el país.

[5] Presentado en la segunda reunión de la CE 2 el 11 de septiembre de 2011.

La política de Uganda en materia de acceso universal (2010) está basada en el programa mundial de desarrollo, los Objetivos de Desarrollo del Milenio (ODM), a los que Uganda suscribe, y en el Plan nacional de desarrollo (2010), vinculado originalmente a la visión nacional conocida como Visión 2025. Esa política también se basa en la política de acceso universal anterior (2001) y se inscribe en el marco de la política del país con respecto a las TIC y las telecomunicaciones.

Los motivos principales que explican la poca difusión de Internet en las zonas rurales son los costos de acceso, el ancho de banda insuficiente, los problemas de alimentación eléctrica y, motivo aún más importante en las comunidades rurales, el analfabetismo y la ausencia de contenido interesante en lengua vernácula. Por consiguiente, la principal finalidad de la nueva política es asegurar la conectividad de banda ancha y respaldar la elaboración de contenidos locales.

El principal impedimento actual del sector de las TIC en Uganda es la falta de una infraestructura de red de banda ancha destinada a facilitar un acceso más rápido y a favorecer la utilización de las TIC en general y de Internet en particular. Esta situación se debe especialmente a las sumas importantes de capital necesario que el sector privado no puede aportar por sí solo y que supone pues una intervención especial de las autoridades estatales.

El Gobierno de Uganda ha comenzado a respaldar la interconexión de todas las grandes capitales de gobiernos locales y de las principales ciudades a la infraestructura nacional de red troncal de datos con el propósito de ofrecer a los usuarios una gran variedad de servicios TIC a bajo costo. Esta medida debería facilitar la creación de puntos de acceso públicos a servicios de datos dando en un primer momento prioridad a los establecimientos de formación profesional, universitarios y secundarios, y a las unidades de salud pública para los niveles IV y III. Se proporcionará una conectividad de banda ancha que permitirá conectar a subprovincias seleccionadas a la infraestructura nacional de red troncal de alta velocidad. Se trata de una opción para asegurar la conexión del "último kilómetro" en las subprovincias. Para ello, se está llevando a cabo un estudio detallado para determinar las opciones tecnológicas más rentables (inalámbricas, por cable) que podrían implantarse en cada emplazamiento.[6]

- **Cibergobierno:** El proyecto ayudará a recopilar información proveniente de las autoridades públicas de todos los niveles, de gobiernos locales al gobierno central. Esa información formará parte de estadísticas demográficas nacionales y otros tipos de datos socioeconómicos afines.
- **Cibereducación:** Educación a distancia: El proyecto facilitará el ciberaprendizaje, que ya está alcanzando gran popularidad en el país. Por ejemplo, las principales universidades locales tienen campus satélites en otras localidades del interior del país en los que se ofrece educación a distancia y en línea.
- **Cibersalud:** El proyecto facilitará los flujos de datos y la telefonía desde las comunidades rurales hacia los centros de salud, los hospitales de distrito, los hospitales regionales de referencia y, por último, los hospitales nacionales de referencia, así como los flujos en sentido inverso. Se espera un tráfico suplementario entre el Ministerio de Salud y las oficinas de distrito, y también entre el Ministerio y los centros de salud.

En Uganda, los niveles de penetración y utilización de Internet, y de acceso a la misma, siguen siendo muy bajos, estimándose que los usuarios representan apenas el 5% de la población total. La presencia de Internet se limita en gran medida a los centros comerciales urbanos debido a las consideraciones de carácter comercial que esgrimen los proveedores de servicios privados. Aunque la política anterior aplicada por el país consistía en respaldar la instalación de puntos de acceso a Internet en todos los distritos desfavorecidos, una Internet a gran velocidad y la calidad de servicio (apagones) constituyen las principales preocupaciones de los usuarios finales.

[6] Presentado en la segunda reunión de la CE 2 el 11 de septiembre de 2011.

3.5 Sistema de información del gobierno local (LGIN)

La Constitución de la República de Corea dispone que "los gobiernos locales se encargan de cuestiones relativas al bienestar de los ciudadanos a nivel local, así como de gestionar bienes, y, dentro de los límites legislativos, están facultados para promulgar disposiciones referentes a las normativas autonómicas locales". Cuando se aplicó el proyecto, existían 16 gobiernos provinciales, de los cuales siete eran gobiernos metropolitanos de ciudades, así como 234 gobiernos de ciudades y distritos. Los encargados de los gobiernos locales gestionan y supervisan asuntos administrativos a menos que la ley establezca otras cuestiones. Entre las funciones de los ejecutivos locales se encuentran las delegadas por el gobierno central, como la gestión de bienes públicos e instalaciones, el asesoramiento fiscal y la recaudación de impuestos locales y de tasas para diferentes servicios. Las juntas educativas de los gobiernos locales se encargan de las cuestiones de educación y actividades de los estudiantes en las comunidades. Básicamente, los gobiernos provinciales sirven de intermediarios entre el gobierno central y los gobiernos locales (ciudad o distrito), de menor nivel.

- Los gobiernos deben hacer frente a la fuerte presión de los ciudadanos, que reclaman la reducción de costos de los servicios públicos, la mejora de los servicios de atención al cliente y la difusión más eficaz de información en las divisiones jurisdiccionales.
- Al aplicarse un sistema nuevo, como LGIN, los funcionarios deben adaptarse a un nuevo entorno de trabajo.
- Esta estrategia puede ampliarse a procesos comerciales y servicios de solicitudes.
- Esta iniciativa permitió a los organismos gubernamentales intercambiar información, lo cual mejoró los trámites internos de los gobiernos locales, así como la calidad de los servicios ofrecidos al público.
- Además, los gobiernos locales intercambian información y datos; de este modo, se reduce el número de documentos que deben tramitar los servicios públicos.
- La simplificación del flujo de trabajo en los procesos del proyecto LGIN ha eliminado el solapamiento en los procedimientos y las tareas de gestión de los servicios públicos.
- Esta mayor eficacia de la administración pública ha permitido optimizar el entorno de los servicios públicos y aumentar la confianza en la administración pública.
- El sistema LGIN es una infraestructura de información en la que están integradas todas las esferas del servicio público.
- Los servicios móviles están disponibles en algunas esferas de aplicación.

El sistema LGIN resulta fundamental para que las aplicaciones de cibergobierno del gobierno central tengan el máximo efecto, dado que los diferentes servicios públicos gestionados a nivel central se canalizan a continuación a través de las vías correspondientes en los gobiernos locales.

Los factores de éxito del proyecto identificados *supra* provienen de nuestra experiencia en su aplicación. El sistema LGIN ha podido alcanzar los logros actuales respondiendo con eficacia a los problemas que se resumen a continuación[7]:

- cómo solucionar las controversias entre las diferentes entidades implicadas en el proyecto;
- cómo financiar el proyecto y distribuir los costos entre gobiernos locales y centrales;
- cómo abordar las tensiones psicológicas de quienes aceptan el nuevo sistema técnico y sus posibles miedos ante la inseguridad laboral;

[7] Presentado en la tercera reunión de la CE 2 el 17 de septiembre de 2012.

- cómo evitar grandes pérdidas derivadas de posibles fallos debido a procesos complejos de implantación y a la gran envergadura de un proyecto a escala nacional;
- cómo conseguir el apoyo de dirigentes políticos y gubernamentales para obtener condiciones propicias para la financiación y la revisión de las leyes y reglamentaciones correspondientes, etc.

3.6 Panorama general de los servicios TIC en Bangladesh

Considerado uno de los países más densamente poblados del planeta, Bangladesh sigue siendo uno de los países del Asia Meridional con más baja densidad telefónica. Hasta ahora, sólo una proporción relativamente pequeña de la población tenía acceso a las telecomunicaciones. Hace apenas 10 años, la densidad telefónica era inferior al 1%, pero la era de la telefonía móvil ha cambiado el panorama puesto que, actualmente, Bangladesh registra una proporción superior al 46%.

En cierta medida, la situación general del país se ha mejorado gracias al rápido crecimiento del mercado de la telefonía móvil. La utilización de tecnologías de la información y la comunicación (TIC) en las actividades gubernamentales ha pasado a ser moneda corriente en los últimos años.

Hasta la fecha, se han aplicado diferentes tecnologías (intercambio electrónico de datos, telefonía interactiva, mensajería vocal, correo electrónico, prestación de servicios web, realidad virtual e infraestructura de clave pública) para tener en cuenta las características singulares del cibergobierno.

Se entiende por cibergobernanza la utilización por parte de los sectores públicos de las tecnologías de la información para dar servicio e información, y para incitar a los ciudadanos a participar democráticamente en el proceso de adopción de decisiones procurando de esa forma que las autoridades públicas sean más transparentes y responsables. Es necesario crear un portal que centralice las informaciones oficiales por Internet para que los ciudadanos dispongan de toda la información necesaria de los diferentes ministerios. Se debe poner a disposición de los ciudadanos la teledescarga de todo tipo de formularios y solicitudes. Asimismo, se podrá añadir una función de presentación en línea para evitar trámites burocráticos complicados. Para conseguir transparencia y combatir la corrupción, ese portal web permite también responder a un llamado a licitación, presentar declaraciones de impuestos y adjudicar terrenos. Habría que comprender no obstante que cuando se habla de gobierno móvil se alude únicamente a una de las modalidades de comunicación electrónica con las autoridades públicas, y sólo tiene sentido si existe un sistema de cibergobierno8.

- Se entiende por cibergobernanza la utilización por parte de los sectores públicos de las tecnologías de la información para dar servicio e información, y para incitar a los ciudadanos a participar democráticamente en el proceso de adopción de decisiones procurando de esa forma que las autoridades públicas sean más transparentes y responsables.
- Nuestros productos y servicios se deben proponer en el mercado mundial mediante estrategias adecuadas de comercialización orientadas a las TIC.
- Para incentivar a la comunidad empresarial a utilizar las TIC, se puede crear una red de empresas especializadas.
- Con un sistema de negociación de valores en línea, un número mayor de agentes de diferentes comunidades participarán en el mercado de capitales.
- El sistema jurídico y el sistema de salud pueden ser también muy importantes en todos los ámbitos de la comunidad.

8 Presentado en la tercera reunión de la CE 2 el 17 de septiembre de 2012.

- La instauración de un sistema eficaz de gestión de la relación médico-paciente en todos los hospitales públicos permitirá mejorar los servicios de salud en zonas aisladas.
- El entorno de la "aldea mundial" en la que vivimos está cambiando, se redefine y evoluciona a la velocidad de Internet.
- Para mantener la competitividad en el mercado mundial, Bangladesh debe seguir el ritmo de esa evolución e implantar el sistema de cibergobierno.
- En Bangladesh, el cibergobierno recién comienza, pero ya ha dado los primeros pasos hacia la revolución de Internet.
- Hay enormes posibilidades para el desarrollo del cibergobierno en Bangladesh.

La digitalización de Bangladesh está en marcha. Una infraestructura de redes nacionales duraderas y fiables fortalecerá las autopistas de la información del país y eliminará la brecha digital entre zonas rurales y zonas urbanas. La descentralización y los servicios públicos digitales favorecerá a todos los ciudadanos.

3.7 Implantación del cibergobierno en la República Kirguisa – Experiencia y próximas etapas

El Gobierno de Kirguistán está adoptando una posición muy activa dado que hace hincapié en la gran importancia que adquieren las tecnologías de la información y la comunicación (TIC) en tanto que herramientas para acelerar el desarrollo de los países. La Estrategia de Desarrollo Nacional a medio plazo (2012-2014) y el Programa especial del Gobierno "Estabilidad y vida digna" indican claramente la necesidad urgente de la adopción del cibergobierno en el país para la transformación de la gobernanza en el plano electrónico, que responderá a las necesidades de los ciudadanos de a pie. En la actualidad, se observa un nivel satisfactorio de informatización en los órganos de la administración pública de la República Kirguisa y, especialmente, en los organismos del gobierno central. En la mayoría de los ministerios que trabajan con una enorme cantidad de datos de información hay servidores especiales para bases de datos, sistemas de correo electrónico, acceso a Internet y otros servicios, e incluso departamentos encargados de la elaboración y gestión de datos. Numerosos ministerios y administraciones gubernamentales están creando sus propias redes locales y sus propios sistemas de información con acceso a Internet.
Aunque el marco jurídico del país relativo al cibergobierno, que comprende 16 leyes en materia de TIC, es suficiente, hay que preparar y adoptar nuevas leyes para facilitar una mayor implantación de servicios electrónicos y el intercambio de información en el país (por ejemplo, promulgar una Ley sobre comercio electrónico, unificar normas y requisitos técnicos).
La República Kirguisa adoptó en 2002 la Estrategia y Plan de Acción Nacional, "*TIC para el Desarrollo de la República Kirguisa*" para 2002-2010. Según la evaluación del PNUD sobre la aplicación de esa estrategia en 2007, se ha obtenido sólo el 30% de resultados.

El país ya ha reconocido la importancia de facilitar el acceso a tecnologías y servicios modernos a todos los ciudadanos y a todas las empresas. El cibergobierno y los servicios electrónicos ofrecerán a la administración estatal la posibilidad de utilizar las tecnologías de la información para proponer mejores servicios a los ciudadanos, a las empresas y a otros actores de la gobernanza.[9]

- El Ministerio de Finanzas de la República Kirguisa lanzó en 2012 algunas ciberiniciativas sobre transparencia presupuestaria (www.okmot.kg), por ejemplo: "Presupuesto transparente" (http://budget.okmot.kg), un sistema automático de suministro de datos sobre los ingresos y

[9] Presentado en la tercera reunión de la CE 2 el 17 de septiembre de 2012.

gastos del presupuesto central y los presupuestos locales. Es la primera vez en la historia del país que los ciudadanos de a pie y las personas jurídicas tienen libre acceso a una información completa sobre la aplicación del presupuesto del Estado. Los datos presentados consisten en informaciones detalladas provenientes tanto de particulares como de los organismos gubernamentales y las regiones. Los datos se actualizan en línea mediante la interconexión electrónica con la base de datos del Tesoro Central; "Compras en línea del Estado" (http://zakupki.okmot.kg), un sistema automático para las compras del sector público, incluidas inscripción en línea, participación en ofertas y otras informaciones y acciones afines; "Mapa económico en línea" (http://map.okmot.kg), un mapa electrónico de la República Kirguisa en el que pueden visualizarse todos los datos socioeconómicos de cada localización geográfica del país.

- El **Comité Nacional de Estadísticas** de la República de Kirguistán trabaja activamente en la puesta en práctica de la recopilación y análisis de datos estadísticos por medios electrónicos. Ese organismo ha elaborado y aprobado sus estrategias institucionales en materia de TIC hasta 2020.
- Ciertos organismos estatales, como la **Comisión de Impuestos** y la entidad encargada de la **Gestión de aduanas y fronteras**, también utilizan herramientas electrónicas en sus actividades (declaración en línea, intercambio de datos electrónicos entre organismos, etc.).
- El **Fondo Social**, el **Fondo de Seguro Médico Obligatorio**, el **Ministerio de Salud** y el **Ministerio de Desarrollo Social** modernizan regularmente sus sistemas de información y sus bases de datos para la prestación de servicios sociales por medios electrónicos y el intercambio de datos.
- El **Ministerio de Justicia** y el **Ministerio del Interior** comenzaron a utilizar documentos en línea y herramientas electrónicas para sistemas adecuados de gestión de recursos humanos.
- El **Ministerio de Relaciones Exteriores** está empezando a utilizar una serie de documentos y visados electrónicos.

Debido a la experiencia práctica en la introducción de diferentes proyectos sectoriales de servicios electrónicos, los dirigentes gubernamentales comprendieron la necesidad de fomentar las TIC para el desarrollo nacional. La falta de coordinación de actividades en la materia puede ocasionar la duplicación de tareas y la utilización ineficaz de los recursos aportados por los donantes y el propio Gobierno. La descoordinación de los trabajos entre los organismos origina nuevas dificultades en la interconexión electrónica. La creación de un órgano eficaz de coordinación de las TIC, el establecimiento de normas nacionales de interfuncionamiento electrónico y una infraestructura integrada y unificada para servicios electrónicos son esenciales para la implantación satisfactoria del cibergobierno en la República Kirguisa.

3.8 Actividades encaminadas a facilitar el acceso a sistemas administrativos con terminales móviles gracias a la cooperación entre servicios en Japón

"La nueva estrategia en el plan general de las tecnologías de la información y la comunicación (TIC)" formulada por la Jefatura Estratégica para la promoción de una sociedad de redes avanzadas de la información y las telecomunicaciones, presenta los siguientes objetivos relativos a los programas de diversificación de métodos para acceder a los servicios administrativos, en relación con la renovación del portal gubernamental, y para alentar a la población a acceder a los servicios estatales; en 2011, discusión, verificación y demostración del método para el acceso móvil a los servicios administrativos con autenticación desde teléfonos móviles; de 2012 a 2013, teniendo en cuenta la demostración del método indicada *supra*, introducir, crear y promover servicios en forma parcial en zonas de prueba e implantarlos gradualmente en todo el país; en 2020, implantar servicios administrativos electrónicos de suma utilidad, a saber, un "servicio de ventanilla única".

Sobre la base de dicho programa, el MIC llevó a cabo en 2011 el proyecto "Promover sistemas administrativos para la cooperación entre servicios (Verificación de métodos para mejorar la practicidad de los teléfonos móviles utilizados como medio de acceso)", teniendo en cuenta los resultados de una "investigación y estudio de la diversificación de medios de acceso a servicios administrativos electrónicos, etc. (investigación y estudio de la tecnología de telefonía móvil para acceder a servicios administrativos electrónicos, etc.)" llevada a cabo en 2009.

Los terminales móviles con funciones NFC (*Near Field Communication*, comunicaciones de campo cercano) se comercializaron en 2012. En dispositivos a prueba de manipulaciones, esas funciones protegen, en línea o fuera de línea, la información personal del usuario del servicio, que puede ser información de autenticación (como identificadores/contraseñas, puntos y cupones), y además permiten la lectura de esa información. Con esas funciones, la autenticación de los usuarios es más práctica cuando se accede con terminales móviles a servicios de cibergobierno; y todos los ciudadadanos, cualesquiera sea su edad, tienen un acceso fácil y seguro a los servicios administrativos a través de terminales móviles.

En la investigación llevada a cabo por el MIC en 2009 se examinó la seguridad de los siguientes espacios de almacenamiento de información de identidad facilitados para los usuarios por los proveedores de servicios como medio de acceso móvil a los servicios de cibergobierno: 1) sistema de tarjetas públicas de circuito integrado, que se utiliza colocando la tarjeta nacional de identidad emitida por el gobierno cerca del teléfono móvil, 2) sistema de tarjetas públicas para teléfonos móviles, que se utiliza insertando en los terminales móviles tarjetas aptas emitidas por el gobierno, 3) sistema de información de identificación público, que se utiliza anotando en los terminales móviles la información facilitada por el gobierno, etc. Se supone que los dispositivos a prueba de manipulaciones son 1) tarjetas de circuito integrado de tamaño natural para el sistema de tarjetas nacionales de identidad, 2) dispositivos de memoria flash que contienen circuitos integrados del sistema de tarjetas públicas para teléfonos móviles, 3) UICC (tarjeta de circuito integrado universal) para el sistema de tarjetas nacionales de identidad.

Sin el examen indicado *supra*, para almacenar y utilizar la información de identificación o la información de los usuarios en dispositivos a prueba de manipulaciones, era necesario crear y explotar una aplicación de teléfonos móviles (en adelante, aplicación móvil) para cada proveedor de servicios. Por otra parte, los usuarios debían descargar e instalar aplicaciones móviles independientes suministradas por los proveedores de servicios. En otras palabras, tanto proveedores de servicios como usuarios tienen inconvenientes cuando se proporciona un servicio a prueba de manipulaciones. Con la intención de crear un entorno propicio a los usuarios y de fácil utilización y explotación para los proveedores de servicios, se examinaron especificaciones técnicas para llevar a cabo el sistema de acceso móvil.

Con miras a resolver las dificultades planteadas, se ha estudiado un sistema que pueden utilizar a la vez usuarios y proveedores de servicios. En otras palabras, se examinaron las especificaciones técnicas de un sistema de acceso móvil formado por servidores que permiten el almacenamiento y la lectura de forma segura, en lugar de que cada proveedor de servicios, con una aplicación móvil utilizada en común para todos los servicios, almacene y utilice la información de identificación en dispositivos a prueba de manipulaciones. Asimismo, se estudiaron la verificación mediante la experimentación con especificaciones técnicas, la especificación de problemas a la luz de la institución y su funcionamiento, y las soluciones a esos problemas.

Cada vez más los habitantes de los países en desarrollo tendrán terminales móviles; asimismo, en esos países sigue aumentando el número de usuarios de teléfonos inteligentes. Habría que pensar que en los países en desarrollo también es necesario un ámbito consagrado a los servicios públicos.[10]

3.9 Cibergobierno en el Líbano

El plan general de cibergobierno se funda en el sólido compromiso de nuestras autoridades gubernamentales de construir un portal de cibergobierno con la intención de mejorar y facilitar el acceso de los ciudadanos a los servicios públicos y a la información pública.

La iniciativa de cibergobierno da prioridad al cumplimiento de los siguientes objetivos estratégicos: una administración pública centrada en los ciudadanos (y no en la burocracia), orientada a los resultados y

[10] Presentado en la tercera reunión de la CE 2 el 17 de septiembre de 2012.

basada en el mercado (promoción activa de la innovación) tiene una buena gobernanza y asegura el desarrollo económico y la integración social[11].

- Ciberreforma: brinda la oportunidad ideal para reestructurar los procesos de la administración pública con la finalidad de aprovechar las ventajas de la tecnología y utilizar las TIC como punta de lanza del proceso de reforma.
- Ciberciudadano: agrupa a todos los servicios que las autoridades gubernamentales proponen actualmente a los ciudadanos del Líbano y cuya prestación puede efectuarse por medios electrónicos.
- Ciberempresa: privilegia los servicios públicos que revisten importancia para la comunidad de empresas libanesas y los inversores extranjeros. Una prestación más eficaz de esos servicios contribuirá a fomentar el crecimiento del sector privado en el país y a obtener resultados en el desarrollo económico nacional
- Cibercomunidad: se ha obtenido un consenso amplio con respecto al hecho de que las TIC son fundamentales para participar en la incipiente economía del conocimiento, tienen grandes posibilidades de acelerar el crecimiento económico, promueven el desarrollo sostenible y el empoderamiento, y reducen la pobreza.
- Diferentes iniciativas de cibergobierno en diferentes ámbitos: jurídico, infraestructura de las TIC, aplicaciones verticales y diferentes normas y políticas nacionales.

Se entiende por plan general de cibergobierno el conjunto de macroactividades e hitos esenciales con distintas perspectivas: jurídica, administrativa, en materia de infraestructura, reestructura de procesos administrativos, interfuncionamiento y portal de cibergobierno. Este plan general estará respaldado por un programa de creación de capacidades gracias al cual los funcionarios públicos podrán aplicar con efectividad y eficacia todos los proyectos de cibergobierno.
La próxima etapa será preparar diferentes proyectos de ley, decisiones y proyectos técnicos que podrían ser adoptados por el Gobierno de Líbano como, por ejemplo:

- Proyecto de ley – Transacciones electrónicas
- Proyecto de ley – Ley sobre escala salarial de las TI
- Adopción de la ley sobre transacciones electrónicas
- Simplificación de procedimientos.

3.10 MWANA (Zambia)

El papel y la incidencia de las TIC en Zambia han aumentado rápidamente debido a factores sociales y al avance pujante de las TIC. Según la encuesta ZICTA relativa a la utilización de las TIC, en Zambia, que tiene una población de 12 millones de habitantes, 7,8 millones tienen acceso a servicios móviles y 4 millones, a Internet. El aumento de la demanda de servicios en la comunidad y la mayor utilización de las TIC ha obligado a las autoridades públicas y al sector privado a ser más innovadores y a realizar importantes inversiones en los enlaces de conexión a las telecomunicaciones.[12]

- Para reafirmar el diagnóstico infantil precoz con el doble propósito de aumentar el número de madres que reciben resultados y atenderlas de manera más rápida y eficaz, utilizando la aplicación SMS (mHealth).

[11] Presentado en la tercera reunión de la CE 2 el 17 de septiembre de 2012.

[12] Presentado en la tercera reunión de la CE 2 el 17 de septiembre de 2012.

- Para mejorar la tasa de seguimiento posnatal y aumentar el número de inscripciones de nacimiento en las clínicas y en la comunidad, incrementando a la vez el número de visitas médicas realizadas por las madres gracias al rastreo efectuado por agentes de la salud comunitaria, utilizando la aplicación "RemindMi.
- Para mejorar la prestación de servicios estatales a los ciudadanos.
- Para reducir la burocracia y el tiempo invertido en la prestación de servicios estatales.

Tecnologías y opciones implantadas:

- Tecnología SMS – Innovación de gran alcance que, en Zambia, ha reducido las demoras para recibir un diagnóstico infantil precoz (EID, early infant diagnosis) a partir de los resultados de las pruebas del VIH por DBS, ha mejorado la comunicación entre profesionales de la salud y voluntarios de la comunidad, y, lo más importante, alienta a los pacientes a regresar con mayor confianza a la clínica a retirar los resultados de las pruebas.
- Tecnología RapidSMS – Se ocupa del diagnóstico infantil precoz del VIH. Desde los laboratorios que han realizado los correspondientes análisis, se envían mensajes SMS con los resultados del VIH a las unidades de la clínica donde se han recogido las muestras. En las clínicas más pequeñas, los resultados llegan por teléfono, y en las más importantes, a través de impresoras de SMS. El sistema también realiza un seguimiento de las muestras y ofrece un control en tiempo real para funcionarios provinciales y de distrito.
- RemindMI – Esta tecnología está destinada al seguimiento de la atención postnatal del paciente. Se envían mensajes SMS a los agentes de la comunidad para que busquen a los niños y a quienes se encargan de su cuidado y les pidan que regresen a la clínica para efectuar un control a los 6 días, 6 semanas y 6 meses después del parto o en circunstancias especiales, por ejemplo, cuando llegan los resultados a la unidad correspondiente.

Se ha creado un plan de desarrollo nacional, que comienza con una etapa de preparación seguida por una etapa iterativa durante la cual se imparte capacitación en las clínicas añadiéndolas al sistema y se evalúan los problemas y los resultados satisfactorios de esa inclusión. El objetivo es que, en 2015, los establecimientos encargados de la salud ofrezcan servicios de diagnóstico infantil precoz en todo el país. La etapa de preparación privilegiará el reforzamiento de la infraestructura técnica, física, de seguimiento y humana para que el sistema logre afrontar las tensiones de escala. Durante todo su desarrollo, el proyecto estará sujeto a un estricto control para garantizar que los sistemas tengan un efecto positivo en problemas de salud específicos.

3.11 Servicio de cibergobierno en Montenegro

Consciente de la importancia del desarrollo y la utilización de las TIC, Montenegro ha dado pasos considerables al respecto en el pasado. Esto se ha reconocido con claridad en la clasificación del Foro Económico Mundial, el Índice de preparación a la red, según la cual Montenegro ocupa la 44ª posición entre los 138 países presentes, muy por encima de otros países europeos de la región. Con un crecimiento del número de usuarios de redes móviles de casi el 200% y un aumento constante de usuarios de Internet, no cabe duda que el sector de las TIC en el país está registrando un intenso crecimiento[13].

- Sostenibilidad de las TIC – con los siguientes programas: aspectos básicos de las TIC (marco tecnológico, un marco del espectro de frecuencias radioeléctricas, un marco para la protección de los consumidores), infraestructura de las TIC, marco jurídico y normativo, seguridad de la

[13] Presentado en la tercera reunión de la CE 2 el 17 de septiembre de 2012.

información con el objetivo de mejorar la infraestructura de banda ancha, marco jurídico y normativo concebido para crear un sector de las TIC competitivo y sostenible.

- TIC para la sociedad – con los siguientes programas: cibereducación, cibersalud, integración en la esfera electrónica, con el objetivo de alentar a todos los actores de la sociedad a utilizar tecnologías modernas.
- Las TIC en la administración pública – con el programa de cibergobierno, que alienta a la administración pública a utilizar las tecnologías de la información y la comunicación de forma innovadora para mejorar la calidad de los servicios prestados por las autoridades estatales.
- Las TIC para el desarrollo económico – un programa de tecnologías TIC para I + D (investigación y desarrollo) y para la innovación aplicadas a la evolución de la ciencia y la investigación con el fin de crear sistemas TIC productivos y sostenibles a través del establecimiento de una base de datos de expertos y del fomento de la creatividad y el espíritu empresarial.
- Con la intención de implantar el cibergobierno en Montenegro, el Ministerio de la Sociedad de la Información y las Telecomunicaciones creó el portal web del proyecto de cibergobierno, www.euprava.me (el portal), a través del cual todas las instituciones de la administración pública y de las unidades de los gobiernos autónomos locales prestarán servicios electrónicos a personas físicas y jurídicas y a otras instituciones.
- eDMS (sistema electrónico de gestión de documentos) es un proyecto cuyo principal objetivo es la informatización de las oficinas del Gobierno de Montenegro, con el fin de aumentar la eficacia, ahorrar tiempo, reducir costos y ofrecer una gestión de la documentación de mejor calidad.

Los próximos pasos y actividades darán prioridad al marco de interfuncionamiento (que, por su naturaleza, no es un documento técnico) dirigido a quienes participan en la definición, el diseño y la prestación de servicios públicos.

Aunque en la mayoría de los casos la prestación de servicios públicos supone el intercambio de datos entre sistemas de información, el interfuncionamiento es un concepto más amplio dado que brinda la posibilidad de organizar conjuntamente los trabajos respondiendo a objetivos acordados de común acuerdo y por lo general ventajosos.

4 Herramientas para prácticas óptimas

4.1 Conjunto de herramientas para servicios TIC utilizando comunicaciones móviles

[14] El conjunto de herramientas para la creación de servicios TIC describe la utilización de las comunicaciones móviles para los servicios de cibergobierno y la manera de integrar todos los servicios móviles que necesitan una autenticación y una conexión segura, como los servicios móviles de cibergobierno (gobierno móvil), el pago móvil, la banca móvil y la salud móvil. En esta parte del Informe se describen los principios generales de la creación de dichos servicios y se enumeran las Recomendaciones del UIT-T relativas a los aspectos de seguridad.

- Además de su objetivo principal (comunicaciones vocales y transferencia de mensajes entre usuarios), las comunicaciones móviles son sumamente útiles para otras aplicaciones, como el comercio móvil, la salud móvil, el gobierno móvil y otras. Sin embargo, hay que comprender que el gobierno móvil es sólo uno de los diversos medios de comunicación electrónica con la administración pública, y lo mismo se aplica a los sistema de salud móvil, educación móvil, comercio móvil y pago móvil.

[14] Resumen de la contribución presentada por Intervale. El documento completo figura en el Anexo.

A pesar de las pequeñas dimensiones de sus pantallas y teclados, los teléfonos móviles ofrecen grandes posibilidades a los usuarios de servicios de cibergobierno. Debido a la extrema rapidez de la evolución tecnológica actual y a las ventajas considerables de las comunicaciones móviles, los ciberservicios basados en terminales móviles *(gobierno móvil, salud móvil, pago móvil, aprendizaje móvil, etc.)* son muy prometedores. En efecto:

- no todos disponen de una computadora personal pero, por lo general, cada uno de nosotros tiene un teléfono móvil (según el Informe de la UIT, "Tendencias en las reformas de telecomunicaciones 2012", a finales de 2011 había en todo el mundo 6.000 millones de abonados móviles y prácticamente 3.000 millones de usuarios de Internet;
- los teléfonos móviles siempre están cerca de sus usuarios y están conectados permanentemente;
- en algunos casos, las comunicaciones móviles pueden ser la única forma de comunicación disponible;
- las comunicaciones móviles son al menos tan seguras que Internet.

4.1.1 Principios aplicados a la seguridad de los servicios móviles

Por lo general, los sistemas móviles utilizados en la prestación de servicios a distancia seguros (servicios móviles de cibergobierno, cibermedicina o comercio electrónico), deben presentar una infraestructura que procure la transmisión segura de bloques de datos entre los usuarios del terminal móvil y el proveedor de servicios. Como garantía de seguridad, esa estructura debe contar con un elemento de autenticación y criptado. Los bloques de datos transmitidos pueden contener información confidencial que exige un tratamiento seguro. El intercambio de datos tiene que llevarse a cabo únicamente entre usuarios autorizados, no debe ser accesible a terceros y debe estar debidamente registrado para evitar los riesgos de no repudio. La autenticación del usuario será el resultado de la autenticación de numerosos factores.

4.1.2 Identificación y autenticación

A los fines de la identificación, es necesario que el cliente valide su identidad y cree un enlace único entre su dispositivo móvil y su cuenta en la base de datos del proveedor de servicios. Tras la identificación inicial, el cliente deberá recibir un "código secreto" que autenticará sus futuras relaciones con ese proveedor de servicios. El "código secreto", también llamado “firma móvil", es uno de los factores de autenticación. En la práctica, la firma móvil es una clave criptográfica única que también puede servir para criptar los datos. Por ese motivo, la utilización de claves permite la criptación de los datos y la autenticación del usuario. El segundo factor de autenticación puede ser suministrado por el código PIN o contraseña del usuario, que permite el acceso a las aplicaciones instaladas en el teléfono. Ese código PIN impide que las aplicaciones sean utilizadas sin autorización.

Los sistemas de pago móvil actuales ya han establecido sus propios procedimientos de seguridad, cuyos requisitos están determinados por acuerdos concertados entre los proveedores de servicios y sus clientes. Evidentemente, los servicios de cibergobierno necesitan un sistema de seguridad controlado por el Estado y que cumpla las disposiciones de la legislación nacional relativa a la firma electrónica. El sistema debe garantizar la transmisión segura de datos confidenciales entre los organismos públicos y los usuarios autorizados, y proporcionar al mismo tiempo firmas electrónicas. Se puede utilizar también para servicios de cibersalud y otros servicios de reciente creación cuyos datos deben ser protegidos. Y aunque los sistemas privados de pago móvil tengan probablemente sus propios medios de protección, no hay que descartar soluciones complejas, que propongan una autenticación centralizada, y ciertos proveedores de servicios (frecuentemente, de servicios financieros) utilizan sus propios procedimientos de criptación y verificación. Por lo tanto, parece razonable ofrecer, con las aplicaciones móviles, varios bloques independientes con diferentes conjuntos de claves. En la Figura 2 se observa un modelo de autenticación unificada para dispositivos que admiten servicios móviles e Internet.

Aunque hay numerosos centros de identificación y autenticación, todos ellos utilizarán reglas unificadas para expedir a sus clientes identificadores móviles o mID, registrados en el directorio del sistema central, para asegurar el encaminamiento adecuado de los mensajes. El cliente puede tener numerosos mID pero tendrán que guardar relación con su MSISDN (número RDSI internacional de estación móvil).

La opción Service Enabler (activador de servicio) presta apoyo tecnológico y desempeña un papel muy importante en esta estructura. Asegura la integración de varios medios de acceso, el interfuncionamiento con los proveedores de servicios y el centro de autenticación, y proporciona a los usuarios aplicaciones para esos medios de acceso (computadoras personales y terminales móviles).

Todos los centros de identificación y autenticación deben cumplir las mismas reglas que rigen la atribución de identificadores mID, registradas en el directorio del sistema central para garantizar la transmisión de mensajes a los clientes.

4.1.3 Administración de claves

La criptografía se puede utilizar con claves simétricas y asimétricas para criptar los datos transmitidos y crear firmas móviles. La ventaja de la criptación simétrica (normas 3DES, AES) es que utiliza algoritmos de fácil aplicación en dispositivos informáticos de bajo costo. Generar una clave simétrica es una operación sencilla que no requiere medios especiales. Sin embargo, por definición, la utilización de la misma clave, compartida entre el usuario y el proveedor de servicios (centro de autenticación del proveedor), podría dar lugar a que el usuario impugne la transacción completada. Hay que señalar que los sistemas de pago móvil, que han logrado crear sistemas fiables de registro de transacciones en caso de controversia, utilizan sin ningún problema la criptografía de claves simétricas.

La criptografía de claves asimétricas utiliza la infraestructura de clave pública (PKI) para vincular dos claves diferentes pertenecientes a una misma persona: la clave "pública", con una identidad de dominio pública, y la clave "privada", cuyo almacenamiento es seguro y está protegida contra todo acceso no autorizado (por ejemplo, en una tarjeta SIM o en una tarjeta inteligente especialmente protegida). Las interacciones matemáticas entre claves se efectúan de tal forma que una acción realizada con una clave puede estar "vinculada" a otra clave, sin que se revelen los datos relativos a la clave privada. Esto resulta particularmente útil para la creación de una firma electrónica, dado que la firma efectuada por la clave privada identifica al titular de ésta sólo en relación con la clave pública asociada (cuya identidad se conoce). En la tecnología PKI lo más importante es, por una parte, asegurar la "privacidad" de las claves privadas y, por la otra, verificar la relación entre claves abiertas y claves privadas. Esto se consigue mediante una gestión cuidadosa del proceso de registro, cuando se expiden las claves, y del proceso de certificación, que confirma la identidad de la clave pública. Se encargan de gestionar, respectivamente, estos elementos entidades conocidas como autoridades de “registro” y autoridades de “certificación”. Con respecto a la firma móvil, su función principal es reconocer la relación singular establecida entre la utilización de la clave privada y la identidad registrada de la persona, dado que es el titular de la clave pública asociada.

Los métodos de criptación asimétrica necesitan dispositivos informáticos más costosos, pero pueden aplicarse en numerosos modelos de interacción. La "doble clave" ofrece más posibilidad de adaptación y facilita la resolución de controversias. Este enfoque propicia un modelo de confianza más eficaz y la simplificación de la gestión administrativa y de los servicios (por ejemplo, un solo par de claves asimétricas pueden dar soporte a diferentes aplicaciones y modelos de interacción). Por ese motivo, los documentos que describen marcos de interfuncionamiento para firmas electrónicas a escala mundial se refieren casi exclusivamente a métodos de criptación asimétricos.

4.1.4 Seguridad

La seguridad es el requisito más importante para los sistemas de pago y para los servicios de cibergobierno y cibersalud, incluidas sus opciones móviles. Las normas en la materia están contempladas en las Recomendaciones del Sector de Normalización de la UIT, que ha publicado el Manual, "La seguridad de las telecomunicaciones y las tecnologías de la información[6]". Ese Manual ofrece una visión general de

las normas del UIT-T y su aplicación práctica en lo que concierne a la seguridad de las telecomunicaciones. Esas normas deben respetarse. Aunque se trata de Recomendaciones, su cumplimiento es esencial para asegurar la compatibilidad y coherencia de los sistemas de telecomunicaciones de diferentes países.

Dado que estos sistemas contemplan numerosos agentes, las consideraciones en materia de seguridad pueden dividirse en varias categorías:

a) seguridad de los puntos extremos;

b) seguridad de las aplicaciones móviles;

c) seguridad de las redes móviles;

d) identificación del solicitante, que incluye la identificación adecuada de la persona que solicita la transacción financiera.

Antes de la era de los teléfonos inteligentes, la gestión de las aplicaciones móviles en los teléfonos móviles era una labor relativamente fácil para los operadores. Esencialmente, tenían el control de las aplicaciones que podían descargarse en el dispositivo y sus características en materia de seguridad. Con la llegada de los teléfonos inteligentes y la posibilidad de descargar gratuitamente aplicaciones de terceros, la gestión de las aplicaciones móviles se ha vuelto más compleja. Hoy, prácticamente es imposible tener la absoluta certeza de que cada aplicación utilizada en un dispositivo móvil proviene de una fuente fiable. Por ello, los usuarios de sistemas móviles están expuestos a nuevos riesgos, como la usurpación de identidad y la pérdida de datos personales.

Las dimensiones de seguridad definidas y utilizadas correctamente respaldan la política de seguridad definida para una determinada red y facilitan la aplicación de las normas de gestión de la seguridad.

La dimensión de seguridad control de acceso protege contra la utilización no autorizada de recursos de la red. El control de acceso garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. Además, el control de acceso basado en las funciones (RBAC, *role-based access control*) establece varios niveles para restringir el acceso a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones, a las personas y los dispositivos autorizados.

La dimensión de seguridad autenticación se utiliza para confirmar la identidad de las entidades comunicantes. La autenticación garantiza la validez de la identidad que se atribuyen las entidades que participan en una comunicación (por ejemplo, personas, dispositivos, servicios o aplicaciones) y que una entidad no interviene usurpando una identidad o reproduciendo una comunicación anterior sin autorización.

La dimensión de seguridad no repudio evita que una persona o una entidad niegue que ha realizado una acción de tratamiento de datos, proporcionando la prueba de distintas acciones de red (por ejemplo, prueba de obligación, de intención o de compromiso; prueba de origen de los datos; prueba de propiedad; prueba de utilización del recurso). Garantiza la disponibilidad de pruebas que se pueden presentar a terceros y utilizar para demostrar que un determinado evento o acción sí ha tenido lugar.

La dimensión de seguridad confidencialidad de los datos impide que los datos sean divulgados sin autorización. La confidencialidad garantiza la imposibilidad de que las entidades no autorizadas entiendan el contenido de datos. Los métodos utilizados habitualmente son la criptación, las listas de control de acceso o las autorizaciones de archivos.

La dimensión de seguridad comunicación garantiza que la información sólo circula entre los puntos extremos autorizados (no hay desviación ni interceptación de la información que circula entre estos puntos extremos).

La dimensión de seguridad integridad de los datos garantiza la exactitud y la veracidad de los datos. Protege los datos contra acciones no autorizadas de modificación, supresión, creación o reactuación, y señala estas acciones no autorizadas.

La dimensión de seguridad disponibilidad garantiza que las circunstancias de la red no impiden el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. Esta categoría incluye soluciones para la recuperación en caso de anomalía.

La dimensión de seguridad privacidad protege la información que se podría conocer observando las actividades de la red. Por ejemplo: los sitios web visitados por un usuario, la posición geográfica del usuario, las direcciones IP y los nombres de dominio (DNS) de los dispositivos en la red de un proveedor de servicio.

4.1.5 Tecnología móvil

Hasta la fecha, el término "comunicaciones móviles" está asociado por lo general a la norma GSM de la segunda y tercera generación. Esos sistemas utilizan diferentes subsistemas para la voz y la transferencia de datos (tecnologías de conmutación por división de tiempo y de conmutación de paquetes), lo que constituye una etapa intermedia en la evolución de las comunicaciones móviles. Las redes de la próxima generación (NGN), que ya han sustituido las redes actuales, proporcionan a los abonados el acceso en banda ancha y sólo utilizan la tecnología de conmutación de paquetes.

Las NGN ofrecen servicios de transmisión de la voz, imágenes, texto y multimedios, en tanto que aplicaciones del proceso universal de transmisión de datos por lotes. En consecuencia, las tecnologías de transmisión de datos por SMS y MMS, sumamente difundidas en la actualidad, podrían dar paso a nuevas tecnologías sin que los usuarios se dieran cuenta de esos cambios. Con todo, convendría elaborar opciones tecnológicas para servicios móviles que se adaptaran al proceso de evolución de las comunicaciones móviles.

Aunque en la actualidad está muy difundida la utilización de terminales móviles, originalmente no fueron concebidos para sistemas que necesitaban una sólida autenticación. Los terminales de diferentes fabricantes e incluso diferentes modelos de terminales creados por el mismo fabricante, pueden utilizar distintos algoritmos, de ahí su mayor complejidad y, en algunos casos, la incapacidad de crear aplicaciones que realicen todas las funciones necesarias del sistema. Por ejemplo, una aplicación tendría que activarse automáticamente al recibir un mensaje del sistema de pago móvil (enviada por un comerciante). Lamentablemente, una aplicación de ese tipo no puede implantarse en cada terminal móvil.

Para unificar el funcionamiento de esos sistemas, habría que normalizar otros protocolos, tarea de la que podría encargarse la UIT, junto con los fabricantes de equipos. Otra dificultad importante es el emplazamiento de la criptoaplicación y la administración del acceso a esa aplicación. Como se indica en el capítulo correspondiente a la "Seguridad", para lograr un nivel máximo de seguridad, esas aplicaciones deben situarse en un módulo especial (elemento de seguridad del hardware) que proteja las informaciones almacenadas de todo acceso no autorizado. Las tarjetas SIM/UICC pueden servir de módulo, siempre que se resuelva la cuestión de la delegación de derechos administrativos para acceder a la tarjeta SIM, que pertenecen al operador de servicio móvil. Ese problema se resuelve fácilmente cuando ambas funciones son realizadas por la misma entidad; de lo contrario, resulta más difícil. La creación de terminales móviles equipados con un elemento de seguridad de hardware suplementario puede considerarse una solución para resolver los problemas planteados por la gestión conjunta de tarjetas SIM, gracias a un módulo de seguridad incorporado o a una tarjeta memoria a prueba de manipulaciones especialmente instalada.

Hay distintas modalidades de transferencia de datos en las redes móviles, entre ellas CDS, SMS, USSD, GPRS, EDGE y LTE. Cada una tiene ventajas e inconvenientes. Por ejemplo, el sistema SMS es muy fiable y fácil de utilizar pero la longitud de los mensajes está limitada. En cambio, no está limitada en el caso del GPRS, pero este sistema es menos fiable y debe ser adaptado para utilizarse en terminales móviles, especialmente en modo itinerancia, que por otra parte es muy caro. Los avances tecnológicos han llevado a una implantación generalizada de servicios de geolocalización en teléfonos inteligentes con sistemas GPS o GLONASS. Fundamentalmente, la geolocalización amplía las funciones de los terminales móviles, lo que explica que esos servicios de geolocalización sean sumamente utilizados en las aplicaciones para

dispositivos móviles que, debido a su rápido crecimiento, son cada vez con más frecuencia teléfonos inteligentes.

4.1.6 Conclusiones

Como se observa en los casos presentados por la Unión Europea, Japón, EE.UU., Rusia, y otros países, descritos en el Anexo, los niveles de desarrollo y utilización de dispositivos móviles para los servicios de *gobierno móvil, salud móvil, pago móvil, aprendizaje móvil, etc.,* varían de un país a otro. No obstante, en nuestro mundo globalizado la penetración de las innovaciones tecnológicas aumenta de forma espectacular, da paso a una convergencia gradual de los niveles de desarrollo tecnológico y reduce la brecha digital entre los países desarrollados y los países en desarrollo. Hoy, los países desarrollados ya cuentan con sistemas de pago electrónico y de gobierno móvil totalmente funcionales. En ciertos países en desarrollo, con la simple utilización del SMS para transferir datos entre establecimientos médicos se obtienen ventajas concretas puesto que hay menos retrasos en la recepción de un diagnóstico infantil precoz a partir de los resultados de las pruebas del VIH por DBS, como se indicó en la descripción del proyecto MWANA puesto en marcha en la República de Zambia[17]. Es un indicio de que muy pronto se reducirá esta brecha tecnológica. Los sistemas actuales más avanzados para dispositivos móviles ofrecen una gama completa de servicios en constante renovación. Así pues, aparte de los servicios de pago móvil y de banca móvil, los servicios basados en la geolocalización han alcanzado gran difusión. Por otra parte, en el *White Paper Mobile Payments*[18], publicado por el *European Payments Council* en 2012, el terminal móvil deberá constituir un "monedero digital" que sustituya con la autenticación y la firma digital un gran número de contraseñas, documentos de identidad y tarjetas de fidelidad de los comerciantes.

Del mismo modo que un monedero normal, el monedero "digital" contiene información sobre su titular: sus datos de identidad, los medios de pago que tiene a su disposición y, en ciertos casos, datos personales (imágenes, documentos, etc.). Puede haber también informaciones sobre sus documentos de identidad, firmas y certificados digitales, datos sobre la conexión, direcciones para la transmisión de datos, así como información sobre los medios de pago. Asimismo, puede incluir otras aplicaciones como, por ejemplo, puntos de bonificación, billetes o documentos de viaje. Una vez aprobada la autenticación por la central, se puede tener acceso a una cuenta personal del comerciante o navegar por las redes sociales (Facebook, LinkedIn y otras), lo cual es muy práctico y evita la necesidad de memorizar o guardar en forma segura numerosas contraseñas vinculadas a varias cuentas. A corto plazo, cabe esperar que los dispositivos móviles se utilicen como terminales para servicios de cibergobierno y cibersalud, como lo prueban iniciativas recientes en la materia formuladas en ITU Telecom 2012 por la UIT y la OMS.

El rápido desarrollo de sistemas para dispositivos móviles se debe a las medidas de seguridad aplicadas a los servicios. Las medidas de seguridad, elemento común esencial para los servicios de cibergobierno, los servicios financieros y la cibersalud, deben ajustarse a las Recomendaciones del UIT-T.

Gracias a esas Recomendaciones, la criptografía, que se utiliza en la autenticación y codificación de datos transferidos en sustitución de las contraseñas utilizadas en los sistemas anteriores, ha reforzado considerablemente la seguridad de los dispositivos móviles y facilitado su empleo, dando lugar a una mayor difusión de los servicios implantados en esos dispositivos.

4.1.7 Recomendaciones

- Puesto que el teléfono móvil ha logrado implantarse completamente en el mercado y ofrece servicios de excelente calidad, el terminal de pago ideal y un instrumento de comunicación seguro.
- Es importante ofrecer interfaces de teléfono móvil fáciles de usar en todo tipo de dispositivos y que respondan a las exigencias de los usuarios, aunque los teléfonos inteligentes más avanzados tengan magníficas pantallas a color e interfaces táctiles. Las condiciones de utilización dependen en gran medida del pequeño formato del aparato que, por ejemplo, limita la cantidad de información que puede visualizarse y la posibilidad para el usuario de introducir textos complejos.

- El dispositivo móvil es un "monedero "digital" que almacena información sobre su titular: sus datos de identidad, los medios de pago que tiene a su disposición y, en ciertos casos, datos personales (imágenes, documentos, etc.). Puede haber también informaciones sobre sus documentos de identidad, firmas y certificados digitales, datos sobre la conexión, direcciones para la transmisión de datos, así como información sobre los medios de pago. Puede incluir también otras aplicaciones, como cartas de fidelidad, documentos de transporte o billetes.
- Se aconseja a los clientes que no se comprometan con un solo banco o a un solo operador de redes móviles, y que se reserven la posibilidad de elegir el proveedor de servicios.
- Las partes que participan en un diálogo por medios electrónicos deben ser autorizadas a utilizar una autenticación con dos factores como mínimo, y la transferencia de datos debe realizarse en forma segura con ayuda de medios criptográficos.
- Se aconseja utilizar el nivel de seguridad 4 ó 3, de conformidad con la Recomendación UIT-T Y.2740.
- Los clientes deben conocer el nivel de seguridad del sistema, que se estipulará en el acuerdo de los participantes. La autenticación del usuario puede ser efectuada por el centro correspondiente.
- Para garantizar la seguridad, el dispositivo móvil debe tener una aplicación especial para servicios móviles que asegure la autenticación y la criptación.
- La perspectiva más realista corresponde a la de un mercado en el que coexistirán numerosas aplicaciones, con varios servicios disponibles en un solo dispositivo móvil.
- La inscripción y la puesta en servicio de una aplicación móvil debe realizarse en un entorno seguro. El acceso a esa aplicación sería más fácil para el cliente si pudiera mantener una relación de confianza con su proveedor de servicios.
- Para lograr un nivel máximo de seguridad, las aplicaciones móviles deben situarse en el elemento de seguridad del hardware.
- La elección del elemento de seguridad tiene una incidencia importante en el modelo de servicio y en las funciones de las diversas partes interesadas. Hasta el momento se utilizan tres tipos de elementos de seguridad: tarjeta UICC, elemento de seguridad integrado y elemento de seguridad amovible, por ejemplo, microtarjeta SD.
- El activador de servicio presta apoyo tecnológico y asegura la integración de varios medios de acceso, el interfuncionamiento con los proveedores de servicios y el centro de autenticación.
- Se recomienda utilizar aplicaciones móviles con varios bloques independientes y diferentes conjuntos de claves.
- El cliente puede tener numerosas identidades móviles (mID) vinculadas a su MSISDN. Se deben establecer normas unificadas para expedir esos números, que quedarán registrados en el directorio central del sistema, para asegurar el encaminamiento adecuado de los mensajes al cliente.
- Todos los centros de identificación y autenticación deben cumplir las mismas reglas de adjudicación aplicadas a los identificadores móviles del cliente (mID), que quedarán registradas en el directorio central del sistema, para asegurar la entrega de mensajes a los clientes.
- Los sistemas móviles deberían utilizar, siempre que sea posible, tecnologías e infraestructuras que ya hayan sido ampliamente difundidas.

4.2 Evaluación de la eficacia del cibergobierno y su incidencia en Corea (República de Corea)

4.2.1 Introducción

En la actualidad son numerosos los proyectos de tecnologías de la información, en particular la creación de sistemas de cibergobierno gigantescos a escala nacional, iniciados no sólo en países desarrollados sino también en países en desarrollo debido al creciente consenso de que fomentarán la eficacia y la transparencia de las actividades comerciales. De todas formas, sin una gestión adecuada de esos proyectos, no se conseguirán los resultados esperados, pudiéndose ocasionar, en el peor de los casos, el despilfarro del presupuesto público. Por ese motivo, en la ejecución de proyectos de tecnologías de la información convendría llevar a cabo una gestión de la eficacia debidamente planificada.

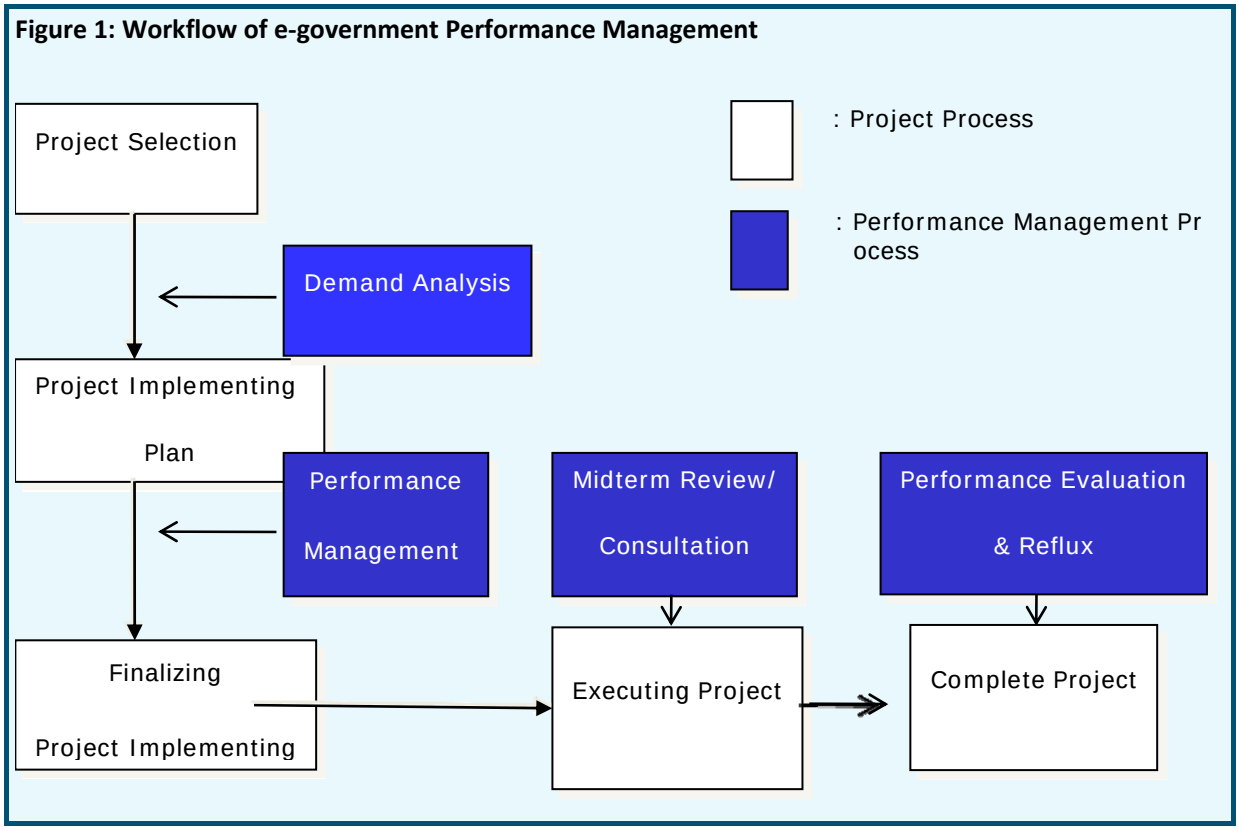
La gestión de la eficacia es un aspecto mucho más amplio que la simple evaluación. Por regla general, la evaluación se realiza inmediatamente después de la finalización del proyecto, en tanto que la gestión de la eficacia persigue un enfoque holístico y, por ello, su objetivo es ofrecer la capacidad de gestionar convenientemente el proyecto. En este sentido, con respecto a la gestión de la eficacia de los proyectos de cibergobierno, las autoridades gubernamentales de Corea han incorporado un enfoque integral en el marco del cual la entidad a cargo de la ejecución de un proyecto de cibergobierno se beneficia de un servicio de consulta previa y de un examen a mitad de periodo.

A continuación se facilita una información más completa sobre el modelo de gestión de la eficacia de proyectos de cibergobierno y sobre las actividades realizadas para difundir esa práctica entre todas las entidades encargadas de la puesta en marcha de ese tipo de proyectos.

4.2.2 Organigrama de la gestión de la eficacia del cibergobierno

La gestión de la eficacia del cibergobierno abarca el proceso completo de aplicación del proyecto, es decir, su selección, ejecución y evaluación. A continuación se presenta el organigrama de la gestión de la eficacia del cibergobierno.

Figure 1: Workflow of e-government Performance Management



Mediante un análisis de la demanda que contiene las dos etapas del proceso de examen, se selecciona un nuevo proyecto que, seguidamente, se confirma. Antes de ejecutar el nuevo proyecto, cada organismo debe elaborar su propio plan de gestión de la eficacia, que describe los métodos que supervisan y evalúan el proyecto, y que deberían por tanto prever una definición clara del objetivo del proyecto, así como la descripción detallada de los indicadores para medir los resultados.

Por consiguiente, el organismo de ejecución debe evaluar el proyecto en función del plan de gestión de la eficacia elaborado. Durante la ejecución del proyecto, se presta un servicio de examen/consulta a mitad de periodo a proyectos de gran escala, un 10% del número total de proyectos de cibergobierno. Este servicio no sólo permite evaluar la situación sino también ofrecer soluciones para resolver los problemas, llegado el caso.

La etapa final de la gestión de la eficacia es su evaluación e incidencia. Todos los proyectos se evalúan con arreglo a cinco categorías: S, A, B, C, D. Un proyecto de la categoría S recibirá la primera prioridad en la asignación presupuestaria siguiente; a veces, un aumento de presupuesto, si fuera necesario. La categoría A indica que se prosigue el proyecto sin ninguna modificación.

Los proyectos de la categoría B se modificarán en la etapa siguiente, en tanto que en los proyectos de la categoría C se deberán introducir importantes modificaciones. Por último, los proyectos de la categoría D deben modificarse completamente; de lo contrario, no recibirán ningún presupuesto.

4.2.3 Orientaciones futuras

Aunque se ha implantado en 2009 en Corea, la gestión de la eficacia del cibergobierno constituye hoy un factor esencial y no una opción. Los proyectos de cibergobierno requieren una gestión más rigurosa de la eficacia que otros proyectos. Por ese motivo, se puso en práctica además un análisis a fondo de la demanda para seleccionar los nuevos proyectos así como un diagnóstico y consultas a mitad de período. Se estima que la gestión de la eficacia proseguirá evolucionando y modificándose para adaptarse a la evolución del entorno en que se aplican los proyectos de cibergobierno.

4.3 eGovFrame: Plataforma de innovación abierta

4.3.1 Panorama general

La aplicación de diferentes marcos de desarrollo plantea numerosos inconvenientes: dificultades para el mantenimiento del sistema, dependencia del proveedor e imposibilidad de interfuncionamiento de los sistemas. Con el fin de resolver estos problemas, el gobierno coreano ha elaborado un marco de elaboración de normas de cibergobierno denominado eGovFrame (*e-Government Standard Framework*, marco normalizado de cibergobierno). Para la normalización del marco informático eGovFrame, las partes interesadas examinaron pormenorizadamente la cuestión. Las grandes empresas temían el derrumbe del mercado, las entidades públicas deseaban saber cómo conseguir una asistencia técnica estable, los diseñadores rechazaban los instrumentos recientemente creados, el gobierno estaba preocupado por la eficacia empresarial y las PYMES, por la promoción de proyectos dirigidos exclusivamente por grandes empresas. Dada la situación, las partes interesadas se vieron obligadas a acordar una normalización del marco informático. Para conseguirla y superar los problemas mencionados, se procedió a aplicar la estrategia de innovación abierta en cuatro fases: (1) fuentes abiertas, (2) procesos abiertos, (3) productos abiertos y (4) ecosistemas abiertos. A continuación se analizan detalladamente el marco eGovFrame y la estrategia de innovación abierta.

El gobierno coreano ha llevado a cabo muchos proyectos de cibergobierno y creado una serie de aplicaciones en la materia. A una parte considerable de esos proyectos se aplicaron marcos informáticos dado que éstos constituyen una herramienta útil para aumentar la productividad y calidad del desarrollo de aplicaciones. En la actualidad, los marcos informáticos son instrumentos muy difundidos para la creación de aplicaciones de cibergobierno, aunque plantean ciertos problemas. Para resolverlos, el gobierno coreano trató de normalizar el marco informático eGovframe. Debido a los diferentes puntos de

vista de numerosas partes interesadas, y con el propósito de superar las dificultades, se aplicó la estrategia de innovación abierta en cuatro fases. Gracias a esa estrategia, se logró normalizar el marco de cibergobierno y establecer el ecosistema abierto de eGovframe.

4.3.2 Antecedentes del marco informático eGovFrame

Corea ha apostado activamente por el cibergobierno, que considera fundamental para que su gobierno sea más competitivo, aprovechando al máximo las tecnologías de la información y la comunicación (TIC) más vanguardistas, como Internet de banda ancha. Tras sentar las bases del cibergobierno, el gobierno coreano comenzó a priorizar la aplicación de éste a escala nacional en la década de 2000. Como consecuencia de estos esfuerzos, el cibergobierno ha quedado sólidamente implantado en todas las áreas gubernamentales del país y producido resultados visibles. En este sentido, la eficacia del cibergobierno coreano ha sido muy aclamada por la comunidad internacional. El cibergobierno coreano es considerado uno de los mejores a escala mundial por organizaciones internacionales como las Naciones Unidas. Además, se están exportando diferentes sistemas de cibergobierno a otros países.

Para lograr estos resultados, el gobierno coreano ha puesto en marcha numerosos proyectos de cibergobierno y elaborado muchas aplicaciones relacionadas con el concepto. Se han aplicado marcos informáticos a muchos de los proyectos mencionados. Estos son instrumentos muy útiles que permiten aumentar la productividad y la calidad del desarrollo de aplicaciones. Hoy en día se han convertido en un instrumento muy utilizado para el desarrollo de aplicaciones de cibergobierno. Por otra parte, el uso de dicho marcos informáticos también ha planteado algunos inconvenientes.

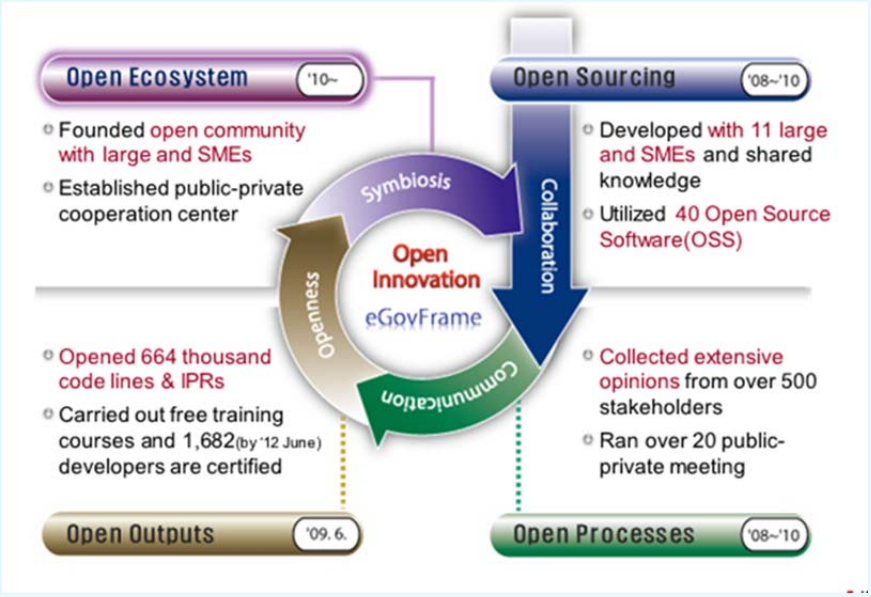
Al utilizar marcos informáticos, los proyectos de cibergobierno pasan a depender en gran medida de las empresas informáticas, por lo que resulta complicado mantener una aplicación sin contar con el apoyo del proveedor de marcos que creó la aplicación original. En caso de proyectos continuos, el marco que se aplicó en el proyecto anterior se convierte en un obstáculo técnico para el nuevo competidor, lo cual crea un injusto círculo vicioso en el mercado informático. La dependencia a las empresas informáticas plantea una serie de problemas. En primer lugar, la lógica empresarial de una aplicación depende a su vez de un marco determinado. En segundo lugar, y puesto que algunos marcos son de tipo “caja negra”, tan solo el proveedor puede mantener la aplicación, lo cual consolida la postura del proveedor de marcos. En tercer lugar, el uso de varios marcos provoca el solapamiento de actividades en la configuración de los procesos de la aplicación, la contratación, la formación y el mantenimiento.

Para superar estos problemas, el gobierno coreano optó por normalizar un marco informático, el eGovFrame, integrado por una serie de herramientas informáticas normalizadas para el desarrollo y la ejecución de aplicaciones de cibergobierno, lo cual permite mejorar la eficacia de la inversión en TIC y la calidad de los servicios de cibergobierno. Se centra en optimizar la capacidad de reutilización y la interoperabilidad de las aplicaciones de cibergobierno fijando un marco normativo para el desarrollo de programas informáticos de cibergobierno, garantizando la independencia de la empresas informáticas con la adopción de herramientas informáticas abiertas y neutras, y mejorando la competitividad de las PYMES informáticas al permitir que se compartan las herramientas de forma abierta a través de varias vías.

4.3.3 Estrategia de innovación abierta

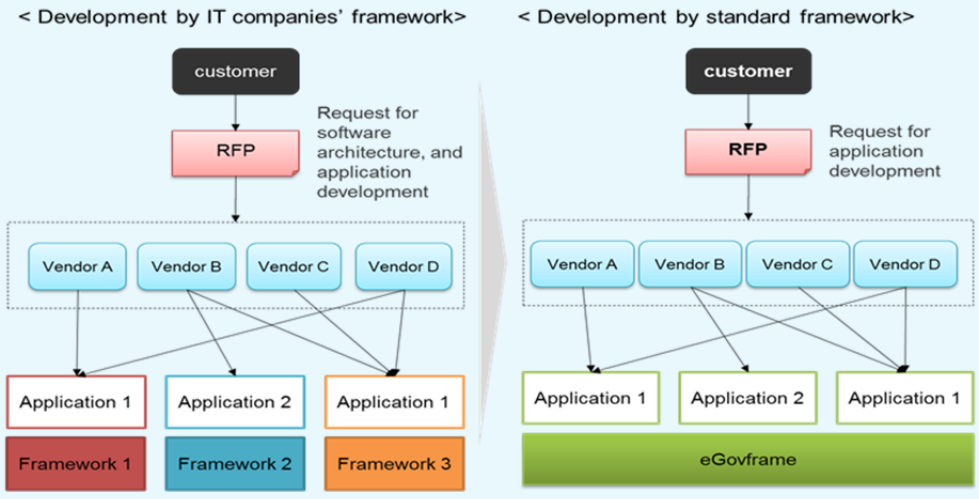
Con el fin de solucionar los problemas derivados de la normalización del marco informático de cibergobierno, se implantó una estrategia basada en un paradigma de innovación abierta denominado estrategia de innovación abierta. Para ello no bastaba con el impulso y la promoción gubernamentales, sino que también se precisaba de los conocimientos, la participación, la cooperación y los comentarios de numerosas partes interesadas en el proceso. A efectos de organizar las necesidades para la normalización y aplicación del marco de cibergobierno, se elaboró una estrategia de 4 fases: fuentes abiertas, procesos abiertos, productos abiertos y ecosistema abierto. La figura 2 representa la estructura general de la estrategia de innovación abierta.

Figure 2: Open Innovation Strategy Open sourcing



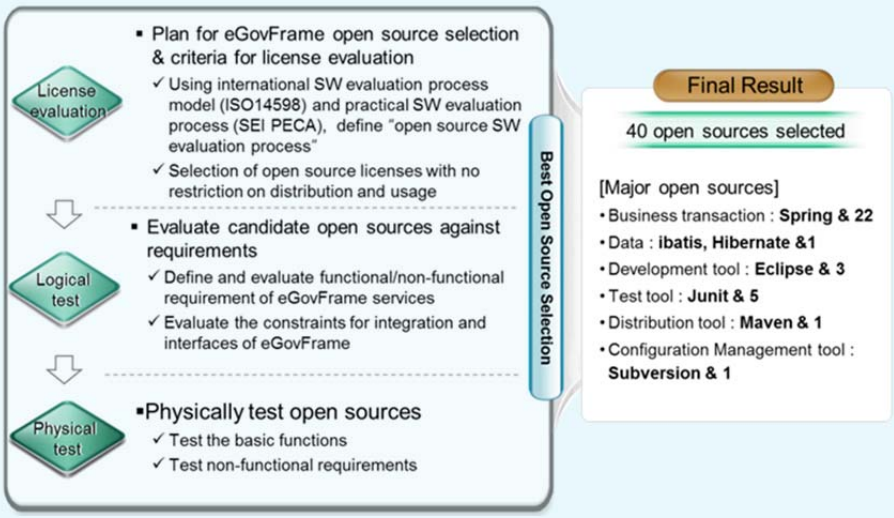
Con el fin de normalizar eGovFrame, se realizaron análisis de entorno y de funcionalidad de los marcos de las cinco principales empresas del sector de las TI, así como un estudio y detalladas entrevistas a todas las partes interesadas. A raíz de esta iniciativa se comenzó a trabajar con cuatro entornos integrados por 13 grupos de servicios y 54 funcionalidades de servicios. Para evitar el desarrollo en paralelo de las mismas funciones en diferentes sistemas gubernamentales, se realizó un análisis de 67 proyectos de cibergobierno, de los años 2004 a 2007; concretamente, se examinaron 31 114 funcionalidades. Los criterios de extracción de funcionalidades comunes para los componentes fueron los siguientes: elevada probabilidad de trabajos de desarrollo reiterados, reutilización de sistemas gubernamentales y adopción de las normas. Después de someterlos a cinco procesos de control de calidad, se definieron 219 componentes comunes.

Figure 3: To-be image of eGovFrame



Para reducir la dependencia con respecto a las principales empresas informáticas, se seleccionaron fuentes abiertas fiables y bien conocidas. Con ayuda del modelo internacional de proceso de evaluación de software (ISO 14598) y el proceso práctico de evaluación de software (SEI PECA), se procedió a definir el proceso de evaluación de software abierto de eGovFrame. Durante la primera prueba lógica, se evaluaron 175 softwares de fuente abierta, haciéndose especialmente hincapié en requisitos sobre las limitaciones de integración y de las interfaces de eGovFrame. Durante la segunda prueba física se evaluaron 85 softwares de fuente abierta derivados de la primera prueba lógica. Se examinaron sus funciones básicas y sus requisitos no funcionales. A continuación se seleccionaron 40 softwares de fuente abierta que pasaron a integrar eGovFrame. El marco eGovFrame de fuente abierta presenta numerosas ventajas. Puede adoptar fácilmente tecnologías que evolucionan a gran velocidad, y ser utilizado en aplicaciones de cibergobierno en el extranjero.

Figure 4: Evaluation and final selection of open source Open processes



Los procesos de desarrollo están abiertos al público que crea el entorno necesario para reunir numerosas opiniones entre más de 500 partes interesadas. Además, se organizaron más de 20 reuniones con el sector público y el sector privado, gracias a las cuales las numerosas partes interesadas lograron comprenderse mejor y llegar a un consenso.

Figure 5: Many stakeholders of eGovFrame

Resultados abiertos

Todos los productos están abiertos al público, como los códigos fuente y los diagramas entidad-relación. Están disponibles en el sitio web de eGovFrame (www.egovframe.go.kr), que constituye un entorno que propicia la participación voluntaria de diseñadores, proveedores y funcionarios públicos en el proceso de aplicación. Además, se han organizado cursos gratuitos de formación y 1.236 diseñadores han recibido una certificación.

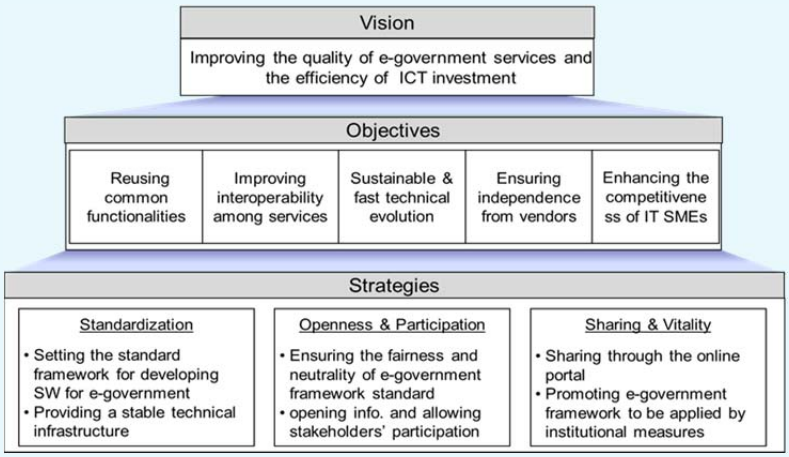
Ecosistema abierto

Se ha creado una comunidad abierta con participación de grandes empresas y PYMES, así como un centro de cooperación público-privada. Constituyen el punto central encargado de la promoción de eGovFrame a escala mundial, la prestación de asistencia técnica sólida y la introducción permanente de mejoras. La comunidad abierta, las reuniones trimestrales de expertos y el foro abierto de representantes de los sectores público y privado contribuyen al perfeccionamiento constante de eGovFrame. Gracias a todo lo anterior se ha creado un ecosistema abierto para eGovFrame

4.3.4 Cambios y ventajas de eGovFrame

La finalidad de este proyecto es ofrecer una serie de herramientas informáticas normalizadas, denominadas eGovFrame, destinadas al desarrollo y la ejecución de aplicaciones de cibergobierno, lo cual permite aumentar la eficacia de la inversión en TIC y la calidad de los servicios de cibergobierno. Su objetivo es optimizar la capacidad de reutilización y el interfuncionamiento de las aplicaciones de cibergobierno fijando un marco normativo para la elaboración de programas informáticos de cibergobierno, garantizando la independencia de las empresas informáticas con la adopción de herramientas informáticas abiertas y neutras y mejorando la competitividad de las PYMES informáticas al permitir que se compartan las herramientas de forma abierta a través de varias vías.

Figure 6: Vision and strategies of eGovframe

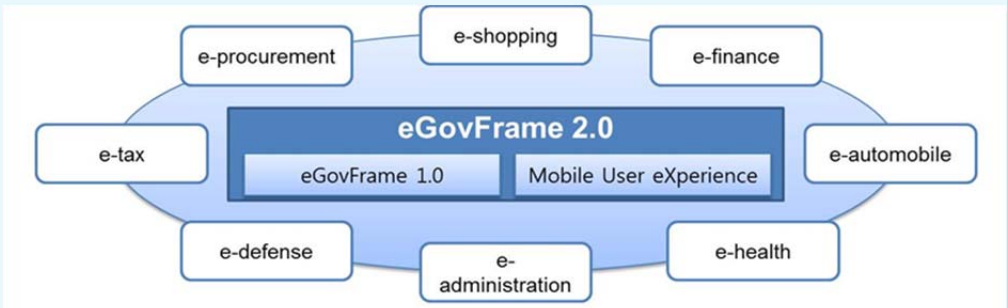


El marco eGovFrame está elaborado con software de fuente abierta fiable y bien conocido. Todos los códigos fuente están abiertos y al alcance de todos en el portal en línea. Está integrado por cuatro entornos de software: entorno de ejecución para aplicaciones, entorno de desarrollo para diseñadores de aplicaciones, entorno de gestión que reagrupa a los responsables del marco y entorno operacional para operadores de aplicaciones.

En la fase de desarrollo de aplicaciones, se puede ahorrar aproximadamente el 30 por ciento de los costos y esfuerzos de desarrollo aplicando eGovFrame, lo cual indica que eGovFrame funciona como tampón a la hora de adaptar diferentes aplicaciones a un tipo específico de infraestructura. Asimismo, sirve de base

para el desarrollo de funciones comunes. La última versión, eGovFrame 2.0, se presentó con el componente móvil Mobile User eXperience, como se observa en la Figura 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

4.3.5 Futura expansión de eGovFrame móvil

Dado el uso creciente de dispositivos móviles avanzados, como teléfonos inteligentes o tabletas, la demanda de servicios móviles va en aumento tanto en el sector público como en el privado. En respuesta a esta nueva demanda y con el fin de mejorar su calidad y eficacia, se lanzó a finales de 2011 eGovFrame 2.0, que incluye características de HTML 5 y una nueva interfaz de usuario. Además, es compatible por lo menos con tres navegadores móviles (Chrome, Safari y FireFox). Numerosos servicios móviles de cibergobierno de la República de Corea se han desarrollado a través de eGovFrame 2.0, como se indica en la Figura 7.

Con el fin de utilizar algunas características móviles, como las vibraciones, el control por cámara, la brújula, etc., eGovFrame 2.0 introducirá además componentes nuevos compatibles con la creación de aplicaciones móviles. Se prevé que esa nueva versión aliente a los diseñadores de software a crear diferentes servicios web móviles, así como aplicaciones móviles.

4.3.6 Oportunidades para otros países

Partiendo de su experiencia positiva, el gobierno de la República de Corea contribuye en gran medida a la labor de informatización internacional. El marco normalizado ha despertado sumo interés en países que desean resolver problemas relacionados con el monopolio de ciertas empresas o trabajar con programas informáticos de fuente abierta más seguros. El marco eGovFrame ya se ha aplicado en varios países, como se indica en el Cuadro 1.

Cuadro 1: Países que han adoptado eGovFrame

Países	Proyectos	Entidades encargadas	Duración del proyecto
Bulgaria	Sistema de administración de la Universidad de Sofía	Universidad de Sofía	11/2011~10/2012
Ecuador	Sistema de ventanilla única	Servicio de Aduanas de Ecuador	01/2011~03/2013
Viet Nam	Inversión en la modernización y expansión del proyecto del sistema de distribución del agua	Ministerio de Recursos Nacionales y Medioambiente	09/2010~12/2013
Mongolia	Sistema de registro estatal	Autoridad General del Registro Estatal	07/2011~06/2012
Túnez	Sistema electrónico de contratación pública	Observatorio Nacional de Contratación Pública	11/2011~11/2012

Otros países en desarrollo se han mostrado interesados en obtener más información sobre la experiencia de Corea en el ámbito del cibergobierno y, más concretamente, sobre eGovFrame. En respuesta a ello, el gobierno coreano contribuye de diversas formas a mejorar los servicios de cibergobierno de otros países, cooperando activamente con organizaciones internacionales. Con la intención de alentar a otros países a adoptar eGovFrame, el código fuente puede descargarse desde la versión inglesa del portal (http://eng.egovframe.go.kr). El gobierno ofrece también asistencia técnica en línea. Además se ofrecen cursos de formación sobre eGovFrame, por ejemplo a través del programa Korea IT Learning (KoIL) o del Centro de Cooperación de Tecnologías de la Información (ITCC), encargado de promover la cooperación en materia informática entre la República de Corea y otros países interesados.

5 Ámbitos de aplicación en beneficio de países en desarrollo

5.1 Directrices relativas a la identificación de ámbitos de aplicación

En el mundo hipertecnológico actual, las TIC se están convirtiendo rápidamente en el eje central de los programas de modernización estatales, y no sólo en los países desarrollados. Los países en desarrollo han tomado conciencia de que las posibilidades de las nuevas tecnologías transforman el modo de funcionamiento de la administración pública. Aunque se conoce muy bien la utilización que éstas hacen de las TIC (el "cibergobierno"), que forman parte de la actividad del Estado, se deben elaborar directrices relativas a la identificación de ámbitos de aplicación y el establecimiento de prioridades en beneficio de los países en desarrollo. Esas directrices deberían tratar los siguientes puntos:

1) Características singulares de cada país en desarrollo (condiciones económicas y sociales).

2) Necesidades y capacidades actuales de cada país.

3) Prioridad para las aplicaciones que presentan gran interés para los países en desarrollo.

4) Examen de la utilización de plataformas móviles e inalámbricas para la interacción entre autoridades gubernamentales y ciudadanos (pedidos de información y prestación de servicios públicos).

Los ámbitos de aplicación para países que recién comienzan a poner en marcha servicios de cibergobierno pueden seleccionarse teniendo en cuenta los siguientes principios:

- Programas estrechamente vinculados a la vida cotidiana de los ciudadanos, de tal forma que puedan beneficiarse al máximo de los nuevos servicios electrónicos.
- Programas que contemplan principalmente procesos comerciales de una organización a la otra.

- Optimización de los intercambios de información entre organismos públicos para eliminar la duplicación en la recopilación y gestión de los datos.
- Promoción de la utilización de las TIC para racionalizar los procedimientos administrativos mediante el método de reestructuración administrativa (BPR, business process reengineering).

Además de estos principios, se deben tener en cuenta, por una parte, la falta de recursos nacionales atribuidos al cibergobierno, especialmente en los países en desarrollo, y, por la otra, la necesidad urgente de aplicar los principios de cibergobierno para lograr el avance del país. La solución se apoya en tres elementos esenciales: estrategia, selección y concentración. Un pequeño número de proyectos de cibergobierno son seleccionados sobre la base de los principios enunciados y los recursos limitados se concentran en dichos proyectos.

5.2 Infrastructuras

- Modernización del sistema jurídico para el cibergobierno y la seguridad.
- Formación de personal y reestructuración de la gobernanza en la esfera de las TIC.
- Sistema de autenticación electrónica.

5.3 Servicios G2G

- Sistema electrónico de documentos conectado a sistemas públicos como, por ejemplo, sistema de compras públicas, sistema de administración local, sistema fiscal, etc.
- Sistema de administración local.
- Sistema de gestión de finanzas públicas (a escala nacional y local).
- Sistema de intercambio de información.

5.4 Servicios G2C y G2B

Experiencias y lecciones relativas a la puesta en marcha de servicios de fácil utilización, la integración y personalización de los servicios públicos, la utilización de numerosos canales, la mejora de la calidad de los servicios en función de las necesidades de los usuarios y la comercialización de servicios de cibergobierno.

- Sistema de portal para la prestación de servicios públicos a los ciudadanos
- Sistema tributario por Internet
- Sistema de compras públicas en línea.

6 Factores que garantizan el éxito de las actividades de cibergobierno

6.1 Liderazgo presidencial (Apoyo político)

- En los proyectos nacionales relativos a las tecnologías de la información, en particular los proyectos de cibergobierno, suelen intervenir numerosos organismos, de ahí el riesgo de desacuerdos. La adopción de decisiones se interrumpe con frecuencia debido a rivalidades burocráticas entre los ministerios participantes interesados en un asunto determinado.
- El logro de coordinación entre las organizaciones que intervienen en la implantación de las redes y la puesta en práctica de sistemas de aplicación es tal vez la mayor dificultad que deben afrontar las iniciativas de cibergobierno. Cada organización debe tener en cuenta su nivel de riesgo, la naturaleza de esos riesgos y los incentivos. Es probable que no haya ningún sistema que se adapte a las necesidades de todas las organizaciones. Para solucionar ese problema, se ha creado una

comisión de alto nivel a escala interministerial encargada de resolver las controversias entre los organismos públicos. La eficacia de las actividades de esa comisión depende del apoyo recibido a nivel presidencial, fuente de poder para obtener la coordinación deseada.

- Los proyectos relativos a las tecnologías de la información requieren importantes inversiones que no obtienen una rentabilidad inmediata. Además, esos proyectos no son visibles y no es fácil presentar los resultados a quienes se encargan de asignar recursos nacionales a los proyectos públicos.
- Aunque muchas personas comprenden las posibilidades que ofrece la utilización de esas tecnologías y su repercusión en la eficacia y la competitividad, los encargados de asignar presupuestos públicos no han podido encontrar pruebas tangibles que logren convencerlos de las ventajas de esas tecnologías. Para resolver el problema, es fundamental que el Presidente reconozca las posibilidades que aportan las tecnologías de la información. Así pues, en 1987 el Presidente de Corea decidió atribuir partidas extrapresupuestarias para la utilización exclusiva de proyectos a tal efecto. Esa decisión representa la firme voluntad política puesta de manifiesto en Corea desde el inicio de las iniciativas en la materia.

6.2 Equilibrio entre la oferta y la demanda de servicios de cibergobierno

- Un plan rector nacional centrado principalmente en la oferta ha sido, por lo general, considerado prioritario en el país. El gobierno estima primordial el desarrollo de servicios de aplicación que se ofrecen en primer lugar a los ciudadanos para crear una demanda. Sin embargo, hay que preguntarse qué tipos de servicios justifican las importantes inversiones efectuadas en los proyectos de cibergobierno, dado que se corre el riesgo de crear una solución costosa para un problema que en realidad no existe.
- Privilegiar la oferta no impide tener en cuenta la importancia que adquiere la posible demanda de un determinado servicio de cibergobierno. El problema es que los proyectos relativos a las tecnologías de la información han creado al parecer una demanda cuyo alcance es prácticamente imposible prever hasta que no haya una oferta. Resulta importante que la estrategia adoptada esté a la par de la creación de la demanda, tras la implantación de sistemas TIC, por ejemplo gracias a la capacitación de los posibles usuarios del sistema, lo que les permitirá beneficiarse plenamente de las ventajas de esas tecnologías.
- Con miras a equilibrar la oferta y la demanda de servicios de cibergobierno, hay que tener en cuenta todos los aspectos del servicio previsto. Por ejemplo, el examen de las transacciones fuera de línea entre las autoridades públicas y los ciudadanos es una forma de tener en cuenta la demanda en el momento de decidir qué servicios contemplarán las iniciativas de cibergobierno. Esto podría compensar la imposibilidad de prever la demanda, ya que se puede esperar que cuanto mayor sea el número de transacciones fuera de línea, mayor será la demanda de servicios en línea.

6.3 Comprensión clara del concepto de cibergobierno

- En “cibergobierno” se debe poner más el acento en "gobierno" que en "ciber". Este concepto apunta esencialmente a transformar la administración pública para que modernice sus relaciones internas y externas con la ayuda de las TIC. Los asuntos en materia de cibergobierno deben situarse en el contexto de las iniciativas relativas a la reforma de la administración pública y a la buena gobernanza. El problema de la modernización de la administración pública existe desde que comenzaron a utilizarse aplicaciones informáticas, pero su incidencia real y concreta en los métodos de trabajo ha aparecido muy lentamente.
- En lugar de contentarse con adoptar las tecnologías de la información, las autoridades públicas deben decidir, orientar y supervisar la transformación de los procedimientos administrativos de tal manera que esas tecnologías estén al servicio de la reestructuración de esos procesos.

- Se espera del cibergobierno que lleve a cabo cambios profundos y radicales en las actividades internas del Estado y en los servicios propuestos a los ciudadanos. Esos cambios estarán en función de la tecnología aplicada, en particular de Internet, lo que permite al sector público realizar su labor de manera integrada. Alentada por el intercambio de información, la integración se produce generalmente en grupos de organismos públicos que tienen ciertas funciones en común o que proponen los mismos servicios. La mayoría de los proyectos de cibergobierno pasan por una etapa de reestructuración administrativa (BPR) antes de que se inicie su implantación. Por lo general, esa reestructuración se realiza en varias etapas: análisis de los procesos correspondientes a los objetivos de las organizaciones, eliminación de la duplicación de procesos, racionalización de los métodos de trabajo y simplificación de procesos complejos.
- La eliminación de la duplicación de procesos o la racionalización de los procesos supone reducir el número de puestos de trabajo, a lo cual pueden oponerse las partes interesadas. Quienes se han habituado a métodos de trabajo tradicionales están poco inclinados a aceptar esos cambios. Hay que crear pues incentivos para los funcionarios públicos, y estructuras que garanticen la coordinación entre los organismos públicos en juego. Esos incentivos pueden ser el reciclaje o la redistribución de los trabajadores, según sus deseos. Para reforzar la eficacia y agilidad del sector público, habrá que suprimir procesos innecesarios, simplificar procesos complejos y unificar procesos diferentes.

6.4 Aliento al compromiso y la participación de los ciudadanos

- Debido a las mayores posibilidades de interacción entre las autoridades públicas y los ciudadanos, éstos expresan cada vez su voluntad de participar en la adopción de decisiones. A ello ha contribuido en parte la democratización de la vida pública y la generalización de Internet, que facilita el acceso a diversos organismos públicos. Hay que pensar detenidamente de qué manera la tecnología permite a una persona hacer oír su voz sin perderse en la masa de participantes en el debate público. Por ejemplo, las autoridades públicas tendrían que estar en condiciones de responder a las opiniones expresadas individualmente.
- Para una adecuada participación en línea, los ciudadanos deben estar suficientemente informados de los asuntos de interés público, y los funcionarios públicos tienen que conocer debidamente las posibilidades que ofrece Internet y los límites que impone con respecto a la participación de los ciudadanos en la adopción de decisiones.

6.5 Innovación en la gestión de recursos de información

Dado que en los proyectos de cibergobierno se observa una acumulación de recursos TIC en diversos sectores estatales, es imprescindible encontrar la forma de gestionar esos proyectos para evitar el despilfarro de dichos recursos. Con ese tipo de gestión, los organismos públicos colaboran entre sí con miras a intercambiar e integrar al máximo sus recursos de información.

Una metodología de gestión como la arquitectura de empresa tiene en cuenta las relaciones existentes o previstas entre los procesos de empresa y los recursos de información con objeto de asegurar el intercambio de información y la integración de procesos en las organizaciones y entre ellas. Evita además a los organismos públicos adquirir recursos informáticos por duplicado, para mejorar la eficacia de sus inversiones.

Las actividades relativas a esa metodología dan prioridad al intercambio de información y a la mejora de las inversiones en tecnología proporcionando directrices y modelos de referencia para cada componente. Los modelos de referencia tienen por objeto promover la identificación y utilización comunes, y el intercambio adecuado de datos, procesos de empresa, aplicaciones informáticas y equipos informáticos. Las directrices se establecen para una gestión eficaz de los recursos de información, sobre la base de los elementos menos propensos a los cambios en el contexto de la evolución de las prioridades de la empresa y de los equipos tecnológicos.

6.6 Protección de la vida privada y seguridad de los sistemas

- Dado que la información mantenida por un organismo cada vez más es compartida por otras partes en el marco de las iniciativas de cibergobierno, los posibles usuarios de esos servicios temen que los datos personales sean utilizados indebidamente o en forma abusiva. Hay que lograr un compromiso entre la protección de los datos personales y el intercambio de información con objeto de acelerar el desarrollo de aplicaciones electrónicas relativas a las actividades públicas. Es sumamente importante conciliar el intercambio de información entre los organismos y la elaboración de medidas encaminadas a la protección de la privacidad.
- Puesto que los inconvenientes de las aplicaciones informáticas se pondrán de manifiesto a medida que evolucionen los servicios de cibergobierno, habrá que reforzar las medidas de protección de la vida privada para conciliar ambos extremos. Los sistemas de cibergobierno están siempre expuestos a los ataques del exterior, e incluso del interior. Por ese motivo, hay que prever medidas técnicas, jurídicas e institucionales para luchar contra la piratería, la falsificación y el fraude.

6.7 Estrategias para la adopción de servicios electrónicos

- Aun cuando los servicios electrónicos están disponibles, su adopción por los ciudadanos y las empresas no es automática. Los ciudadanos sólo están dispuestos a aceptarlos si estiman que les aportará un beneficio real. Es bastante habitual que, al comienzo de la implantación de los sistemas de cibergobierno, los servicios electrónicos se facturen por debajo de su precio real, impidiendo llevar a cabo todas sus pobilidades. Se plantea de esta forma el problema de la conveniencia de proseguir con esas iniciativas.
- Convendría analizar detenidamente las aplicaciones Internet utilizadas en las actividades del sector público con objeto de determinar cómo modernizarlas para que los usuarios aprovechen sus ventajas. Los canales de acceso deben ser suficientemente amplios para facilitar el acceso y el número de hiperenlaces, suficientemente bajo para que el ciudadano de a pie pueda encontrar el sitio que le dará la información y los servicios deseados.
- En lugar de ocuparse de todas las aplicaciones, hay que concentrarse en las más importantes, las que facilitan la interacción en línea entre las autoridades públicas y los ciudadanos. Cuando se decide modernizar las aplicaciones de cibergobierno, hay que privilegiar los servicios más solicitados por los ciudadanos para que el mayor número posible de personas pueda valorar sus ventajas.

7 Directrices relativas a la promoción de las actividades de cibergobierno y a la identificación de los ámbitos de aplicación del cibergobierno en los países en desarrollo

7.1 Esfera de acción

Estas Directrices abarcan cuestiones vinculadas a la promoción de las actividades de cibergobierno y a la identificación de los ámbitos de aplicación del cibergobierno en los países en desarrollo.

7.2 Objetivo de las Directrices

Estas Directrices están concebidas para orientar a los países en desarrollo y ayudarlos a determinar los factores de éxito de las actividades de cibergobierno y los ámbitos en los cuales sus aplicaciones pueden revestir mayor utilidad.

Estas Directrices presentan:

a) orientaciones sobre la manera de identificar los ámbitos de aplicación del cibergobierno en beneficio de los países en desarrollo, sin olvidar que cada uno de ellos tiene características peculiares;

b) factores a tener en cuenta para garantizar los buenos resultados de las iniciativas de cibergobierno en los países en desarrollo.

7.3 Directrices para la identificación de los ámbitos de aplicación en beneficio de los países en desarrollo

Hay numerosos ámbitos de aplicación del cibergobierno debido a que prácticamente todas las actividades públicas pueden ser transformadas utilizando las tecnologías de la información y la comunicación.

En la identificación de esos ámbitos en los países en desarrollo, se deben tener en cuenta los siguientes factores:

c) características singulares de cada país en desarrollo (condiciones económicas y sociales)

d) necesidades y capacidades actuales de cada país

e) prioridad para aplicaciones que presentan gran interés para los países en desarrollo

f) examen de la utilización de plataformas móviles e inalámbricas para la interacción entre autoridades gubernamentales y ciudadanos (pedidos de información y prestación de servicios públicos);

g) estrategias y mecanismos nacionales para lograr una simplificación de la organización y de la labor administrativa, y la colaboración entre las autoridades públicas (servicios G2G, según la terminología propia del sistema de cibergobierno);

h) experiencias y lecciones relativas a la puesta en marcha de servicios de fácil utilización, la integración y personalización de los servicios públicos, la utilización de numerosos canales, la mejora de la calidad de los servicios en función de las necesidades de los usuarios, la comercialización de servicios de cibergobierno, la protección de datos personales y la seguridad de las transacciones vinculadas al cibergobierno (servicios G2C y G2B).

7.4 Directrices para asegurar el buen avance de las actividades de cibergobierno

Para asegurar el buen avance de las actividades de cibergobierno, los países en desarrollo deben crear las condiciones propicias para la implantación eficaz de esas iniciativas.

Se han identificado varios factores de éxito fundados en la experiencia de países que han puesto en marcha sistemas avanzados de cibergobierno. Habrá que tener en cuenta esos factores en el proceso de implantación de dichos sistemas:

i) coordinación efectiva y sólida voluntad política. El logro de coordinación entre las diferentes organizaciones interesadas en la implantación de la red y la puesta en práctica de sistemas de aplicación es tal vez el principal obstáculo que deben afrontar las iniciativas de cibergobierno;

j) equilibrio entre la oferta y la demanda de servicios de cibergobierno. Un plan rector nacional centrado principalmente en la oferta ha sido, por lo general, considerado prioritario en el país. El gobierno estima primordial el desarrollo de servicios de aplicación que se ofrecen en primer lugar a los ciudadanos para crear una demanda. Sin embargo, hay que preguntarse qué tipos de servicios justifican las importantes inversiones efectuadas en los proyectos de cibergobierno, dado que se corre el riesgo de crear una solución costosa para un problema que en realidad no existe;

k) comprensión clara del concepto de cibergobierno. En “cibergobierno” se debe poner el acento más en “gobierno” que en "ciber". Esencialmente, este concepto apunta a transformar la administración pública para que modernice sus relaciones internas y externas con la ayuda de las TIC. Los asuntos en materia de cibergobierno deben situarse en el contexto de las iniciativas relativas a la reforma de la administración pública y a la buena gobernanza;

l) aliento al compromiso y la participación de los ciudadanos. Debido a las mayores posibilidades de interacción entre las autoridades públicas y los ciudadanos, éstos expresan cada vez su voluntad de participar en la adopción de decisiones. A ello ha contribuido en parte la democratización de la vida pública y la generalización de Internet, que facilita el acceso a diversos organismos públicos. Hay que pensar detenidamente de qué manera la tecnología permite a una persona hacer oír su voz sin perderse en la masa de participantes en el debate público;

m) seguimiento y evaluación eficaces con un sistema de retroalimentación adaptado. El éxito de un proyecto de cibergobierno no se mide por su buen comienzo. Lo que verdaderamente importa es la realización del proyecto y los resultados obtenidos. Al mismo tiempo que los esfuerzos desplegados para evaluar las ventajas de la inversión en el sector de las TIC, conviene no olvidar el seguimiento y la evaluación de los proyectos de cibergobierno para comprender mejor las necesidades de los usuarios y sus actitudes frente a los servicios electrónicos. Los resultados de esa evaluación deberían integrarse en el mecanismo de retroalimentación;

n) innovación en la gestión de recursos de información. Dado que en los proyectos de cibergobierno se observa una acumulación de recursos TIC en diversos sectores estatales, es imprescindible encontrar la forma de gestionar esos proyectos para evitar el despilfarro de dichos recursos. Con ese tipo de gestión, los organismos públicos colaboran entre sí con miras a intercambiar e integrar al máximo sus recursos de información;

o) protección de la información privada. Dado que la información mantenida por un organismo cada vez más es compartida por otras partes en el marco de las iniciativas de cibergobierno, los posibles usuarios de esos servicios temen que los datos personales sean utilizados indebidamente o en forma abusiva. Hay que lograr un compromiso entre la protección de los datos personales y el intercambio de información con objeto de acelerar el desarrollo de aplicaciones electrónicas relativas a las actividades públicas. Es sumamente importante conciliar el intercambio de información entre los organismos y la elaboración de medidas encaminadas a la protección de la privacidad;

p) estrategias para la adopción de servicios electrónicos. Aun cuando los servicios electrónicos están disponibles, su adopción por los ciudadanos y las empresas no es automática. Los ciudadanos sólo están dispuestos a aceptarlos si estiman que les aportará un beneficio real. Es bastante habitual que, al comienzo de la implantación de los sistemas de cibergobierno, los servicios electrónicos se facturen por debajo de su precio real, impidiendo llevar a cabo todas sus pobilidades. Se plantea de esta forma el problema de la conveniencia de proseguir con esas iniciativas.

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)

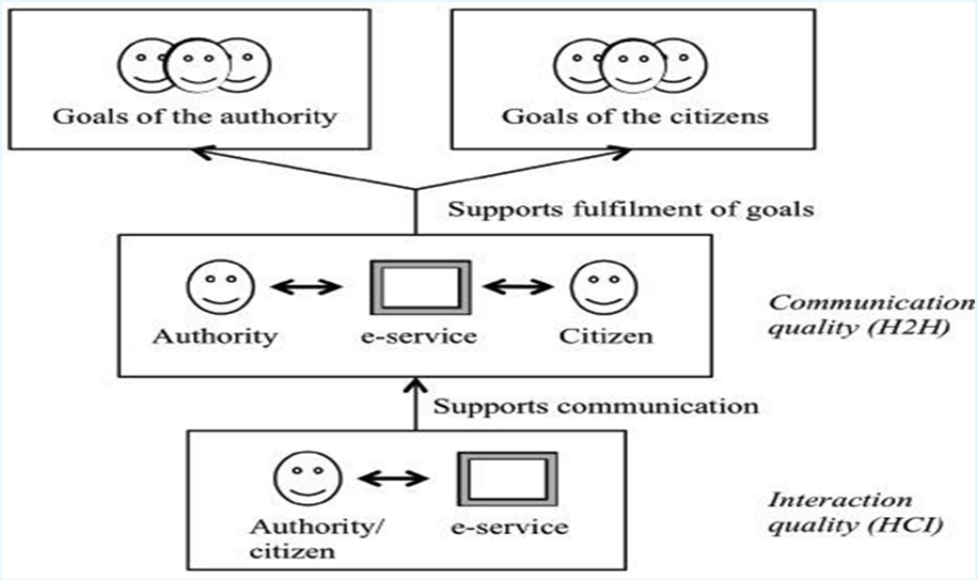
BTCL	**977,000**
Telebarta Ltd.	**56,424**
Jalalabad Telecom Ltd.	**10,900**
Onetel Communication Ltd.	**39,576**
Westec Ltd.	**17,000**
Sheba Phone Ltd. (ISL)	**1,081**
Banglaphone	**5,450**
SA Telecom	**18,033**
RANKS TELECOM LTD	**16,139**
Total	**1,141,603**

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
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

Table 6: Global recognition for KONEPS

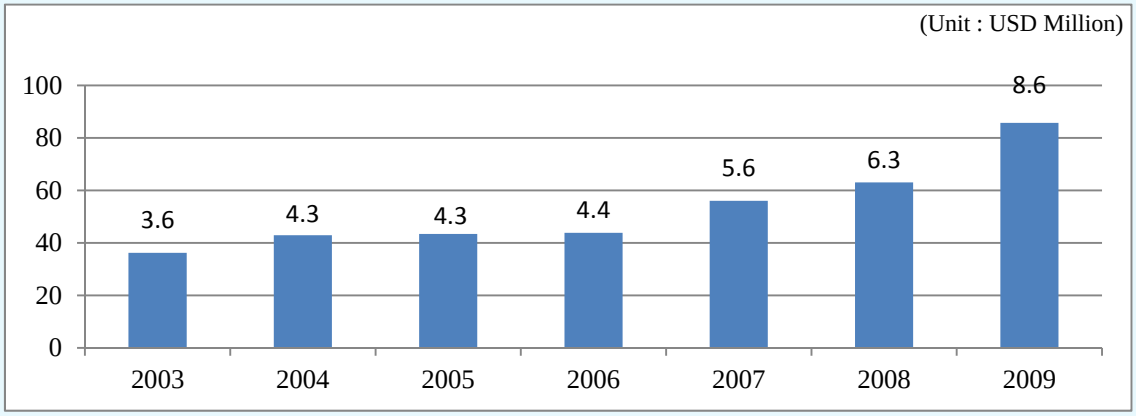
Awarding Organization	Award	Date
WITSA	Global IT Excellence Award PPS was named as the public institution of best service innovation using information technology at WCIT	May 2006
AFACT	2007 eAsia Award KONEPS was named as a best practice model of e-Transaction in the public sector	August 2007

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.

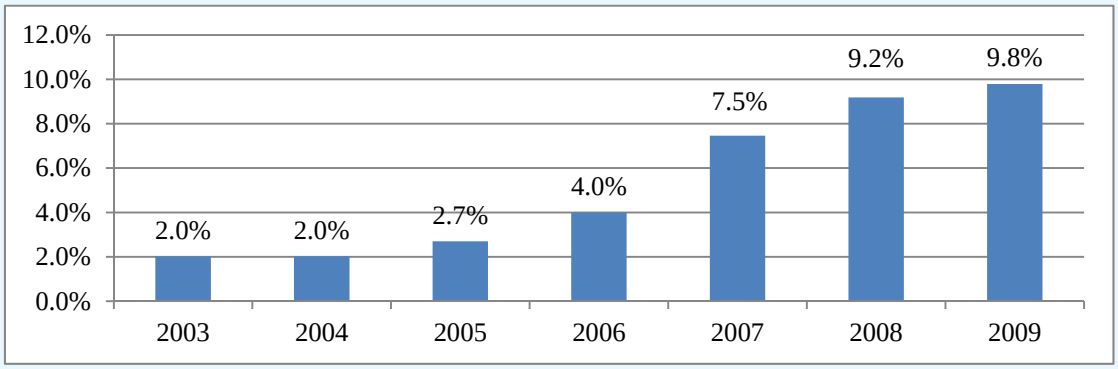
Figure 1: Transactions via KONEPS



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.

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

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.
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

Country overview

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

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

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**	**95**
1.	**1. E-Government Delivery Models – Use of Mobile Terminals**	**95**
2.	**G2C Activities**	**96**
3.	**General Principles for Secure Mobile Services**	**97**
4.	**Mobile Payment System (MPS)**	**102**
5.	**Security**	**108**
6.	**Mobile Technology**	**115**
7.	**M-Government in the European Union**	**116**
8.	**Case Study in Japan**	**122**
9.	**United States of America National Strategy for Trusted Identities in Cyberspace (NSTIC)**	**125**
10.	**Case study mobile payment in Poland**	**126**
11.	**Case study in the Russian Federation**	**128**
12.	**Findings**	**130**
13.	**Recommendations**	**131**
14.	**Terms and abbreviations**	**133**
15.	**List of References**	**135**

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.

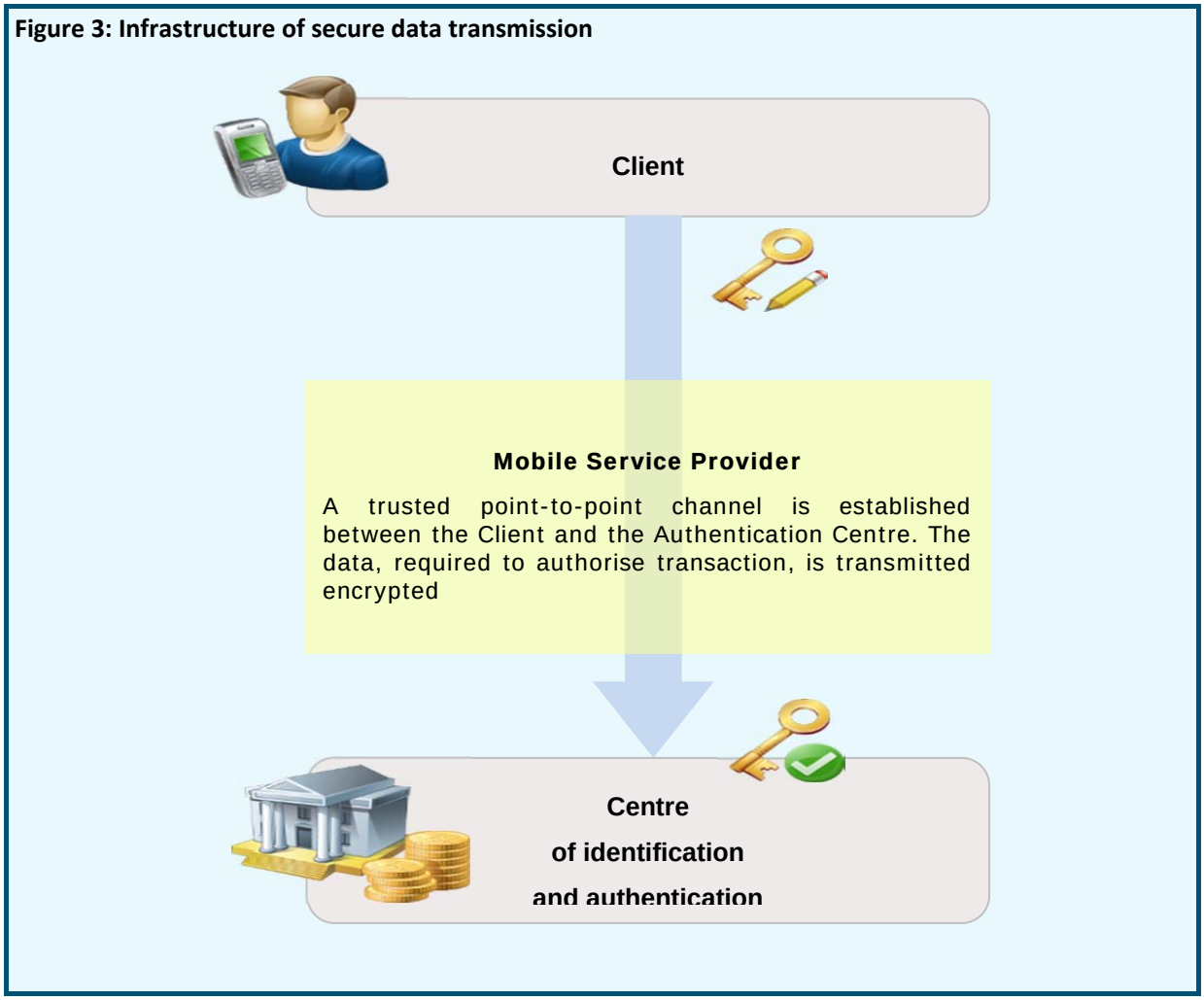
3 General Principles for Secure Mobile Services

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



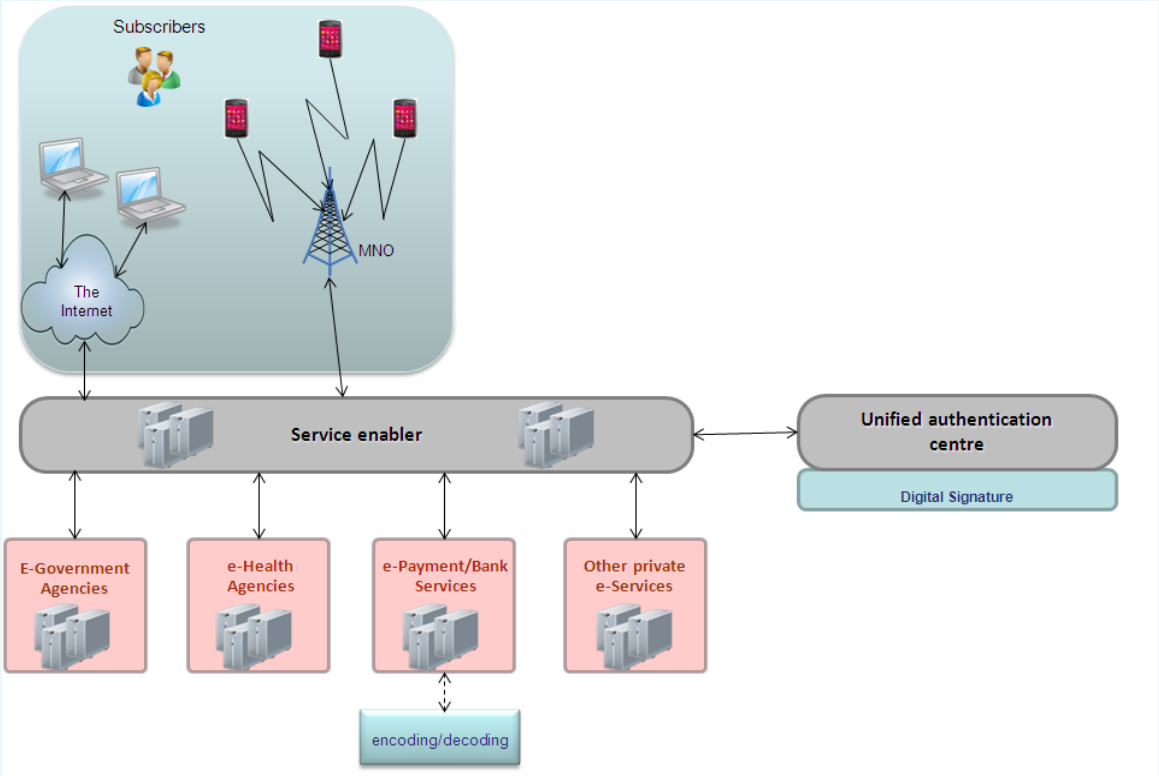
Existing mobile payment systems have already implemented their own security procedures, where security requirements are determined by agreements between service providers and their customers. Obviously, e-government requires a security system, controlled by the State and compliant with national law regulations 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).

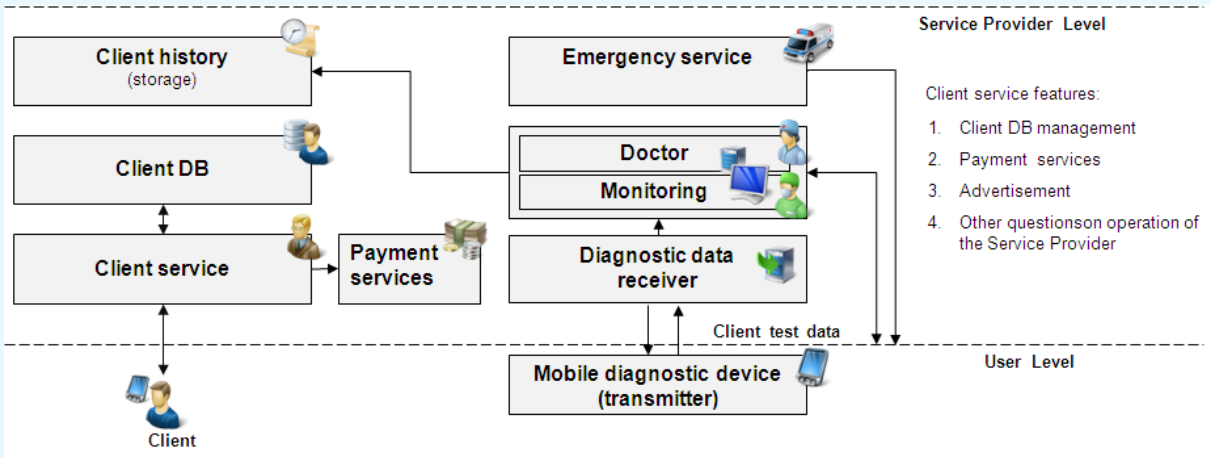
All identification and authentication centres must comply with the same allocation rules and regulations for global identifiers of mobile clients (mID), registered in a central System Directory to ensure message delivery to customers.

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:

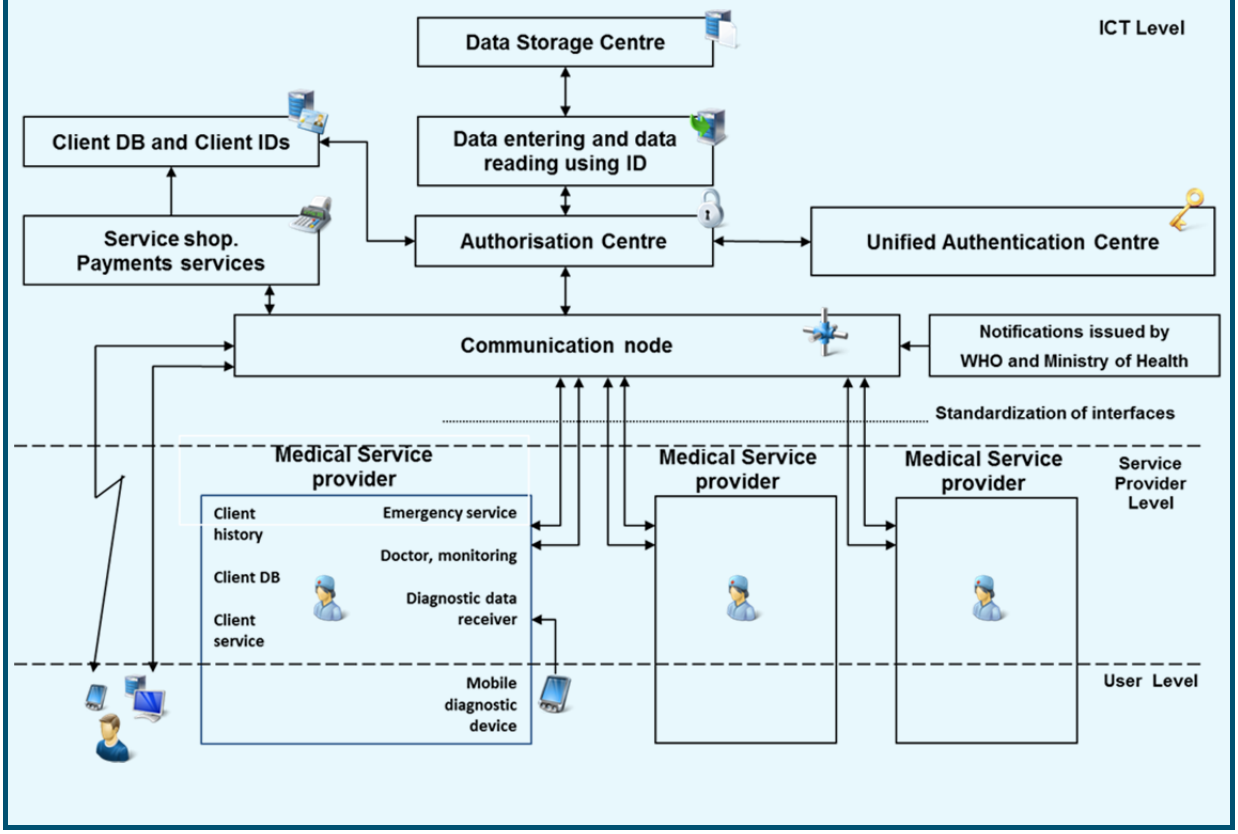
1) Difficulty to present services to the Client (Advertising problem)
2) Difficulty for one service provider to use results obtained by another provider
3) If the client stops to pay, who will store his history?
4) Insufficiency of authentication and protection of personal data
5)In case the Service 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:

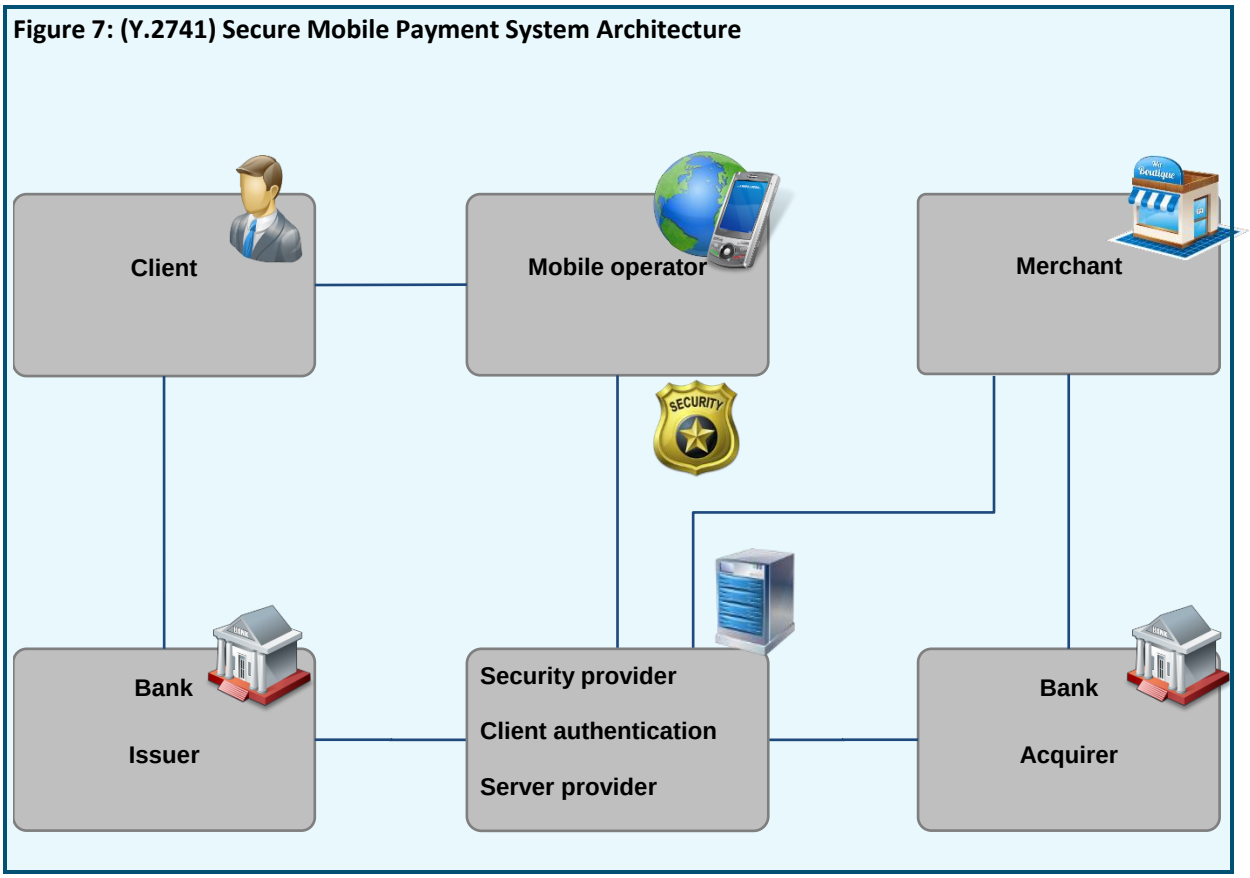
– MPS Operator
– Mobile Operator
– Banks (for typical MPS)
  • Clients' Bank (bank issuer)
  • Acquiring bank, accepting payments and providing access to Clients' banks for merchants or service providers
  • Settlement Bank (interbank settlements)
– Clients (mobile Operator subscribers, using Mobile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

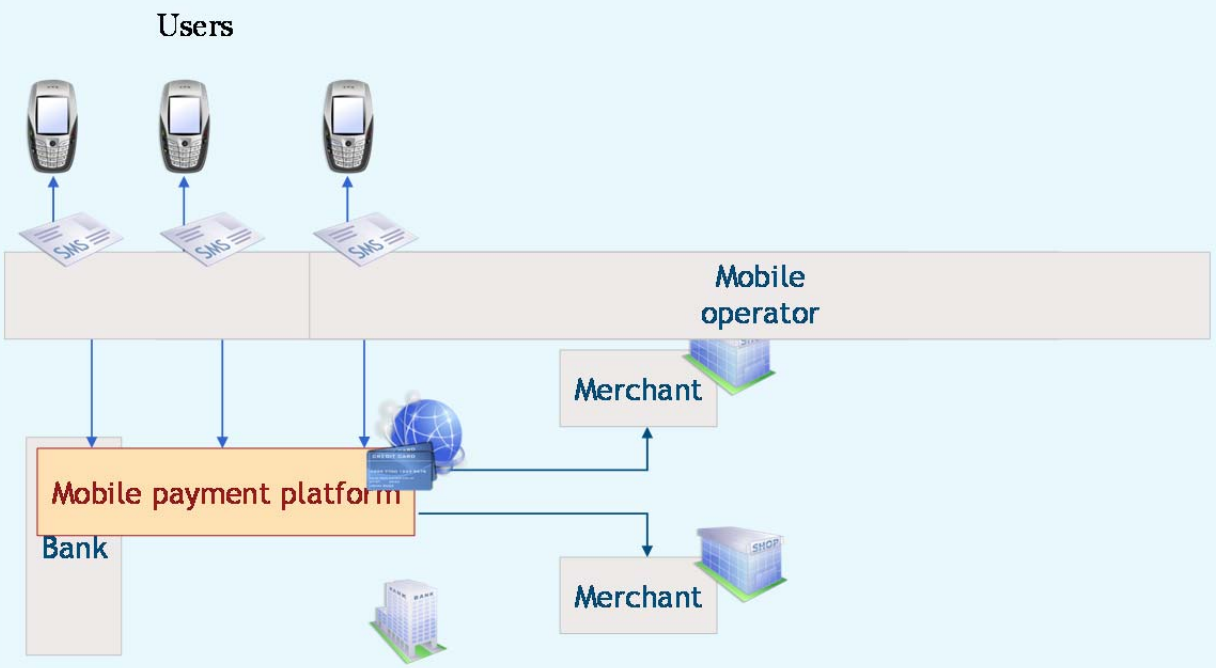


4.3 MPS Models

Different MPS models exist:

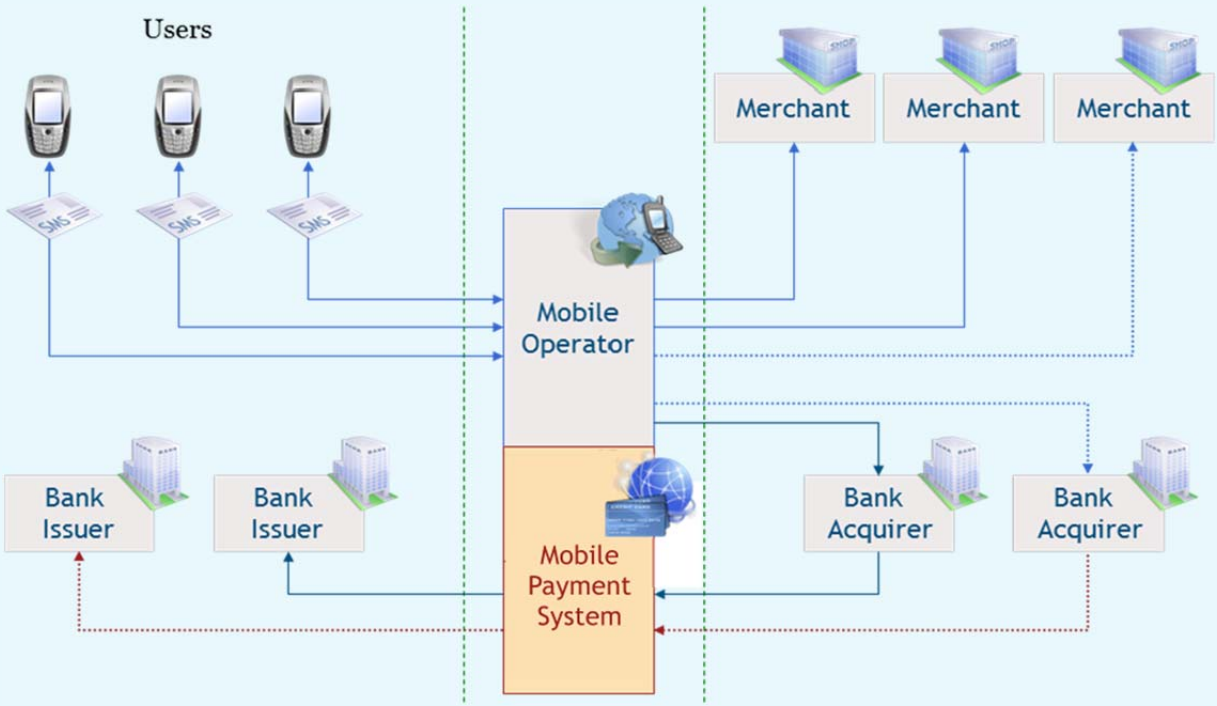
– Bank-oriented model (Figure 8), where bank offers mobile payment services with many mobile operators.

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.

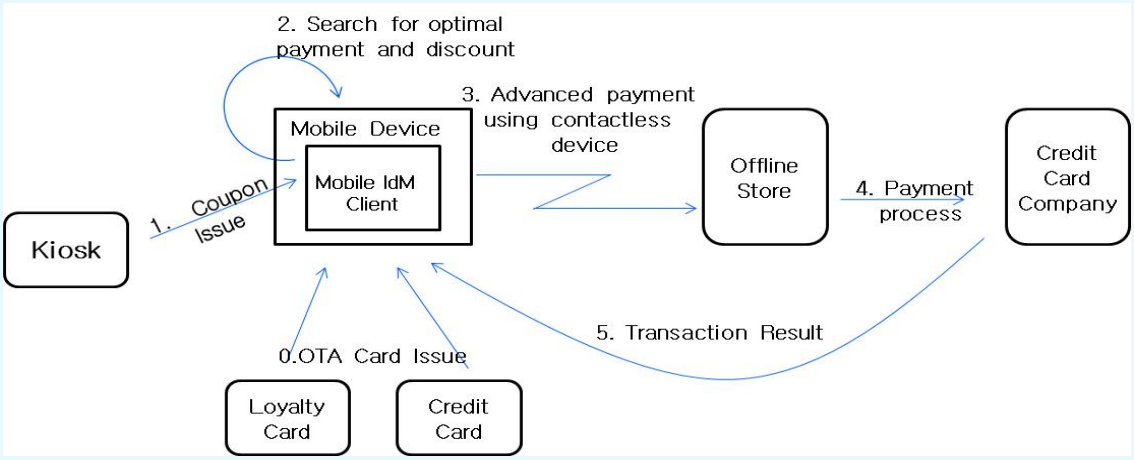
Mobile NFC business models are being developed to be integrated in any mobile security framework for financial transactions. Typically, mobile NFC system involves the following elements:

– 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.

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).

---

[3] ITU-T Recommendation X.800 "Security architecture for Open Systems Interconnection for CCITT applications (page 12).

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:

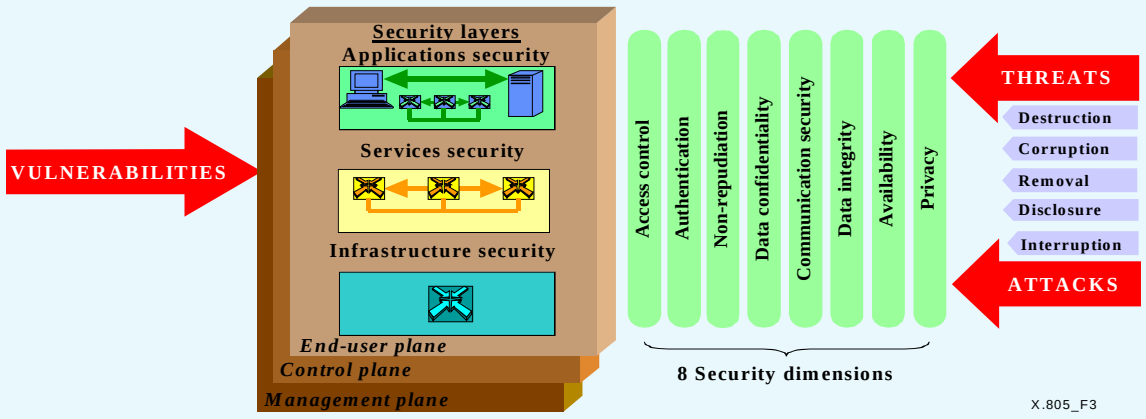
– Infrastructure security Layer, consisting of network communication means and individual network elements (routers, switches, servers, communication lines);
– Services security Layer to protect service providers and their clients (both basic services – connection to resources, DNS, and additional services – 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?

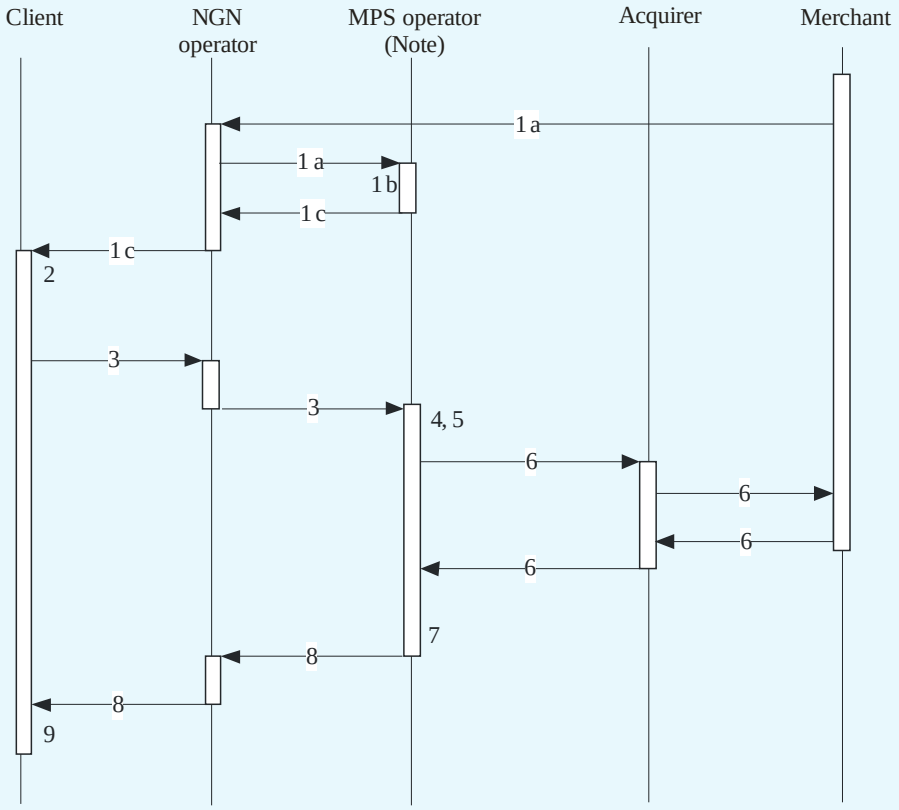
These questions are addressed by three architectural components: security dimensions, security layers and security planes.

– 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



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>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 or members of shared groups with equal authority to access a resource or service. Also one person may

[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).

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.

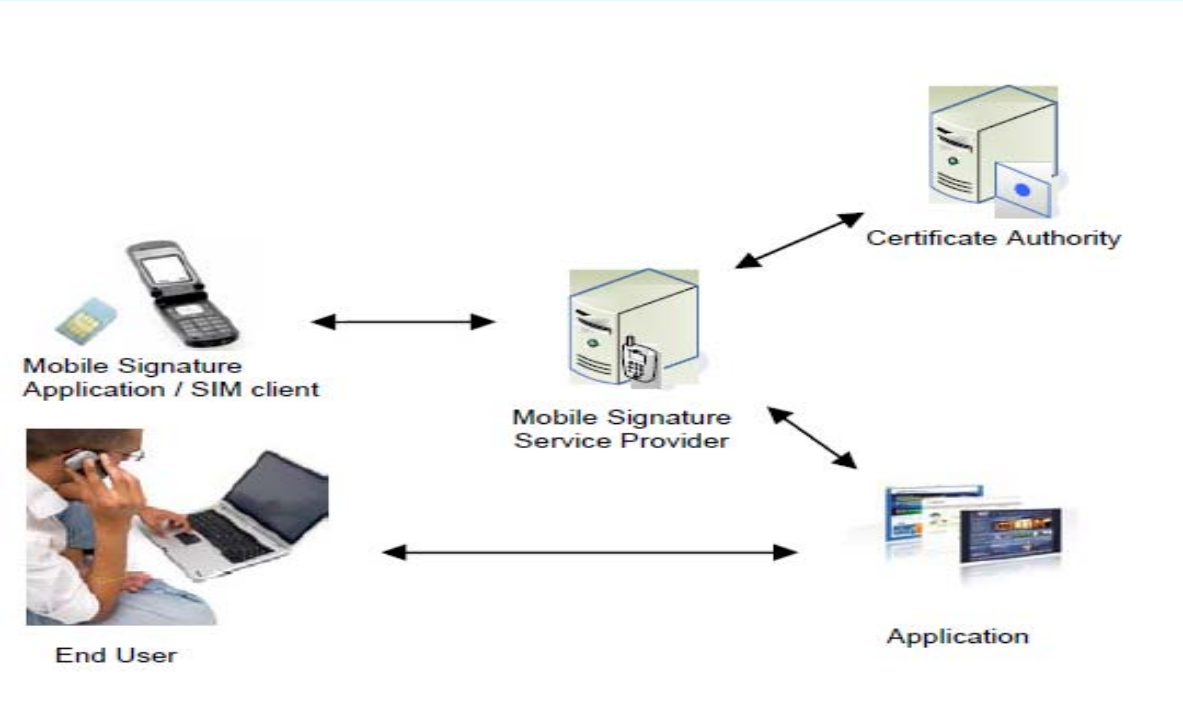
Mobile signature creation is achieved using a crypto-processor on a smartcard, such as Subscriber identity module (i.e. SIM card) found inside GSM mobile handsets or the Universal Integrated Circuit Card (UICC) that has been adopted for 3rd Generation mobile devices (Figure 12). The use of SIM or UICC 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.

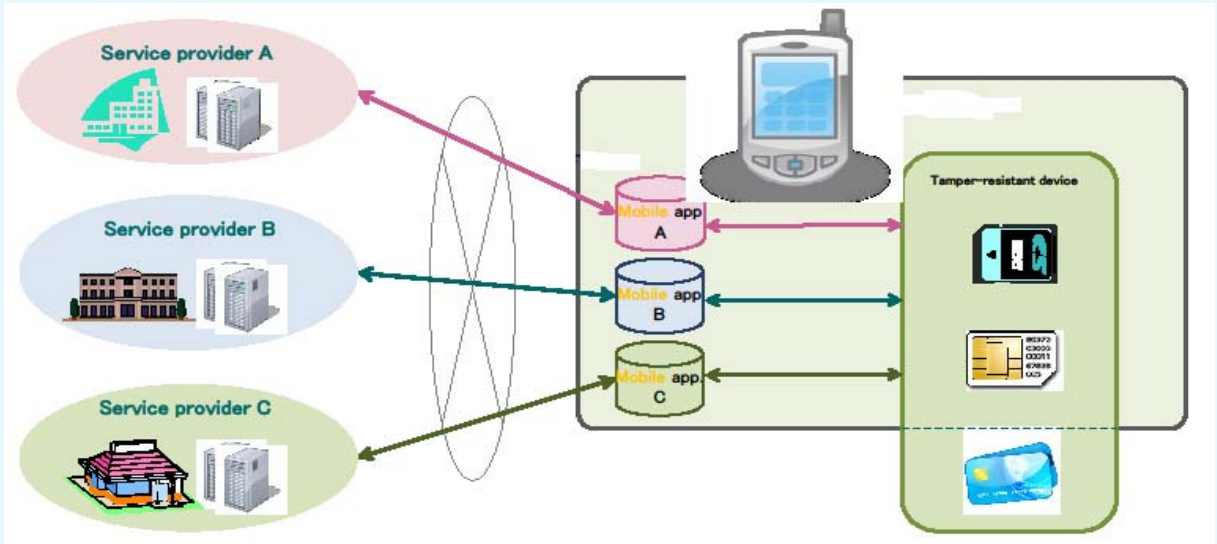
In addition, spread of smartphones has been progressing rapidly. Smartphone shipments in Japan in FY 2011 amounted to 23.4 million units (2.7 times increase year-on-year), accounting for 55.8 % of total shipments of mobile phone terminals[16]. Furthermore, since FY 2012, mobile phone terminals with NFC (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

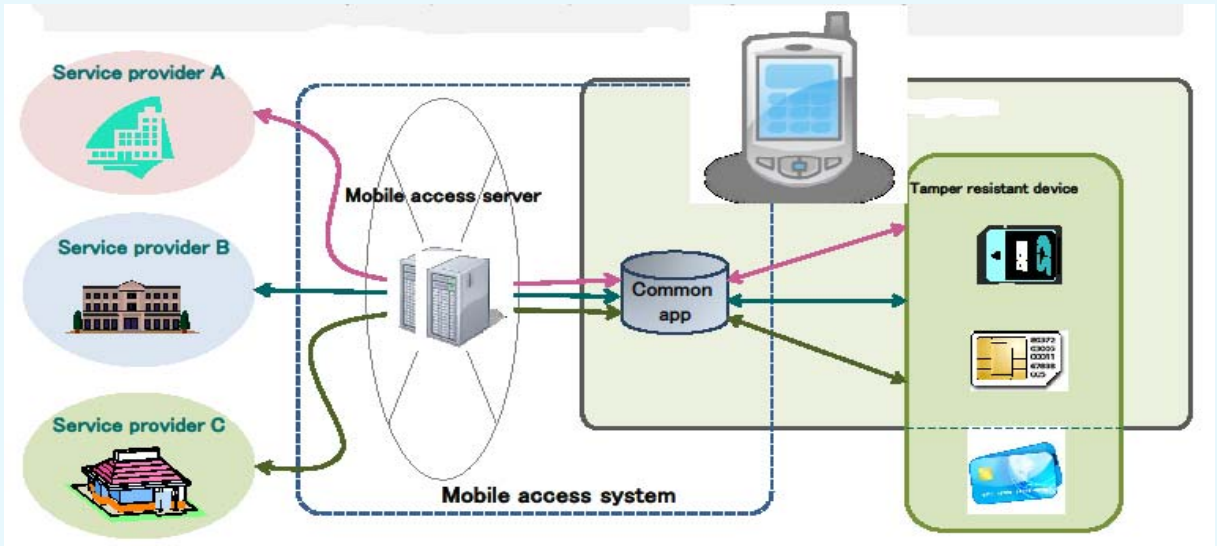
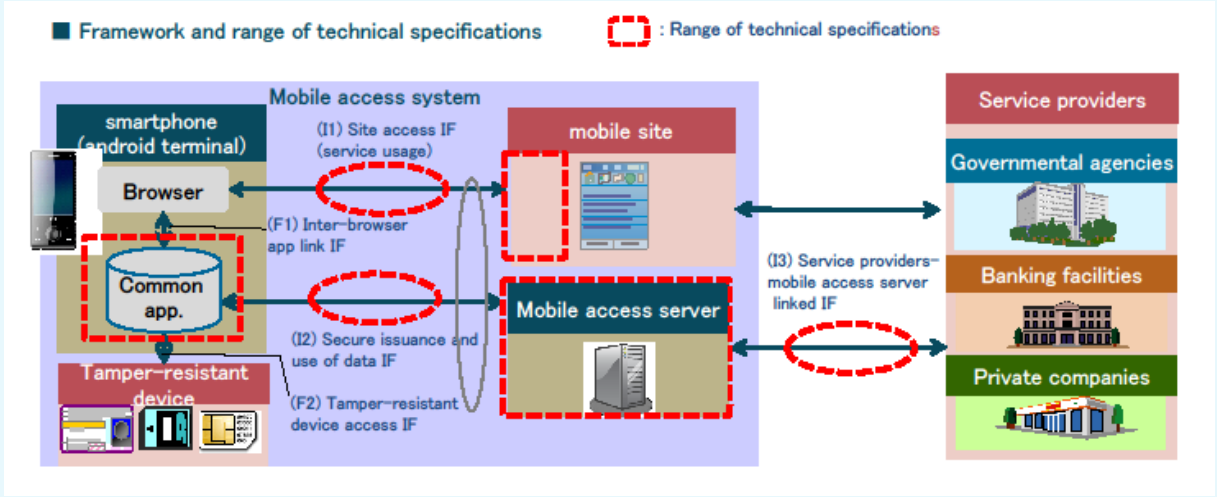


Figure 17: Common application and unified mobile access server for all service providers. Further, verification by experimentation with technical specifications etc. was studied. In other words, **A:** Examination of technical specifications for a mobile access system realising online storage and use 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

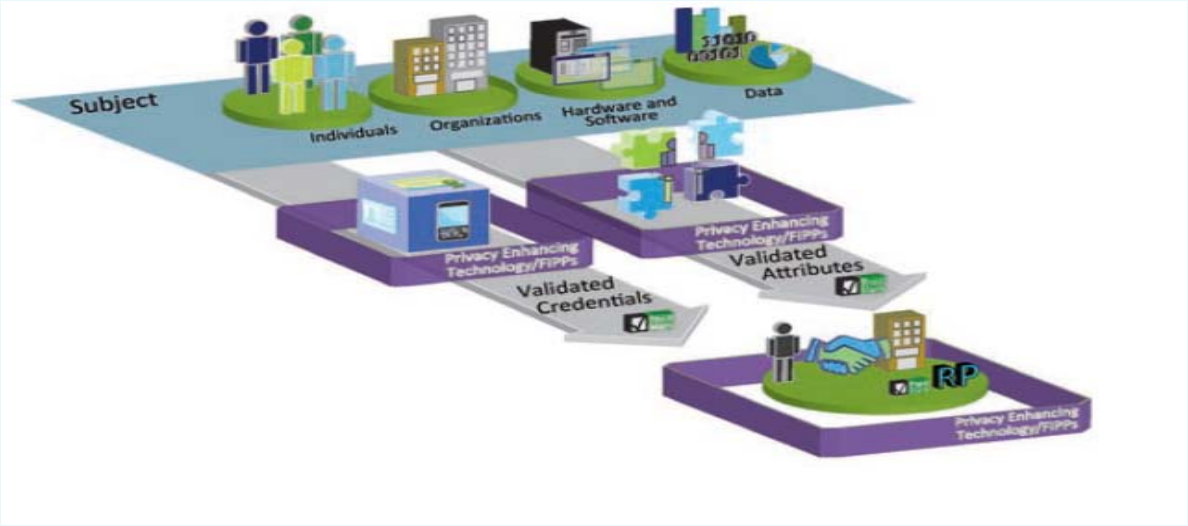
methodologies of authentication of the issuing terminal when storing the ID information, such as an e certificate, etc. and scheme such as a mobile access system, considering the way of exchanging ID information between mobile phones and outer terminals, through local communication.

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)

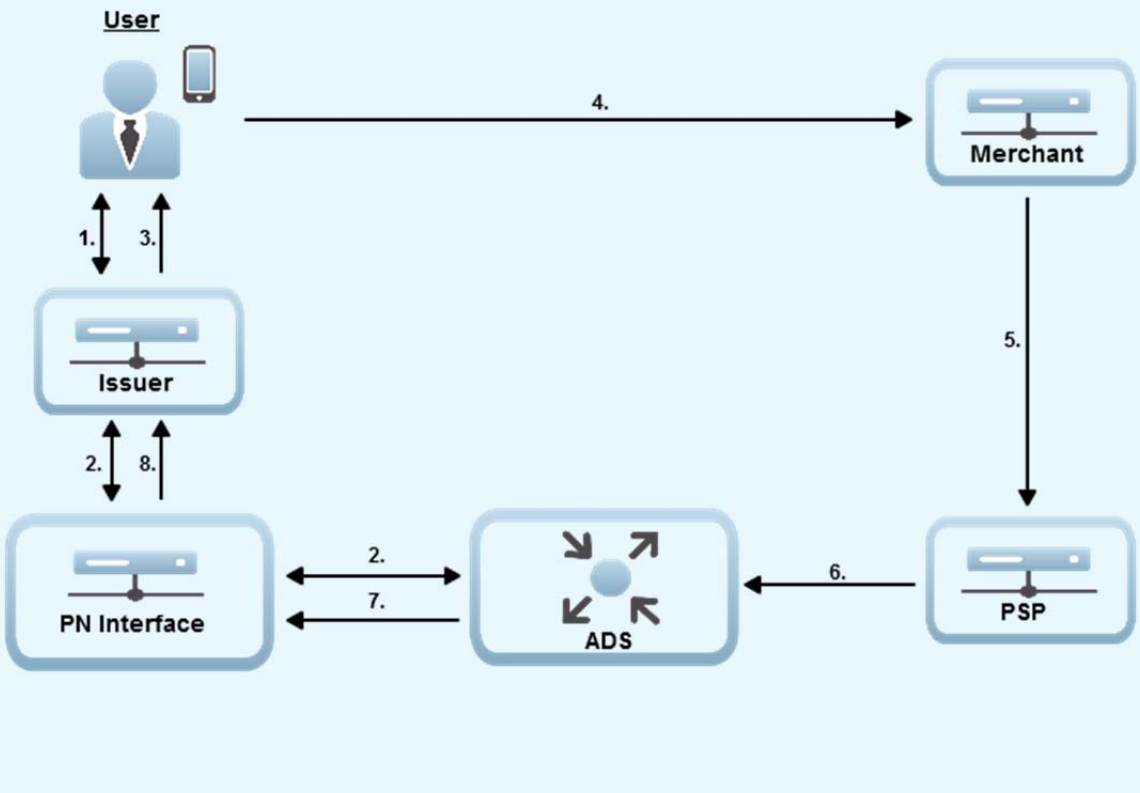
1. Open mobile payment app (can be set with or without PIN)
2. Choose pay and for example swipe mobile at POS-terminal (an OTT is shown on the mobile and transferred to the merchant)
3. Approve payment in app with PIN (can be set without need of OK or OK+PIN for low value transactions)
4. Receipt printed

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

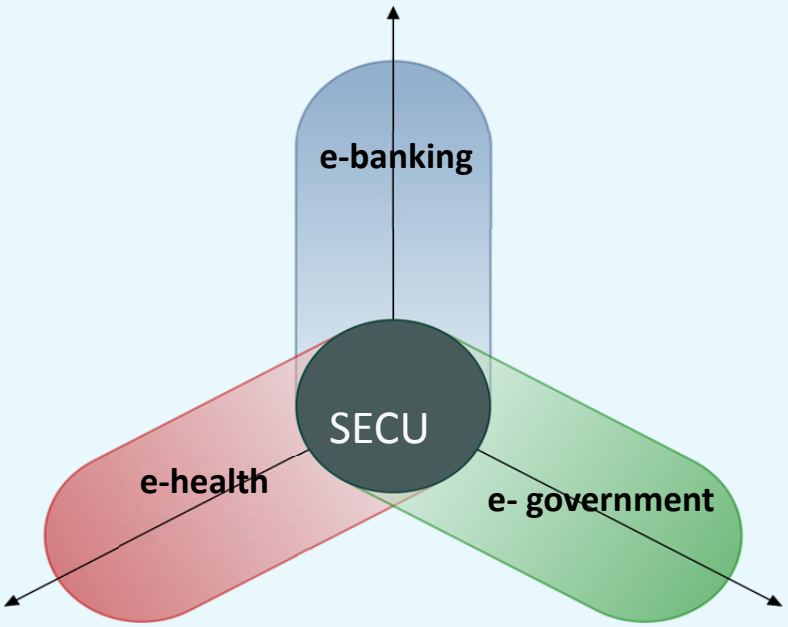
As shown in implementation cases described in chapters 6-9 above, development and usage of mobile devices for *m-Government, m-Health, m-Payment, m-Learning and so on* are at different levels in various countries, however, in today's global world the penetration of technology innovations increases drastically, 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

_____

Unión International de las Telecomunicaciones (UIT)
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Oficina del Director
Place des Nations
CH-1211 Ginebra 20 – Suiza
Correo-e: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Director Adjunto y
Jefe del Departamento de
Administración y Coordinación
de las Operaciones (DDR)
Correo-e: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Departamento de Infraestructura,
Entorno Habilitador y
Ciberaplicaciones (IEE)
Correo-e: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Departamento de Innovación y
Asociaciones (IP)
Correo-e: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Departamento de Apoyo a los
Proyectos y Gestión del
Conocimiento (PKM)
Correo-e: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

África

Etiopía

International Telecommunication
Union (ITU)
Oficina Regional
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Etiopía

Correo-e: itu-addis@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Camerún

Union internationale des
télécommunications (UIT)
Oficina de Zona
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Camerún

Correo-e: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des
télécommunications (UIT)
Oficina de Zona
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Senegal

Correo-e: itu-dakar@itu.int
Tel.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe

International Telecommunication
Union (ITU)
Oficina de Zona de la UIT
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

Correo-e: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Américas

Brasil

União Internacional de
Telecomunicações (UIT)
Oficina Regional
SAUS Quadra 06, Bloco "E"
11º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Correo-e: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication
Union (ITU)
Oficina de Zona
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Correo-e: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chile

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484 – Plaza de Armas
Santiago de Chile – Chile

Correo-e: itusantiago@itu.int
Tel.: +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

Correo-e: itutegucigalpa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

Estados Árabes

Egipto

International Telecommunication
Union (ITU)
Oficina Regional
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egipto

Correo-e: itucairo@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacífico

Tailandia

International Telecommunication
Union (ITU)
Oficina de Zona
Thailand Post Training Center ,5th floor
111 Chaengwattana Road, Laksi
Bangkok 10210 – Tailandia

Dirección postal:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Tailandia

Correo-e: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication
Union (ITU)
Oficina de Zona
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Dirección postal:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

Correo-e: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322
Tel.: +62 21 380 2324
Fax: +62 21 389 05521

Países de la CEI

Federación de Rusia

International Telecommunication
Union (ITU)
Oficina de Zona
4, Building 1
Sergiy Radonezhsky Str.
Moscú 105120 – Federación de Rusia

Dirección postal:
P.O. Box 25 – Moscú 105120
Federación de Rusia

Correo-e: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

Europa

Suiza

Union internationale des
télécommunications (UIT)
Oficina de Desarrollo de las
Telecomunicaciones (BDT)
Unidade Europa (EUR)
Place des Nations
CH-1211 Ginebra 20 – Suiza
Correo-e: eurregion@itu.int
Tel.: +41 22 730 5111

Unión Internacional de Telecomunicaciones
Oficina de Desarrollo de las Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza
www.itu.int

Impreso en Suiza
Ginebra, 2014

01/2014