最后报告

ITU-D第2研究组

第17-3/2号课题

电子政务活动的进展并确定可使发展中国家受益的电子政务领域

2010-2014年第5研究期

电信发展部门

联系我们

网站：	www.itu.int/ITU-D/study_groups
国际电联电子书店：	www.itu.int/pub/D-STG/
电子邮件：	devsg@itu.int
电话：	+41 22 730 5999

第 17-3/2 号课题

电子政务活动的进展
并确定可使发展中国家
受益的电子政务领域

ITU-D 研究组

作为电信发展局知识共享和能力建设议程的后盾，ITU-D 研究组支持各国实现其发展目标。通过推动为减贫和经济社会发展进行 ICT 知识的创建、共享和运用，ITU-D 研究组鼓励为成员国创作条件，利用知识更有效地实现其发展目标。

知识平台

ITU-D 研究组通过的输出成果和相关参考资料，被用于 193 个国际电联成员国的政策、战略、项目和特别举措的落实工作。这些活动还有助于巩固成员的知识共享基础。

信息交换和知识共享中枢

共同关心议题的共享是通过面对面会议、电子论坛和远程与会，在鼓励公开讨论和信息交流的气氛中实现的。

信息存储库

研究组成员根据收到的供审议的输入文件起草报告、导则、最佳做法和建议书。信息通过调查、文稿和案例研究采集，并通过内容管理和网络发布工具提供成员方便地使用。

第 2 研究组

第 2 研究组由 WTDC-10 受命研究涉及信息通信基础设施和技术发展、应急通信和适应气候变化等领域的九项课题。着重为在规划、发展、实施、运营、维护和持续提供电信服务过程中能够优化用户得到的服务价值，并能最合适、最成功地提供服务的方法和方式。该工作包括将具体工作重点放在宽带网络、移动无线电通信和农村与边远地区的电信/ICT、发展中国家对频谱管理的需要、ICT 在缓解气候变化对发展中国家的影响中的使用、用于减轻自然灾害和赈灾的电信/ICT、合规性和互操作性测试及电子应用，特别强调通过电信/ICT 手段支持的应用。该项工作还研究探讨信息通信技术的实施，同时兼顾 ITU-T 和 ITU-R 开展研究的成果以及发展中国家的优先事宜。

第 2 研究组与 ITU-R 第 1 研究组一道共同负责涉及第 9 号决议（WTDC-10，修订版）问题的研究 – 各国，特别是发展中国家对频谱管理的参与。

本报告是由来自不同主管部门和组织的众多志愿人员编写的。文中提到了某些公司或产品，但这并不意味着它们得到了国际电联的认可或推崇。文中表述的仅为作者的意见，与国际电联无关。

目录

页码

页码

图目录

页码

表目录

页码

第 17-3/2 号课题 电子政务活动的进展并确定可使发展中国家受益的电子政务领域

1 引言

1.1 ICT 变革及互联网应用的扩展

“互联网将改变一切”是对 ICT，特别是互联网技术所引发的根本性变革的概略表述。ICT 的发展及其全面的推广与应用，对社会的各个方面均产生了影响。人们将其称之为 ICT 革命。因 ICT 革命而形成的社会称之为信息社会。ICT 革命的具体体现为推行变革、创建信息社会，并对企业和公共服务等各行各业施加影响。互联网彻底改变了政府为公众及全球企业提供服务的面貌。许多国家对 ICT 应用的关注反映出这些政府及其国民相信，电子政务的核心技术将成为推行有效行政管理和为人民提供便利服务的强大动力，为信息社会带来竞争优势。

1.2 电子政务及国际电联第 2 研究组

ITU-D 项目 3 已与私营部门和联合国其它组织开展协作与合作，进行电子政务应用（包括服务获取和支付的现代系统）方面的研究。为充分实现电子政务应用的潜在益处，发展中国家需要了解有关战略、最佳做法、专业技术来源和经济支持以及各类电子政务应用和技术平台（能够按照其本国需求和当前能力，为本国人民带来最大福祉）的信息。

国际电联决定就电子政务问题成立一个新的研究组，该研究的主要课题为评估世界电子政务活动进展并确定可为发展中国家带来最大益处的领域，包括在农村和偏远地区将移动和无线平台用于服务提供和支付。

此项研究的输入意见来源如下：ITU-T 相关研究组（如第 13、17 研究组）研究与此问题相关的课题（鉴权、隐私等）的进展；电信发展局与联合国其它组织和私营部门开展的电子政务服务和应用举措的进展，其重点在于促进发展中国家的参与；国际电联总秘书处或电信发展局开展的所有其它相关活动的进展；成员国和部门成员提供的有关可用于提供电子政务应用的举措、应用或技术的进展报告和案例研究。

国际电联发布了电子政务实施工具包和电子政务就绪程度评估框架（2009 年）。此工具包通过对电子政务环境的重要领域的研究，依据相关方面的就绪程度和国家发展战略，帮助决策者确定行动的重点领域。此外，国际电联还仔细研究了移动技术，确定其对负责任的政府行为和社会连通产生的影响，并与经合发组织（OECD）和联合国经济社会事务部（UNDESA）共同起草了“移动政务”报告。该报告突出强调了移动技术在完善公共治理方面的重要潜力，深入分析了移动政务的各项前提、主要益处与挑战、价值链与核心利益攸关方，为决策者跟踪和更新有关移动政务的知识，开列了具体行动清单。

1.3 国际组织对电子政务的评估研究

电子政务问题被联合国、经济合作与发展组织、国际电信联盟、世界银行以及亚洲开发银行、非洲开发银行等地区发展银行视为发展中国家可持续发展方面的一项重要议程。联合国经济和社会事务部（DESA）自 2002 年以来便定期开展调查，研究国家电子政务发展层面的问题，给出各成员国在电子政务就绪问题上的排名。为此，联合国开发了一种由五个明确阶段构成的电子政务发展模型，各阶段均有特征性的相关指标。

OECD 早在二十一世纪初就成立了电子政务工作组，出版了多本涉及电子政务基本问题的书籍，例如 2003 年出版的《电子政务急需解决的问题》和 2004 年出版的《利用电子政务提升治理水平》。继这些书籍出版之后，芬兰（2003 年）、墨西哥（2004 年）、挪威（2005 年）、匈牙利（2007 年）、荷兰（2007 年）、土耳其（2007 年）等也分别开展了一系列电子政务研究，通过对各国电子政务水平和所做工作的评估，提出了相应的政策建议。OECD 的电子政务研究工作依然致力于主题研究，其输出成果包括 2007 年推出的《效益落实管理》和《将电子政务作为变革工具》，以及 2009 年出版的《电子政务身份标识管理系统成本效益评估的经济框架》。

世界银行开展的电子政务活动主要侧重于帮助客户国建立发展电子政务应用所需的必要制度，以此提升政府的管理水平并完善问责，特别是在提供公共服务问题方面。世行的全球 ICT 部门为设计和推出电子政务解决方案及应用提供了技术意见和投资支持。其具体内容包括，战略、政策、监管和法律问题、制度框架、企业构架和互操作标准、基础设施和服务的共用、培训和变更管理、电子政务应用，以及包括公私合作伙伴关系在内的融资安排。由世行提供此类支持的国家包括突尼斯、蒙古、加纳和卢旺达。

2 电子政务的原则

2.1 何为电子政务？

电子政务的概念形成于二十世纪 90 年代早期，由两个毫不相干的单词构成。一个单词属于技术术语，另一个却是管理体系历史长河中脍炙人口的熟词。尽管在引入之初新词的接受并非一帆风顺，但其很快便成为了大多数致力于实现管理现代化并建立创新结构的政府们急于达到的目标。未来主义者预计，改革之后，政府的管理系统必将出现革命性变化。

OECD 和联合国等国际机构为电子政务给出了定义。OECD 将电子政务定义为将信息通信技术（ICT），特别是互联网技术，作为提升管理水平的工具（OECD，2003 年）。联合国将其视为一种应用信息和通信技术改变内部和外部关系的管理方式。电子政务的终极目标是建立“良政”，从公众角度实现最为高效与便利的治理。电子政务的愿景是，塑造一种 ICT 框架，并使其成为向清晰、透明、高效治理成功过渡的关键因素。

电子政务的本质是改革公共管理，在电子技术的帮助下创建新型的内外关系，因此要按 OECD（2003 年）指出的那样，更加重视‘政务’而非‘电子’。依据这一点，电子政务问题被置于国家公共管理改革和优良治理的举措之下。电子政务不仅涉及技术创新，还关乎政府改革，既着眼于公共部门的需求，又要关注公民与企业，从而确保 ICT 能够在改变政府机构内部运作方式的同时变革公共和私营部门间的互动形式。

鉴于电子政务追求改变政府的内部运作程序和对外关系，即与公民之间的关系，因此应将其视作一种能让政府职能随社会变化而不断演进的流程。

2.2 电子政务 ICT 的发展趋势

2.2.1 电子政务 ICT 的特性

在当今技术驱动型的社会中，ICT 已成为政府改革进程中的桥梁。政府对 ICT 的使用现已十分成熟，成为其运作中不可分割的组成部分。信息基础设施，特别是互联网技术，具备开放性、互连性和可接入性等特征。因此，各国均将 ICT 视为变革的关键推动因素。电子政务问题被视作政府结构的变革，政府机构与公民间互动方式的改变。此外，ICT 是提升公民参与公共政策制定的一种强大工具。通过应用 ICT 来打破机构间的藩篱对改革政府机构至关重要，它能够精简公共行政管理机构，有时甚至能够消除机构的重复设置。ICT 亦增加了公众对政府机构的使用，让公民们参与到决策进程中来。

2.2.2 固定与移动

ICT 应用于政府改革伊始，大多数电子政务举措均是基于固定互联网技术。互联网的运作又是基于作为国家信息基础设施的地下固定线路网。电子政务仅能通过家庭或办公室等有限场所，以有线通信的方式提供。但随着移动技术的全面普及[1]，移动互联网和无线接入已对电子政务环境中产生了重大影响。移动技术提高了公共部门使用 ICT 完善内部运作和与公民及企业开展互动的能力。因此，电子政务的范围得到了扩大或是实现了向移动政务的革命性地过渡，成为公共部门下一代 ICT 应用中冉冉升起的新星。

发展中国家的固定宽带接入水平要低于移动接入。有线技术及固定宽带互联网所需的基础设施成本高昂，是造成此现象的原因。移动技术以创建和扩充通信信道的方式，为不存在互联网所需基础设施和有线电话服务的地区提供接入（OECD 和国际电联，2011 年）。廉价、随时可用的移动设备，为固定互联网业务曾十分有限地区的人们消除了接入壁垒。

在起初的 2G 时代，移动技术被视作访问大量信息和服务的一种低劣工具，而随着 3G 和 4G 网络一同问世的智能手机，为向公民和企业提供公共服务创造出前所未有的机遇。此外，移动技术使政府与公民的实时交流可能性大增，让政府官员能够了解公民的需求，以更快地反应速度提供相关解决方案。与此同时，实时通信使公民能够更好地了解政府的管理，增加了其参与决策进程的机会。

2.2.3 移动与社会

关于 ICT 在电子政务举措方面的发展，我们应当关注社会化技术，使政府以前瞻性的方式请公民就公共政策给出反馈，以便能对其加以改进。利用“脸谱”、“推特”等公众经常访问的网上渠道，政府可与大众直接接触，倾听人民对公共部门运作及公共服务的意见。社会化技术一经与移动设备结合，其对公共管理的影响便得到了加强。

政府将能够摆脱被动地对公众请求做出响应，参与到大量的社会媒体网站交流中去，了解人们对政府项目绩效的看法。尽管电子政务一开始只是提供信息和通过政府网站对公民的请求做出响应，但如今人们要求电子政务做的已不仅仅是被动的等待公众质询和投诉。ICT 在社会化技术方面的新前进方向，为电子政务举措翻开了新的篇章。

[1] 全球有 90%的人口能够使用移动网络，80%的农村人口可以接入移动网，OECD 国家移动宽带的签约率在 2007 年至 2009 年间以复合年增长 20%的速率上升。（OECD 和国际电联，2011 年）

2.2.4 强化政府透明度、问责制、参与和协作趋势的“开放政务数据”[2]

近年来，开放政府数据已成为多国的新发展趋势。此项趋势旨在与企业、民间团体及公民一起共同创造公共价值。这一政治模式是基于透明、参与和协作的原则。此项文化变革，使政府、公民及其它社会利益攸关方能够同舟共济。现将开放政府数据的核心价值总结如下：（i）透明：政府应当向公众宣布施政信息，以利问责；（ii）参与：政府应当积极寻求专业技能帮助，咨询社会各行各业，充分利用最佳信息制定政策；（iii）协作：作为工作中的一部分，政府官员应与公民和私营部门戮力同心，共同解决地方和国家的问题。

信息社会改变了人们对社会机构及其职责领域的看法。世界各国政府都在不断提升开放程度，与公民、媒体及其它利益攸关方分享信息，以此做为对被普遍接受的“良政”的响应，为实现和平与发展目标奠定基础。

开放政府数据（OGD）是开放性政府战略的支柱。此术语是指政府机构将其数据以人类能够读取和计算机（最好是能够由机器处理、采用开放格式的原数据或结构化数据，且开放性允许第三方重复使用这些数据）能够处理的方式放在网上。公众可以审核和下载这些数据，甚至可在此数据的基础上创建新的分析与应用。

OGD 将公民参与、政府问责和透明度提升到了全新水平，而这反过来又会促进公共服务的提供和公共资源的使用。尽管因数字鸿沟造成的“各国不同的发展水平会从经济和社会角度给政府、企业、卫生和教育等方面的相关应用造成影响”，但世界各国政府仍在越来越多地通过国家、区域及当地层面的互联网络使用和分享数据。

OGD 的内在价值和潜在益处似乎已十分明确，但通过积极交流设想与经验，仍能利用集体智慧对其加以拓展。由于政策制定者和利益攸关方缺乏对相关益处的了解以及技术知识的匮乏，各级政府（国家、区域、当地）发起和维护开放数据的举措将面临挑战。

这就要求公务员以及来自企业、科学界和民间团体的其它利益攸关方加强能力，从而能够启动、实施和评估具备创新和可持续能力的数据发布举措。人们已就更加透明、可靠、参与和高效的政府能够全面惠及社会和民主达成了共识，但近期研究亦指出，重复利用开放政府数据的新产品与服务将给经济带来积极影响。

目前，已有大量指标用于评估政府绩效，特别是针对电子政务。未来政府面临的挑战之一是，如何为衡量政府绩效设计和实施新的标准，以确保公民参与和开放政府数据举措得到监督和完善。有必要实现从公民角度对政府的“改革就绪程度”和“公共价值”的完善水平加以衡量的能力。近年来，在世界各地方兴未艾的开放政府数据举措明确的支持以下事实，即利益攸关方依然缺乏对此工具潜在益处的认识，不了解其如何能够实现政府透明和问责并促进社会和经济成果的全面推广。

2.3 电子政务的构成

2.3.1 门户网站、信息共享、安全

政府门户是电子政务的核心要素，可为公民和企业访问信息及公共服务提供便利。政府门户的关键设想是汇总各机构的信息与服务，并为所有信息与服务创立统一的访问网址。公

[2] 摘自电信发展局文件

民与企业将能够更好的了解政府信息和项目的负责人、主管部门和级别。与政府之间便利的互动，方便的获取官方文件和行政程序信息，将使公民更乐于参与政府工作，形成更具参与性的管理模式，公民也将更加密切地参与到相关决策进程中来。该门户是遴选与集成海量公共管理信息的有力工具。

随着电子政务技术向移动和社会化技术的演进，目前正在重塑该门户，使之能够成为政府主动寻求公民回应并征求社会各行各业意见的场所，实现决策总体效益的最大化。政府官员能藉此搜集人们对政府政策的看法。与从外部被动地对请求做出响应不同，取而代之的是政府机构将通过感受人民的需要来满足其诉求。

信息共享是电子政务实施的基本要素，支持政府业务流程的调整和集成。信息共享的基本设想是将信息存贮一次而非多次，这样公民和企业就不会因同样的信息被不同政府部门多次问及。公民可减少去政府办公部门的次数，申请某项服务时提交的证明文件也会减少。

信息共享旨在树立一个概念，即政府仅从公民和企业那里收集一次信息，并将其提供给所有政府部门使用。信息是高效政府管理的重要资源。通常多家机构都要求公民提供身份信息，例如纳税和驾照延期。如果与另一部门就某项业务进行交涉时，只需要提供补充信息，则公民与企业的负担将大大减轻。信息共享问题涉及支撑技术、法律、制度安排和组织文化等方面，其中最后一项备受重视，因为多次信息共享失败均是组织利己主义酿成的苦果。在此，信息被当作了一种权利，因此这些组织不愿与他人分享。

信息共享最为敏感的问题之一是，侵犯个人信息以及破坏薄弱的网络安全的可能性。为推行电子政务，如何强调隐私和安全保护都不为过。无论系统多么方便有效，如果隐私无法得到安全保障，则该系统必将遭到用户的抵制且很难恢复信任。保护个人信息可以从技术、法律、组织和文化措施方面着手。如果说信息共享是电子政务的核心要素和推广 ICT 应用的前提，那么信息保护就是防止在信息共享过程中出现个人信息泄露的方法。

2.3.2　网络、人力能力

高速网络是政府官员接入数据库和各类应用的基础设施。它们不仅是各政府机构间，即中央与地方政府以及各部委之间互连互通的前提，而且是公民和企业通过与政府互动获取信息和服务的必要条件。电子政务可以通过宽带网络提供卫生和教育等公共服务。电子卫生系统可为农村地区人口提供远程服务，电子教学系统使学生能够学习校内不能提供的课外知识。

用户使用已安装系统的能力是发挥电子政务系统最大效能的关键。在实施电子政务的早期阶段，经常会出现系统使用频率过低，而被指责为浪费投资的情况。遭受批判的原因很多，其中公民不具备使用系统能力的问题常被指出。培训人们的基本互联网使用技能，特别是在偏远地区，在电子政务实施的初期阶段仍十分重要。此问题已在数字鸿沟的探讨中有所涉及。尽管使用电子政务的差距有时与技术设施，例如缺乏价格可承受的设备和宽带互联网连接相关，但用户能力准备不足仍是妨碍最大限度发挥已安装系统优势的主要绊脚石。建议所有包涵电子政务内容的国家 ICT 规划都为政府官员和公民制定培训计划，特别是针对农村地区。

2.4 电子政务活动的类别

2.4.1 应用：G2G、G2C、G2B

G2G 和 G2C 分别是指‘政府之间’和‘政府与公民之间’。G2B 是指‘政府与企业之间’，从电子政务应用的特征来看，其与 G2C 十分相近。G2G 是负责处理后台业务的电子政务举措，G2C 和 G2B 是针对政府与公民和企业间的互动，即前台业务。

G2G 类举措的主要目标是实施工作流程创新，例如制定电子工作流程、扩大行政信息共享、开展基于服务的业务流程再造。电子文件系统、地方和中央政府的财政系统、电子审计系统等都属于 G2G 类别。

G2C 和 G2B 类别包括负责处理公民与企业服务创新问题的应用。韩国的 G4C（为公民服务的政府）服务是典型 G2C 应用。此外，国家福利体制、食品药品信息系统和就业与职位搜索信息系统，均是 G2C 的实例。G2B 是一种企业服务创新，其中包括处理公司行政事务的企业门户服务，提供行业信息以及为其它各类活动提供补充服务。上述活动贯穿企业从诞生至关闭的整个生命周期。此外，物流、外企等的信息系统亦属于此范畴。G2C 中的另一类应用，是一种鼓励公民参与公共决策进程的系统，对电子民主有巨大的影响。该系统旨在拓宽公民就某项政策提出意见及与各级政府互动的渠道。

2.4.2 融资

电子政务举措所需资金规模庞大，因此必须为其融资制定一项周密的计划。为给电子政务项目筹措资源，许多发展中国家都要依赖对电子政务的重要性有清醒认识的政治领导层。韩国国家 IT 计划实施的早期阶段便是这种情况。鉴于信息技术的特性很难展现出 IT 投资的效益，因此韩国政府决定预留一部分资金，专门用于依据总统行政令批准的 IT 项目。

IT 项目的融资问题引发了供需关系的辩论。学术届深知，在刺激新技术创新和应用方面，人们普遍认为需求政策干预的效果要优于供给干预。如对需求了解不足，则政府预算划分存在很高的失误风险。项目需求方面的核心问题是：哪些类型的服务能与电子政务项目所需的巨额投资相匹配？之所以要提出这一问题，原因在于我们可能会为不存在的问题推出一种价格昂贵的解决方案。

不幸的是，我们在此问题上进退维谷。一系列 IT 相关项目似乎创造了新的需求，但从本质上看，在供给成为可能之前根本无法对其做出预测。鉴于这些进退两难的境地，早期的电子政务项目遵从了供给方的设想。在韩国，电子政务早期的融资机制中反映出了供给方的战略。但是，以供给方的设想为中心，不能抹杀考虑某项电子政务业务服务潜在需求的重要性。例如，在确定将哪些业务放入电子政务举措内时，我们或可通过回顾政府与公民间网下事务处理的方式，将相关需求考虑在内。

2.4.3 法律和制度性安排

在筹备电子政务活动过程中，由于公共行政管理工作是严格基于立法，因此建立相关法律法规是电子政务取得成功的必要条件。例如，纸质文件曾被作为具有法律效力的政府管理文件，而在建立了电子政务系统之后，电子文件承担了公共管理的任务，所面要求应为电子文件制定相应的法律安排。通过合并和协调原先分布于不同政府机构的相关政府职能，可实现法律依据的相关安排。

为给电子政务奠定制度基础，在网下环境中制定的与民政事务相关的法律和行政命令，应为以电子的方式处理民政事务进行修订。即使已从技术角度落实了电子政务系统，如果不为政府官员和公民制定好电子政务系统运营的法律法规，他们的工作与思考方式仍然不会改变。

旨在有效推动电子政务活动的 IT 管理系统是制度安排中的一项重要内容，能够强化其组织结构。鉴于大多数电子政务项目通常会跨几个部门，因此很容易受到电子政务正常实施过程中所发生冲突的影响。为在相关机构间开展协调，专门为解决机构间分歧成立了特设委员会。委员会的成员不仅来自相关机构，亦有在协调过程中将采取中立态度的独立专业人士。

3 成员国的最佳做法（ITU-D 文稿）

在第 3 研究期（2010 – 2012 年）以往的 3 年内，共向九月召开的研究组会议提交了 12 项电子政务举措案例。由于内容相似，关于孟加拉国的 2 个案例被合二为一。各文稿的摘要按提交顺序排列。各文稿的完整版本请参见本报告最后的附录。

3.1 INV（信息网络村）项目（韩国）

此项目旨在为偏远地区居民获取教育、医疗和农业技能等方面的各种信息提供支持，缩小城市与农村间的数字差距。另外，该项目还为直接向消费者直接出售当地土特产提供了渠道，使当地生产者获得更多收益。该项目通过这种方式在促进地方经济，平衡全国各地区发展方面发挥了作用。为偏远地区人口提供基本互联网技能培训，将拉动人们对电子政务的需求。[3]

- 旨在为农村/渔村、边远地区和其他远离信息革命的地方建设宽带互联网基础设施，以解决城市和农村地区的信息鸿沟问题。也期望以此夯实电子政务和电子民主的基础。
- 创建用于本地产品的在线市场等信息内容，以产生实际的效益并恢复本地经济的活力，实现国民经济的平衡发展。
- 使得本地居民在日常生活中更加容易地通过互联网获取有关教育、医疗、文化和农业技能的信息。
- 各村成立了“INV 项目管理委员会”。该委员会确定与信息村运行有关的重要问题。也鼓励创建商业模式，以便委员会即使在没有政府支持的情况下也可自力更生。考虑到当地的独特情况，根据当地需求认真设计了 INV 模式并在严格评估后在全国推广。
- 通过 INV 项目学习如何使用信息系统是项目取得成功的一个关键因素。
- 该项目涉及举办各种活动，提高公众对 INV 项目的认识。

[3] 在 2010 年 9 月 14 日召开的第 2 研究组第 1 次会议上做了介绍。

- INV 项目侧重于提高当地居民的 IT 能力，确保其在飞速发展的信息社会中能够生存。例如，INV 项目的目标之一就是通过本地电子政务项目向当地居民提供网上公共服务。

- INV 项目取得了以下成果。首先，落实前述举措有助于通过改善农村居民等信息缺乏人员的互联网使用环境，消除数字鸿沟。

- 由于 INV 提供了培训，使得边远地区的居民可以享受这些电子政务服务。

- 此外，还为吸引人们参加 INV 项目建立了若干激励机制，例如将电子商务项目放入 INV，以便通过电子贸易出售产品的方式获取得多利益。

- 旨在缩小农村和渔村等信息匮乏地区数字鸿沟的 INV 项目正在成为其他国家的基准。

- 鼓励参与的村庄与有意发展村庄的私营企业通过 INV 项目结成姐妹合作关系。

- 例如，在参观信息网络村时，英特尔公司（世界最大的芯片生产厂商）的一名高级主管称赞韩国的 INV 项目是数字农业和渔村前所未有的典范。

3.2 韩国（大韩民国）在线电子采购系统（KONEPS）

KONEPS 在线处理整个采购业务流程，从发布招标公告、开标、到签订合同、付款。通过连接到政府信息共享设施，KONEPS 消除了提交营业执照和纳税证明等纸质文件的必要性。它将 160 多个官方文件表格（包括标书、合同、视察通知和付款通知）数字化，以便进行电子处理。因为 KONEPS 在线进行支付流程（包括提交报告、视察和付款通知），它可有效减少付款前的等待时间。这是因为负责签订合同、视察和付款的每个部门将其各自的工作集中在同一个平台上，由此简化了付款流程。

已决定各个部门不能分别自行开发电子采购系统，而是建议开发一个标准系统，但根据不部门的不同要求进行实施。2001 年 6 月公布了避免预算浪费的“防止重复开发的导则”。在推动电子政务项目的过程中，修订法律和规章与构建系统本身同样重要。[4]

- 构建 KONEPS 的基础设施技术包括基于公钥基础设施（PKI）的电子签名、文件安全技术、电子数据交换标准和进行大范围网页服务。

- KONEPS 以电子方式公布所有公共机构的招标信息，由此作为公共采购的一个唯一窗口。

- KONEPS 也连接着政府会计系统，采购部门可通过资金电子转账管理其付款。

- 随着智能手机的广泛普及，移动业务将在采购市场中越来越普遍，PPS 则继续开发借助移动电话的移动采购业务。

- KONEPS 大大提高了公共采购流程的透明度。

- 在信息技术全球大会（WCIT）上，PPS 被授予采用信息技术的最佳服务创新公共机构。

[4] 在 2011 年 9 月 11 日第 2 研究组第 2 次会议上做了介绍。

- 为开发集成的采购系统，从服务、数据和技术结构这三个角度对 KONEPS 进行了审核。

- 此外，KONEPS 将与公共采购服务（PPS）的工作系统集成，从而使从事公共采购服务的政府官员能够充分利用电子政务举措。

- 当前，正在依据服务项目的类别以及 PPS 结构内的工作流程，分别对数据进行管理。

- 最后，在采购业务集成和 KONEPS 运营数据重组的基础上，将对其结构加以分析并根据为电子政务制定的标准开发框架 eGovFrame，重新设计该系统。

3.3 乌干达的电子政务之路（乌干达）

乌干达政府一直坚信 ICT 不仅在变革政府运作方面，还在改善政府与民众、政府与企业以及政府内部各部门之间的关系方面有着很大的潜力。乌干达通向电子政务的道路始于 2003 年的 ICT 政策，该政策主要强调构建全国 ICT 基础设施的必要性。在 ICT 政策之后，于 2004 年进行了全国的电子就绪情况调查。2005 年，专门在政府内部进行了电子就绪调查。
2006 年，在中国政府的协助下，乌干达开始在全国发展电子政务基础设施。第一阶段涵盖坎帕拉和恩德培的所有中央政府各部委，也覆盖了 Bombo、Jinja 和 Mukono 的城市。网络向各部委提供了基本话音业务、电视会议和数据。

目前，各部委之间的服务是免费的。当前正在四个部委之间进行试验。这种协作在相同软件平台上运作。第二阶段涵盖乌干达东部、北部和西部，将于 2011 年末投入使用。私营部门也在全国开发了 ICT 基础设施，这也可以用于电子政务。[5]

- 制定了网络法，即《电子交易法》、《数字签名法》和《滥用计算机法》。这些法条将于今年末开始实施。

- 具备必要的基础设施后，乌干达制定了电子政务框架，以指导电子政务的实施。该国所有的区级当地政府均根据农村通信发展计划（RCDP）开发了网页。尽管各地区在定期更新、支付网页托管和互联网费用方面面临问题，但还是在网站上公布公共、投资和其他商业信息机遇。

- 正在开发乌干达政府的门户网站，作为政府服务的门户网站并连接到企业部门。

- 信息通信技术部正在与联合国工业发展组织协作，在 Mityana、Iganga、Lira、Rukungiri、Kamwenge 和 Busia 六个区建立试验型区级商业信息中心，改进向公民提供的 ICT 服务。

- 已建立了一个国家数据库，提升整个政府范围内的数据存储、使用、共享和安全。

- 考虑到乌干达的移动电话普及率高于计算机/互联网普及率，私营部门的绝大多数举措基于移动电话。

[5] 在 2011 年 9 月 11 日第 2 研究组第 2 次会议上做了介绍。

3.4 乌干达在欠发达地区实施宽带连接的方法（乌干达）

乌干达通信委员会（UCC）设立了农村通信发展基金（RCDF），鼓励在农村和欠发达地区提供电信业务。因此，RCDF 成为一种影响该国农村欠发达地区通信基础设施和服务的机制。

尽管该行业已经放宽限制，引入竞争，但该国一些无利可图的地区仍无法吸引私人资金投资于基础设施和业务。RCDF 的主要目标包括在合理的距离范围内提供基本电信业务的接入；确保农村电信发展的有效投资并促进乌干达的 ICT 使用。

乌干达的普遍接入政策（2010 年）是在全球发展议程，即《千年发展目标》（MDG）（乌干达是该文件的签字国之一）以及其具体的国家发展规划（2010 年）的前提下制定的，后者源于称为“愿景 2025”的国家愿景。该政策也是基于以往普遍接入政策（2001 年），在乌干达 ICT 政策和电信政策范围内制定的。

互联网未向农村地区扩展的一个主要原因是接入费用、带宽不足和电力问题，且对于农村社区而言，更重要的是文盲和缺乏相关的以本国语言制作的本地内容。因此，新政策的主要目标是确保提供宽带连通性并支持开放本地内容。

如今，乌干达 ICT 行业的主要障碍是缺乏用来加速接入和使用（特别是）互联网以及一般意义上的 ICT 的宽带基础设施网络。尤其是因为大量的资金需求无法只依靠私营部门来满足，因此政府需要专门介入。

乌干达政府开始支持采用国家数据干线基础设施，将所有地方政府首府和主要城镇相互连接起来，以便向用户提供更多具备成本效益的 ICT 服务。此举有望促进建立公共机构数据接入点，最初侧重于职业、高等和中等教育机构以及 IV 级和 III 级的政府医疗机构。将为选定的乡镇提供连入高速国家骨干基础设施的宽带连接。此连接视为乡镇的“最后一英里”解决方案。为此，正在进行一项详细研究，以决定每个地点可实施的最具成本效益的技术解决方案（无线、有线）[6]

- **电子政务：**该项目将协助收集基层当地政府上报中央政府的信息。这些信息将成为国家人口特征和其他社会经济相关统计数字不可或缺的一部分。
- **电子教育：**该项目将促进电子学习且这已在该国国内越来越受到欢迎。例如，主要的地方大学已在内地设立了分校，正在提供远程教育和在线教育。
- **电子医疗：**该项目将促进从本地社区向医疗中心，再向地区和区域性转诊医院并最终向国家转诊医院进行数据和话音传送。反方向传送也将启动。预期卫生部总部和地区办公室之间以及部机关与医疗中心之间还会有额外的业务流量。

乌干达的互联网普及率、接入和使用水平仍很低，估计用户为整个人口的 5%。由于私人服务提供商的商业考虑，此类服务主要局限于城市商业中心。尽管乌干达此前的政策支持在所有欠发达地区安装互联网接入点，但互联网带宽速度和服务质量问题（中断）一直是最终用户的主要关切。

[6] 在 2011 年 9 月 11 日召开的第 2 研究组第 2 次会议上做了介绍。

3.5 地方政务信息系统（LGIN）

大韩民国宪法规定，“地方政府负责处理与地方居民福利相关的事务，管理财产，并在法律限定的范围内制定地方自治法规方面的相关细则。”在项目实施时，韩国有 16 个省级政府，其中包括 7 个大城市级政府、9 个省级政府和 234 个市/区级政府。地方政府负责领导行政事务的管理和监督，但法律另有规定的事务除外。地方行政职能包括中央政府委派的职能，如公共财产的管理、设施的运行、税收的评估、地方税及各类服务费的收取等。省级政府设有教育委员会，负责处理与各社区的教育活动及学生活动相关的事宜。一般来说，省级政府在中央和下级（市/区）地方政府之间发挥中介的作用。

- 在降低政务成本、改善客户服务和实现更有效的跨区信息共享方面，各国政府均面临着来自选民的巨大压力。
- 如 LGIN 一类的新系统为政府官员带来的是一个全新的工作环境。
- 此战略可扩展到业务流程和应用服务案例层面。
- 这促成了政府机构之间的信息共享，进而改进了地方政府的内部运作，同时提供公共服务给予了便利。
- 此外，各地方政府共享信息和数据亦减少了处理公共服务所需的文件的数量。
- 在 LGIN 项目的实施过程中，工作流程的简化亦消除了提供公共服务时的重叠程序和管理工作。
- 公共行政效率的提高将可改善公共服务环境，增加公众对政府行政部门的信任。
- LGIN 系统是一种支持所有公共服务领域的信息基础设施。
- 在有限的应用领域亦可提供移动服务。

为充分发挥中央政府电子政务应用的效果，LGIN 系统不可或缺，原因是中央安排的各项公共服务均应通过相应的地方政府渠道加以分配。

上述项目成功因素也可以说是我们从项目实施过程中汲取的经验教训。LGIN 系统之所以能取得目前的成功，是因为其有效应对了如下问题[7]：

- 如何在各相关机构间解决与项目相关的争议；
- 如何资助项目，并在中央和地方政府之间分配相关成本；
- 如何在引入新的技术系统时解决相关人士的心理负担，并打消其在工作不安全方面的隐忧；
- 由于全国性项目的实施过程复杂且规模庞大，如何避免因潜在故障而产生较大损失；
- 如何获得政界和政府领导的支持，以便在融资和修订相关法律和法规方面获得有利条件，等等。

[7] 在 2012 年 9 月 17 日召开的第 2 研究组第 3 次会议上做了介绍。

3.6 孟加拉国 ICT 相关业务的概述

孟加拉属于世界上人口密度最高的国家之一，但就电话密度而言，仍然是南亚普及率最低的国家之一。传统上，只有一小部分人可以接入电信设施。仅在 10 年前，其电话密度仍在 1%以下，但移动电话的到来改变了这一切，目前孟加拉的电话密度超过 46%。

在某种程度上，由于移动市场的迅速发展，孟加拉的整体状况有了改善。在政府活动中采用各种信息通信技术（ICT）已是近年来的常见现象。

迄今为止，采用了各种技术支持电子政务的独特特性，其中包括电子数据交换、互动式语音响应、语音邮件、电子邮件、网页服务交付、虚拟现实和关键公共基础设施。

电子政务指公共部门采用信息技术提供服务和信息，鼓励公民通过让政府更透明和问责的方式民主参与决策进程。需要开发一个优秀的官方门户网站和信息库，向公民提供所有来自不同政府部门的必要信息。公众应可下载各种表格和申请；而且，为了减少官僚主义作风，可增加在线申请。为了增加透明度并减少腐败，也可通过此门户网站进行招投标、报税和地皮分配。但我们应认识到，谈及移动政务时我们仅是指与政府进行电子通信的一种方式，且只有在电子政务系统存在的情况下其才有意义。[8]

- 电子政务指公共部门采用信息技术提供服务和信息，鼓励公民通过让政府更透明和问责的方式民主参与决策进程。
- 应采用适当的以 ICT 技术为导向的营销战略在全球市场推广产品和服务。
- 可建设一个专用的企业网络，用以鼓励企业界使用 ICT。
- 在线存货交易系统将涉及到更多的来自不同行业的交易商参与资本市场。
- 法律和卫生系统也在社区的方方面面发挥着重要作用。
- 在所有公立医院配备优秀的医患管理系统将改善偏远地区的卫生医疗系统。
- “全球村”环境以与互联网发展同步的速度不断变化，重组和转型。
- 为保持在全球市场上的竞争力，孟加拉国必须通过落实电子政务的方式紧跟发展的步伐。
- 孟加拉国的电子政务刚刚开始，但互联网革命已然如火如荼。
- 在孟加拉国拓展电子政务机遇良多。

“数字孟加拉”是一个持续发展进程。可靠且可持续发展的全国性网络基础设施将强化国家的信息高速公路建设并消除城乡之间的数字鸿沟。权力下放的同时，可向所有公民提供数字政务服务。

[8] 在 2012 年 9 月 17 日召开的第 2 研究组第 3 次会议上做了介绍。

3.7 吉尔吉斯共和国电子政务实施的经验和今后的行动步骤

吉尔吉斯斯坦采取了十分积极的姿态，指出了信息通信技术（ICT）作为加速国家发展工具的重要性。中期国家发展战略（2012-2014 年）和特别政府项目 –“稳定与有尊严的生活”明确提出了人们对电子政务的迫切愿望，以及只有通过此项服务方可实现国家治理的电子化变革，满足普通公民的需求。如今，吉尔吉斯共和国公共行政管理机构的计算机化水平令人满意，特别是那些中央政府部门。需要处理大量信息数据的多数部委，都有专门的服务器用于承载数据库、电子邮件系统、互联网接入和其它服务，有时甚至有专门的部门负责数据处理和管理。许多部委和政府管理部门都在开发自身的局域网和能够接入互联网的信息系统。

与吉尔吉斯共和国电子政务相关的法律框架相当健全，包括 16 项有关 ICT 的法律。但是，还需要起草和通过更多法律，以便为在该国进一步推行电子服务和信息交换打开大门（例如，有关电子商务的法律、统一的技术标准和要求）。

吉尔吉斯共和国于 2002 年通过了相关国家战略和行动规划，即针对 2002-2010 年提出的“吉尔吉斯共和国 ICT 发展”。2007 年 UNDP 对此项战略实施所做评估揭示，其仅实现了30%的目标。

吉尔吉斯斯坦已认识到为全体公民和企业提供现代技术和服务的重要性。电子政务和电子服务将为国家行政部门使用信息技术提供机遇，使其能够为公民、企业和参与治理的其它各方提供更好的服务。[9]

- 吉尔吉斯共和国**财政部**于 2012 年发起了若干有关预算透明的电子举措（http://www.okmot.kg），例如：“透明预算”（http://budget.okmot.kg）– 便是一种能够提供中央与地方预算收支数据的自动系统。这是该国首次实现普通公民和法律实体自由查询有关国家预算落实情况的数据。显示的数据包含从独立接收方到政府机构和地区在内的各级预算划拨情况的详细信息。该数据与中央财政数据库的电子互连进行了网上更新；“国家电子采购”（http://zakupki.okmot.kg）– 是一种国家采购自动系统，其覆盖范围包括网上登记、投标和其它相关信息与行动。“网上经济地图”（http://map.okmot.kg）– 是一种吉尔吉斯共和国的电子地图，实现了该国各地区所有社会经济数据的可视化；

- 吉尔吉斯共和国**国家统计委员会**积极地开展了电子数据采集与分析的落实工作。该机构制定并批准了 2020 年前的 ICT 公司战略。

- **税收委员会、海关和边境管理**国家机构亦在其工作中积极的应用了电子工具（电子声明、机构间电子数据交换等）。

- **社会基金、强制医疗保险基金、卫生部和社会发展部**，为提供电子社会服务和数据交换积极地升级了其社会信息系统和数据库。

- **司法部、内务部**在部委内部引入了电子文件交流，并为人力资源管理系统提供了恰当的软件工具。

- **外交部**启用了电子签证和电子文件流程。

[9] 在 2012 年 9 月 17 日召开的第 2 研究组第 3 次会议上做了介绍。

不同行业电子服务项目的实际推广经验揭示，在国家层面推行 ICT 发展需要有政府的领导。这一领域缺乏协调会造成工作重复及捐助人和政府资源的低效使用。机构间的协调不善会导致电子互连的难度加剧。创建有效的 ICT 协调机构，设立国家电子互操作标准，统一集成电子服务基础设施是在吉尔吉斯共和国成功实施电子政务的关键。

3.8 在日本以业务协作的形式通过手机终端提高接入行政管理业务系统的便利性

先进信息通信网社会推广战略总部制定的“信息通信技术（IT）新战略路线图”提出了如下目标：推出以多样化手段获取行政管理服务的项目，更新政府门户网站，鼓励人民使用政府服务；2011 年，开发、验证并展示以手机鉴权的方式通过移动手段使用行政业务的做法；2012 至 2013 年，在上述演示的基础上，首先在测试内引入、发展并局部推广该服务，然后逐渐在全国范围部署；到 2020 年，实现极度便利的电子行政管理服务，即‘一站式服务’。

在此项目的基础之上，MIC 于 2011 年开展了“合作企业行政管理系统推广项目（验证提升手机接入用户友好程度的各种方式）”，其工作是基于 2009 年实施的“有关电子行政管理业务等服务接入手段多样化的研究（对将手机作为接入电子行政管理等业务的技术开展研究）”取得的调查研究成果。

具备近场通信（NFC）功能的移动终端将于 2012 年商业化。这些终端实现了将业务用户个人信息以 ID/口令、点数或优惠券等形式加入防篡改装置，并支持信息的读取。这些功能的使用，让通过手机终端获取电子政务服务时的用户鉴权变得更加方便，公民无论老幼均可便利、安全的利用移动终端使用行政服务。

2009 年开展的研究，对下述用户 ID 信息（由服务提供商下发，作为电子政务移动接入的手段）存储空间的安全性进行了审核：1）公共 IC 卡系统，使用时将政府颁发的公共 ID 卡置于手机附近，2）移动电话的公共卡系统，使用时将政府发行的合规卡插入移动终端，3）公共身份信息系统，使用时将政府下发的信息写入移动终端。防篡改装置包括 1）为公共 ID 卡发行的全尺寸 IC 卡，2）用于移动电话公共卡系统的、包含 IC 芯片的闪存，3）用于公共身份卡系统的通用集成电路卡（UICC）。

除上述审核之外，为在防篡改装置中存储和使用 ID 信息或用户信息，有必要为各服务提供商的移动电话开放并安装一种应用程序（下文称移动应用）。此外，用户需要下载和安装服务提供商提供的不同移动应用。换言之，防篡改装置给服务提供商和用户都带来了不便。为给用户创建一个便利的环境，同时为服务提供商的业务提供与操作提供方便，我们对移动接入系统的技术规范进行了审核。

为克服这些困难，我们研究了用户和服务提供商都能使用的系统。换言之，我们研究的移动接入系统技术规范包涵了用于存储和安全读取的服务器而非仅是服务提供商，另外其中还包括供防篡改装置各项业务存储和使用 ID 信息的移动应用。此外，研究工作还包括技术规范的实践验证，针对制度和操作的规范以及这些问题的解决方案。

发展中国家拥有移动终端的人口越来越多，且智能手机用户的数量也与日俱增。因此，对发展中国家而言，公共服务理应在此领域占有一席之地。[10]

[10] 在 2012 年 9 月 17 日召开的第 2 研究组第 3 次会议上做了介绍。

3.9 黎巴嫩的电子政务

电子政务路线图是基于黎巴嫩政府对建立电子政务门户网站的积极参与，该国政府希望以此推动和促进公众使用公共服务和公共信息。

电子政务侧重于实现以下战略目标：建立以民为本（而非官僚政府）、以结果为导向、以市场为根基（积极推动创新）、推行良政，能够确保经济发展和社会包容的政府[11]。

- 电子改革：为重塑政府工作流程，充分利用技术并将 ICT 作为改革进程的先锋，提供理想的机遇。
- 电子公民：将黎巴嫩政府为其公民提供的、有望以电子形式实施的所有服务集中在一起。
- 电子企业：侧重于为黎巴嫩企业团体和外国投资商提供的重要政府服务。更加有效地提供这些服务有助于促进黎巴嫩私营部门的发展，从而带动国民经济的发展。
- 电子社区：目前的普遍共识认为，ICT 在参与新兴知识经济方面发挥着核心作用，在促进经济增长、推动可持续发展、能力赋予及减贫方面拥有巨大潜力。
- 不同领域的电子政务举措：法律、ICT 基础设施、垂直应用，以及不同的国家标准和政策。

电子政务路线图被定义为一组宏观活动和关键性的里程碑，其中包括法律、行政管理、基础设施、企业流程整改、互操作和电子政务门户等方面。此路线图将得到能力建设计划的支持，此项计划将使政府职员具备有效且高效利用所有电子政务项目的能力。

下一步是筹备可能会获得黎巴嫩政府通过的不同法律草案、决定和技术项目，例如：

- 法律项目 – 电子交易
- 法律草案 – IT 业薪金等级表法案
- 通过电子交易法
- 程序简化

3.10 MWANA（赞比亚）

由于社会因素和 ICT 技术的迅速进步，ICT 在赞比亚的作用和影响得到了飞速提升。根据 ZICTA 有关 ICT 使用的调查，赞比亚总人口为 1200 万；其中 780 万能够使用移动网络，400 万能够接入互联网。该团体业务需求的增长和 ICT 使用的增加，迫使政府和私营部门更具创新性，并大力投资于电信回程网络建设。[12]

- 加强婴儿早期诊断，增加收到诊断结果母亲的数量，利用 SMS 以更快、更有效的方式与母亲联系（移动卫生）。

[11] 在 2012 年 9 月 17 日召开的第 2 研究组第 3 次会议上做了介绍。

[12] 在 2012 年 9 月 17 日召开的第 2 研究组第 3 次会议上做了介绍。

- 提高产后跟踪的比例，增加诊所和社区新生儿登记的数量，同时使用“RemindMi”应用程序并通过社区医疗工作者跟踪，增加母亲去诊所的次数。
- 提升政府为公民提供服务的水平。
- 减少官僚现象，缩短提供政府服务的时间。

部署的技术和解决方案：

- SMS 技术- 通过此项强有力的创新，赞比亚缩短了接收 DBS HIV 婴儿早期诊断（EID）测试结果的时间，加强了医疗卫生提供商和社区志愿者间的沟通，更为重要的是提升了患者的信心，鼓励其返回诊所领取测试结果。
- RapidSMS 技术- 解决 HIV 婴儿早期诊断（EID）问题。SMS 消息被用于将测试结果从处理 HIV 结果的实验室发送至采集样本的医疗诊所。对于小型诊所，测试结果将发送至手机，针对大型诊所，结果将传送至 SMS 打印机。该系统亦将跟踪抽样，并为省级和地区级官员提供实时跟踪服务。
- RemindMI – RemindMi 用于产后护理的患者跟踪工作。SMS 消息被发送给社区代表，由其寻找看护人和婴儿，请他们于第 6 日、第 6 周和第 6 个月进行产后复检，或在检查结果到达诊所等特殊情况下返回诊所取件。

全国性的升级计划业已制定。首先是筹备阶段，然后是对诊所人员的不断培训，接下来经过培训的人员会被加入系统并对人员添加的成败做出评估。计划的目标是于 2015 年实现全国范围内的医疗机构均能提供婴儿早期诊断服务。筹备阶段将着力巩固技术、物理、监测和人力资源基础设施，以应对升级带来的压力。在整个升级进程中都将对该项目进行密切监视，以确保这些系统会对特定的卫生挑战产生积极影响。

3.11 黑山共和国的电子政务服务

黑山意识到了发展与应用 ICT 的重要性，且过去在此方面迈出的步伐较大。从世界经济论坛-网络就绪程度指标（ISM）的排名便可明确地发现，该国在 138 个国家中排名第 44 位，远高于该地区的其它欧洲国家。鉴于移动网络用户的渗透率已接近 200%且互联网用户的普及率在持续上升，不难看出黑山的 ICT 部门正在经历大发展。[13]

- 可持续的 ICT – 其项目包括：ICT 基本内容（技术框架、无线电频谱框架、消费者保护框架）、ICT 基础设施、法律和监管框架、以完善宽带基础设施为目标的信息安全，旨在创建一个充满竞争力且能够可持续发展的 ICT 行业的法律和监管框架。
- 服务于社会的 ICT – 其项目包括：电子教育、电子卫生和旨在鼓励社会各方使用现代技术的电子包容性。
- 公共管理中的 ICT – 其项目包括：电子政务，该服务侧重于鼓励公共管理部门以创新方式使用信息通信技术，从而达到提高国家机构所提供服务质量的目的。
- ICT 促经济发展 – 一种研发和创新项目-在科学研究发展中使用 ICT 技术，通过建立人才库、鼓励创新和企业家精神的手段，建立一种高效、可持续发展的 ICT 系统。

[13] 在 2012 年 9 月 17 日召开的第 2 研究组第 3 次会议上做了介绍。

- 为在黑山实施电子政务，信息社会和通信部设立了电子政务项目的门户网页 – www.euprava.me，下文将称之为门户。通过该门户，所有公共管理机构和地方自治部门均可以电子方式为个人和公司实体及其它机构提供服务。
- 电子文件管理系统（eDMS）项目的主要目标是实现黑山政府业务办公室的信息化和电子化，从而提升效率、节约时间，更好地管理文档资料。

未来的步骤与工作将聚焦互操作框架，其本质并非一种用于定义、设计和提供公共服务的技术文件。

尽管提供公共服务多数情况下均涉及信息系统间的数据交换，但互操作仍然是一个广泛的概念，存在就普惠性的商定目标开展协作的可能。

4 最佳做法工具

4.1 使用移动通信的 ICT 服务的工具包

[14]创建 ICT 服务的工具包描述了用于电子政务服务的移动通信以及如何将所有需要认证和安全连接的移动服务（如移动电子政务（m-Government）、移动支付（m-Payment）、移动银行（m-Banking）和移动卫生（m-Health））整合起来。报告的该部分描述了创建这些服务的一般性原则并概括了 ITU-T 有关安全方面的建议书。

- 移动通信除满足自身在用户之间话音通信和消息传送方面的主要目的外特别方便用于其它应用，如移动商务、移动卫生和移动政务等，这里“m”代表“移动”。然而，应认识到，移动政务只是政府采用的多种电子通信手段之一，移动卫生、移动教育、移动商务和移动支付亦如此。

尽管手机的显示器和键盘尺寸较小，但人们依然期盼将其用于电子政务服务。今天移动通信的迅猛发展和其显著的优势使基于移动终端和被称为“移动”的服务（移动政务、移动卫生、移动支付、移动学习等）显示出巨大的潜力，因为：

- 虽然个人电脑并非人手一台，但几乎每个人都拥有手机（根据国际电联 2011 年底出版的题为“2012 年电信改革趋势”报告，全球共有 60 亿移动用户，而互联网用户还不到一半）。
- 手机永远带在机主身边且一直在线；
- 在一些情况下，移动通信可能是唯一可用的通信方式；
- 移动通信在安全性上不亚于互联网。

4.1.1 安全移动服务的移动原则

用来提供安全远程服务（无论是移动电子政务、移动医疗，还是移动商务）的移动系统在通常情况下应具备能够在移动终端用户和服务提供商之间安全传输数据块的基础设施。为确保安全性，该结构必须具备认证和加密元素。所传送的数据块可包含需要安全处理的保密

[14] 这部分为 Intervale 文稿摘要，文稿全文见附录。

信息。数据交换只应在授权用户之间进行，第三方不得接入。数据交换还应经过适当登录，以避免不可否认性。用户认证须采用多元认证进行。

4.1.2 身份识别和认证

为识别身份，需要认证客户的身份并在服务提供商的数据中将客户移动设备与其账户进行独一无二的连接经过初步客户身份认证后，应向其发布“秘密”，以便对用户今后与服务提供商的互动进行认证。这项“秘密”，亦称为“移动签名”，作为认证因素之一。简单地说，移动签名是一个独一无二的加密密钥，可用来加密信息，因此，密钥使用的既可提供数据加密，也可对各方进行认证。多元认证的第二个因素可由用户 PIN 或密码确定，从而允许对安装在手机上的应用予以接入。该 PIN 防止对应用的非授权使用。

现有移动支付系统已采用了自身的安全程序，安全要求是由服务提供商及其客户通过协议确定的。显然，电子政务需要一个由国家控制并符合国家有关电子签名法律规定的安全系统。该系统应确保在政府机构和授权用户之间安全传输保密信息，同时提供电子签名。该系统还可用于电子卫生服务和其它需要数据保护的新兴服务。尽管个人移动支付系统可能有其自身的保护手段，但人们不得排除复杂的解决方案，即在一个中心点提供集中化认证。一些服务提供商（特别是金融服务提供商）还在此基础上使用自己的加密和认证程序。因此，对于移动应用，针对不同组密钥使用多项独立数据块是一种合理的做法。图 2 显示了移动和互联网设备的统一认证模型。

虽然存在多种身份识别和认证中心，但他们须使用统一的规则发布统一客户移动身份 – mID。该身份注册在系统中央目录中，以确保将消息适当地传送给客户。客户可能具有多个 mID，但这些身份应与客户的 MSISDN 相捆绑。

服务使能因素提供了技术支持，在整个结构中发挥至关重要的作用。除整合不同接入手段，与服务提供商和认证中心进行互操作外，服务使能因素还为用户提供接入方式（个人计算机和移动终端）应用。

所有身份识别和认证中心必须符合全球移动用户识别码（mID）的统一分配原则和规定。该识别码登记在中央系统目录中以确保向客户的信息传递。

4.1.3 密钥管理

加密可以使用对称和非对称密钥完成，以便对所传输的数据进行加密并创建移动签名。对称加密（标准 3DES、AES）的优势是使用便于在低成本计算设备中实施的算法。对称密钥的生成是一个简单的操作，无需任何特别手段。然而，顾名思义，在用户和服务提供商（提供商的认证中心）之间使用相同密钥可能在用户对所完成的交易提出质疑时产生问题。可以指出的是，移动支付系统在掌握如何创建可靠的交易登录系统处理争议后成功使用了对称密钥加密。

非对称密钥加密使用公共密钥基础设施（PKI）将属于一个人的两个不同密钥关联起来：公众可使用的身份 –“公共”密钥和得到安全存储和防止非授权接入的“私人”密钥（SIM 卡或得到特别保护的智能卡）。密钥之间通过数学交互作用使一个密钥的行动与另一个密钥“关联”，而不披露私人密钥数据。这对于创建电子签名尤其有用，因为私人密钥完成的签字行动完全根据与相关公共密钥（该密钥身份已知）的关系确定私人密钥所有者。PKI 技术的最重要工作一方面是确保私人密钥的“隐私”，另一方面是确定公开和私人密钥之间的关系。这是通过密钥颁布后对注册程序的认真管理以及确认公共密钥身份的认证程序进行的。这些方面分别由所谓“注册”和“认证”机构（如 RA 和 CA）等实体完成。有关移动签名，

其主要功能是根据公民对相关公共密钥的所有权承认私人密钥使用与所注册的公民身份之间的独特关系。

非对称加密方法需要使用更加昂贵的计算设备，但可采用多种互动模式。使用“双密钥”可提供更大的扩展性并进一步便于冲突的解决。这种方式通过简化的行政管理和服务（例如，很多不同的应用和互动方案可得到统一的单一非对称密钥对的支持）可实现更加高效的信任模式。因此，介绍电子签名全球互操作性框架的文件几乎全部侧重于非对称加密方法。

4.1.4 安全

支付系统以及电子政务和电子卫生（包括其移动变异）的最重要要求是安全性。这需要满足国际电联电信标准化部门建议书的规定。电信标准化部门发布了一份题为“电信和信息技术安全[6]”的手册。该手册概括了现有 ITU-T 标准及其在安全电信中的实际应用。ITU-T 的标准虽然作为建议书，但需要遵守。遵守建议书是确保各国电信系统兼容性和一致性的关键。

由于这些系统涉及多个方面，安全可考虑在多个领域内：

a) 终端安全

b) 移动应用安全

c) 移动网络安全

d) 包含请求金融交易的适当个人身份的请求方识别。

在智能电话时代到来之前，运营商对移动电话的移动应用管理相对简单。运营商基本上只是控制哪些应用可以下载到手机及其安全特性。随着智能电话的面世以及自由下载第三方应用的能力的出现，移动应用的管理日趋复杂。今天，几乎无法肯定移动设备上执行的每个应用均有可依赖的来源。因此，移动用户必须面临更多的威胁，如身份盗窃，钓鱼和个人数据的丢失。

设计完善并得到妥善实施的安全方面有利于针对某个网络制定的安全政策的落实并推进安全管理规则的实施。

接入控制安全方面防止对网络资源的非授权使用。接入控制确保只有经授权的个人或设备可以接入网络元素、存储的信息、信息流服务和应用。此外，基于角色的接入控制（RBAC）提供不同接入等级，以保证个人和设备只能接入其得到授权的网络元素、存储的信息和信息流并完成操作。

认证安全方面用来确认通信实体的身份。认证确保参与通信的实体所宣称的身份（如个人、设备、服务或应用）的有效性并确保实体没有伪装或非授权或未经授权而重复前一次通信的企图。

不可否认性安全方面通过提供各种网络相关行动证据（如义务、企图或承诺证据、数据来源证据、所有权证据、资源使用证据）防止个人或实体否认进行了某项有关数据的行动。该方面提供可呈现给第三方并用来证明已发生的某项活动或行动的证据。

数据保密性安全方面防止数据的非授权披露。数据保密性确保数据内容无法得到非授权实体的理解。加密、接入控制清单和文件许可是用来提供数据保密性的方法。

通信安全方面确保信息流仅在经授权的端点之间交流（信息在这些端点之间流动时不被分流或截获）。

数据完整性安全方面确保数据的正确或准确，防止数据受到非授权修改、删除、创建和复制并对这些非授权活动进行提示。

可用性安全方面确保没有因影响网络的事件出现对网元、存储信息、信息流、服务和应用授权接入的拒绝。灾害恢复解决方案包含在此类别中。

隐私安全方面保护可能通过观察网络活动获取的信息。这种信息包括用户访问的网站、用户地理位置和服务提供商网络中的 IP 地址及设备 DNS 名称。

4.1.5 移动技术

迄今为止，术语“移动通信”通常都与第二和第三代 GSM 标准相关。这些移动通信系统使用用于话音和数据传送的不同子系统（使用时分交换和分组交换技术），是移动通信发展中的过渡阶段。下一代网络（NGN）已开始取代现有网络，为用户提供宽带接入并仅使用分组交换信道技术。

NGN 将话音、图像、文字和多媒体信息传输服务作为批量数据传输统一流程的多项应用。因此，今天广泛使用的 SMS 和 MMS 数据传输技术可能导致其它技术的产生。用户可能完全没意识到这些变化。然而，针对移动服务开发的技术解决方案应配合移动通信的演进过程。

今天的移动终端随处可见，但最初，他们在设计上并非针对需要严格认证的系统。因此，不同厂商的终端乃至同一厂商生产的不同型号的终端可能使用不同算法，从而加大了复杂性，而且在一些情况下造成无法创建可履行所有必备系统功能的应用。举例而言，应用应在收到移动支付系统（由商家启动的操作）的信息后自动启动。遗憾的是，并非所有移动终端都可实现。

为统一这类系统的操作，还应对更多的协议进行标准化。国际电联与设备制造商可以完成这项工作。另一项重要的挑战是加密应用的定位和对此应用接入的管理。如“安全”一章所示，为达到最高安全度，这些应用应置于一个特别模块（硬件安全元素）内，保护存储信息不受非授权接入。因此，SIM/UICC 可以成功地作为一个模块，前提是属于移动运营商的 SIM 卡接入的管理权分配问题得到解决。当所有功能由统一实体进行时，问题将迎刃而解，否则则困难重重。为移动终端配备附加硬件安全元素可作为解决有关 SIM 卡共同管理产生问题的解决方案。这一问题可通过嵌入式安全模块或专门安装的防损存储卡得到解决。

移动网数据传送的可用方式五花八门，如 CSD、SMS、USSD、GPRS、EDGE、LTE，各有利弊。例如，SMS 非常可靠且便于实施，但信息长度有限。相反，GPRS 的信息长度无限，但可靠度较差，需要为移动终端进行适当的调整，特别是在漫游时，因此亦非常昂贵。技术的日新月异实现了基于 GPRS 或 GLONASS 系统的智能电话的定位服务。定位主要扩大了移动终端的功能，因此，最近定位服务广泛用于移动装置的应用中（智能电话比例迅速加大）。

4.1.6 研究成果

如附录中欧盟、日本、美国、俄罗斯等国家实施案列所示，各国开发和使用用于移动政务、移动卫生、移动支付、移动学习的移动服务处于不同水平。然而，在今天全球化的世界中，技术创新迅速普及，逐步实现了技术开发水平的融合，从而缩小了发达和发展中国家之间的数字化差距。今天，发达国家已有了功能完善的电子支配系统和移动政务，而一些发展

中国家虽然只是使用简单的 SMS 在医疗机构之间传送数据，业取得了富有成效的结果，使人们更早地接受了早期婴儿诊断（EID）DBS HIV 测试结果（见津巴布韦共和国实施的 MWANA 项目介绍）[17]。这表明，在不久的将来，这种技术差距将缩小。今天多数基于移动设备的先进系统提供可无限扩大的服务。因此，除移动支付和移动银行服务外，基于定位的服务可得到更广泛的应用。此外，欧洲支付委员会 2012 年发表的移动支付白皮书 [18] 指出，移动终端应代表“数字钱包”，为取代多重密码、ID 和商家会员卡提供认证和数字签名。

作为普通钱包，“数字”钱包实际包含所有者的身份数据、所有者可用的支付手段数据，在一些情况下包含所有者的个人数据（照片、文件等）。钱包中还包含 ID 信息、数字签名和证书、登录信息、提取积分和传送地址以及支付手段信息。此外，钱包还可包含其他应用，如奖励积分、票据或差旅文件。在经过统一中心的认证后，人们可进入个人商家账户或社交网，如 Facebook、LinkedIn 等，非常方便使用，无需牢记或安全存储多个账户的多个密码。在近期内，人们可以期待将移动装置作为电子政务和医疗的终端。国际电联和世界卫生组织在 2012 年世界电信展中推出的使用移动装置的举措就是一个充分的例证。因此，基于移动装置的高速系统的发展得益于各项服务使用的安全措施。安全是电子政务、金融服务和电子卫生共同面对的问题，需要通过遵守 ITU-T 有关安全的建议书予以实现。

通过上述建议书，加密已用于认证和传送数据的编码，取代了以往系统使用的一次性密码，大大提高了移动装置的安全性，同时带来使用的便利，使基于移动装置的服务遍地开花。

4.1.7 建议

- 由于移动电话已在市场全面普及并具有高水平的服务，因此成为理想的支付终端和安全通信手段。
- 对所有受到支持的移动电话应用提供方便使用的界面和统一的用户体验至关重要，虽然多数先进的智能电话宣称色彩“绚丽”并具有触屏界面。用户体验依然与尺寸是否够小密切相关。例如，手机的大小有效地限制了在有效的时间内可显示的信息量以及用户输入复杂案文的能力。
- 移动装置是一个“数字钱包”，用来存储有关钱包持有者的身份信息、钱包持有者可用的支付手段以及属于持有者的可选个人信息内容（如图片、文件等）。这有可能包含与 ID 卡、数字签名和证书相关的信息、登录信息、计费和投递地址以及与信息相关的支付手段。此外，装置内可能还包含其他诸如会员、交通或订票应用。
- 客户最好不与具体的 MNO 或银行挂钩，保持目前选择服务提供商的能力。
- 电子对话各方应得到使用至少二元认证的授权，数据的传送应使用加密手段在安全的模式内进行。
- 建议按照 ITU-T Y.2740 建议书采用 4 级或 3 级安全水平。
- 客户应了解系统的安全水平。这一点应规定在参与协议中。用户认证可通过统一认证中心进行。
- 为确保安全性，移动装置必须具有特别移动应用，提供认证或加密。

- 最现实的愿景是实现多种移动应用共存的市场，将多种服务综合在一个移动装置上。
- 移动应用的注册和提供应在安全环境内执行。接入移动应用如能使用现有用户与其服务提供商之间可信赖的关系对用户而言将更加容易。
- 为实现最高安全度，移动应用应放在硬件安全元素上。
- 安全元素的选择对服务模型和攸关各方的角色具有重大影响。迄今为止使用的安全元素（SE）有三类：UICC、嵌入式 SE 和可撤离 SE，如微 SD 卡。
- 服务使能元素提供技术支持和各种接入手段的整合，实现与服务提供商和认证中心的互操作。
- 建议对具有若干独立块的移动应用使用不同套密钥。
- 客户可能有多个客户移动身份 – 与客户 MSISDN 捆绑的 mID。应引入发布注册在系统中央目录中的 mID 的统一规则，确保将信息妥善路由至客户。
- 所有身份识别和认证中心必须符合相同的有关移动用户移动标识符（mID）的位置规则和规定，mID 注册在中央系统目录中以确保消息向客户的传送。
- 移动系统应尽可能使用已广泛部署的技术和基础设施。

4.2 评估电子政务成效及其在韩国（大韩民国）的推广

4.2.1 引言

现今，由于越来越认识到 IT 项目将提高商业流程的效率和透明度，不仅是发达国家，发展中国家也在启动全国范围的大型电子政务系统等许多 IT 项目。但是，如果 IT 项目管理不善，那么将无法实现预期的结果。在更恶劣情况下，可能会浪费政府的预算。因此，在执行项目的过程中，应认真规划项目的绩效管理。

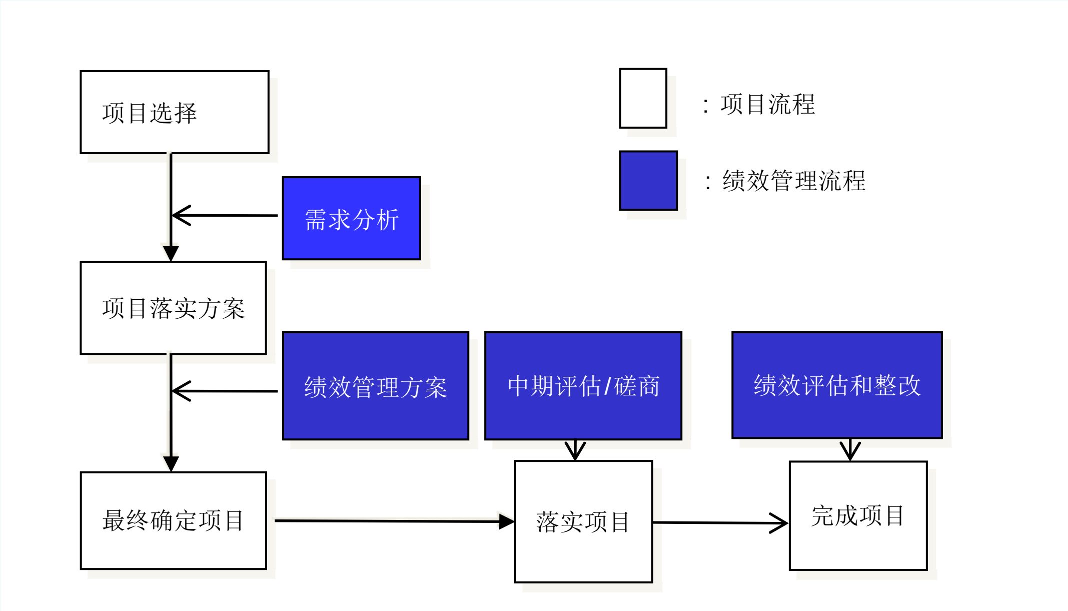
相对于简单评估本身，绩效管理是一种范围更广的手段。通常在项目结束时进行评估，但是绩效管理采用整体分析方法，因此其目标是提供恰当管理项目的能力。在此方面，针对电子政务项目的绩效管理，韩国政府引入了综合手段，向落实电子政务项目的实体提供事先咨询服务和中期评估分析。

后附文件包含我们电子政务项目绩效管理方案以及我们努力向落实电子政务项目的所有实体推广绩效管理做法的更详细信息。

4.2.2 电子政务绩效管理的工作流程

电子政务绩效管理涉及项目落实中项目选择、项目落实和项目评估等整个流程。下图显示了电子政务绩效管理的流程。

图1：电子政务绩效管理的流程



通过需求分析选定新项目，前者包括评估流程的两个阶段，然后确认最终的项目。在落实新项目前，每个部门需要起草其自身的绩效管理方案，说明监控和评估项目的方法，因此该方案应包括项目目标的明确定义并详细描述衡量项目输出和成果的指标。

因此，执行机构须在所起草的绩效管理方案基础上评估项目。在项目的执行过程中，为大型项目（约占整个电子政务项目的 10%）提供了中期评估/咨询服务。这种中期咨询服务不仅提供当前现状的分析，还在需要时提供问题的解决方案。

绩效管理的最后阶段为评估和整改：所有项目按照 S、A、B、C、D 五个类别加以评定。评为 S 的项目将在以后的预算划拨方面获得最优先地位，有时会增加预算（需要的话）。A 类表示项目继续，没有任何更改。

B 类表示在下一阶段进行修改，但 C 类则表示项目需要在根本上进行调整。D 类项目需要变更项目的性质，否则不允许再给予预算支持。

4.2.3 未来方向

韩国在 2009 年引入了电子政务的绩效管理，但是绩效管理正在成为韩国的一个核心，而不是一种可选项，相对于其他类型的项目，电子政务项目需要更加严格的绩效管理。因此，也引入了全面的新项目选择需求分析以及中期评估和咨询。我们认为，将进一步发展和调整绩效管理，以反映电子政务相关项目落实不断变化的环境。

4.3 电子政务框架（eGovFrame）：开放创新的开放平台

4.3.1 概况

多种开发框架的应用引发了诸多问题，如系统维护困难、过于依赖供应商以及系统间缺乏互操作性。为了解决上述问题，韩国政府开发了一套电子政务标准开发框架 – 电子政务框架（eGovFrame）。为实现软件框架 eGovFrame 的统一使用，众多利益攸关方提出了大量意见和问题。大公司唯恐主导市场瓦解，公共组织忧虑能否得到稳定的技术支持，开发者拒绝接受各类新开发工具，政府部门极为关切业务有效性，而中小企业（SME）则担心项目推广只以大公司为主。因此，众多利益攸关方必须就软件框架的标准化事宜达成一致。为了克服上述问题，实现软件框架的统一使用，我们分以下四个阶段实施了开放创新战略：（1）开放源代码，（2）开放流程，（3）开放输出成果和（4）开放生态系统。本文件将对 eGovFrame 及开放创新策略予以详细介绍。

韩国政府开展了很多电子政务项目并实施了大量电子政务应用。这些项目中的很多项目使用了软件框架，因为软件框架是提高生产力和应用开发质量的有效手段。今天，软件框架已成为开发电子政务应用广泛使用的手段，但软件框架也产生了一些问题。为克服这些问题，韩国政府努力实现软件框架 eGovframe 的标准化。然而，很多利益攸关方发表了多种意见并提出了多项问题。为解决这些问题，韩国分四个阶段实施了开放创新战略。根据这些战略，韩国实现了电子政务框架的标准化并建立了 eGovframe 的开放式生态系统。

4.3.2 eGovFrame 背景介绍

韩国一直通过利用包括宽带互联网在内的世界一级的信息通信技术（ICT）积极开展电子政务，将此作为一项重要措施提高政府的竞争优势。在完成电子政务的基础工作之后，韩国政府便开始将开展电子政务作为 21 世纪的一项主要国家议程。自此，电子政务深深植根于韩国政府的方方面面，并取得了显著的成果。相应地，韩国电子政务的工作成效得到了国际社会的广泛认可。韩国的电子政务被联合国等国际组织评选为最佳范例，并有多项电子政务系统引入其它国家。

在实现上述成果过程中，韩国政府一直在开展多项电子政务项目，并开发了大批电子政务应用。在这些项目中，有相当大一部分都采用了软件框架。软件框架是提高应用开发生产率及其质量的有效工具，且目前已经成为开发电子政务应用程序的常用工具。但在另一方面，软件框架也存在一些固有的缺点。

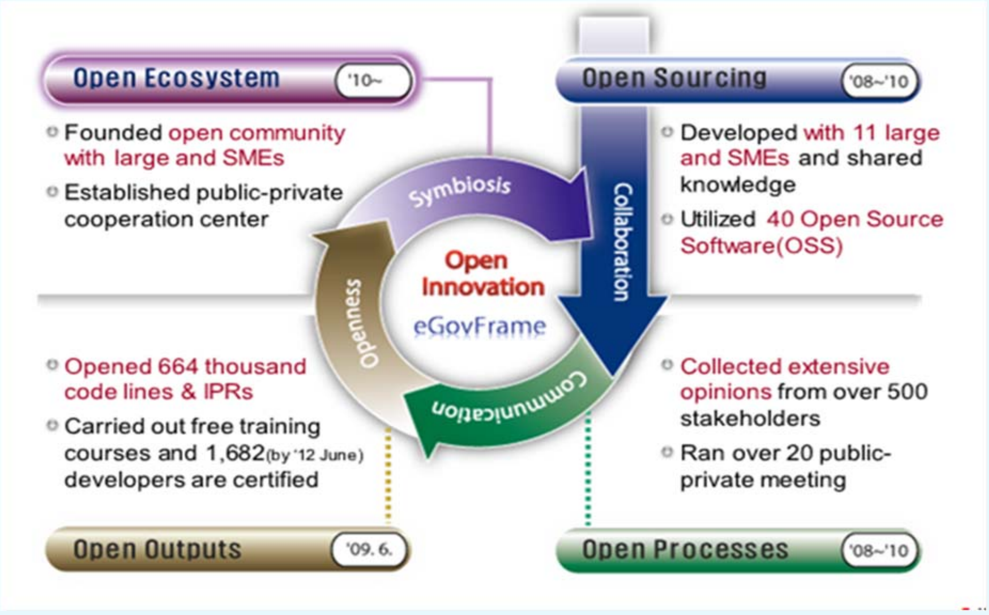
电子政务项目在应用软件框架过程中变得极为依赖信息技术（IT）公司的框架。因此，如果缺乏来自开展原始应用程序的框架提供商的技术支持，应用程序的维护工作将比较困难。在连续进行的项目中，前一个项目所采用的框架将会成为新竞争者的技术障碍，从而形成一个导致软件市场不公平性的恶性循环。同时，对 IT 公司框架的依赖性也产生了诸多问题。首先，一项应用程序的业务逻辑亦取决于某一特定框架。其次，由于每个特定框架的“黑箱”特性，只有框架提供商可以为应用程序提供维护服务，导致只能锁定一家框架提供商。再次，多个框架会导致应用程序设置、吸收、教育和维护方面的冗余活动。

为了克服上述问题，韩国政府开始统一使用一套软件框架 – eGovFrame（电子政务标准框架）。eGovFrame 是一套标准化软件工具，用于开发和运行电子政务应用程序，旨在提高 ICT 投资的效率及电子政务服务的质量。该框架侧重于改善电子政务应用程序的可重复使用性和互操作性，具体措施包括在建立起一套用于开发电子政务软件的标准框架的同时，通过采用开放、中立的软件确保不对 IT 公司过分依赖，并借助多种渠道进行工具共享，从而提高 IT 中小企业（SME）的竞争力。

4.3.3 开放创新战略

为了解决电子政务软件框架标准化引发的问题，我们实施了一项基于开放创新格局的战略，该战略被命名为开放创新战略。电子政务框架的标准化不能仅仅依靠韩国政府单方面的努力。除了政府的努力和推动外，还需要众多利益攸关方的相应知识、参与、经营和反馈。为了满足这些实现电子政务框架统一和应用的必要条件，我们将战略分为 4 个阶段 – 开放源代码、开放流程、开放输出成果和开放生态系统。图 2 展示了开放创新战略的整体结构。

图2：开放创新战略



Open Ecosystem '10~
- Founded open community with large and SMEs
- Established public-private cooperation center

Open Sourcing '08~'10
- Developed with 11 large and SMEs and shared knowledge
- Utilized 40 Open Source Software(OSS)

- Opened 664 thousand code lines & IPRs
- Carried out free training courses and 1,682(by '12 June) developers are certified

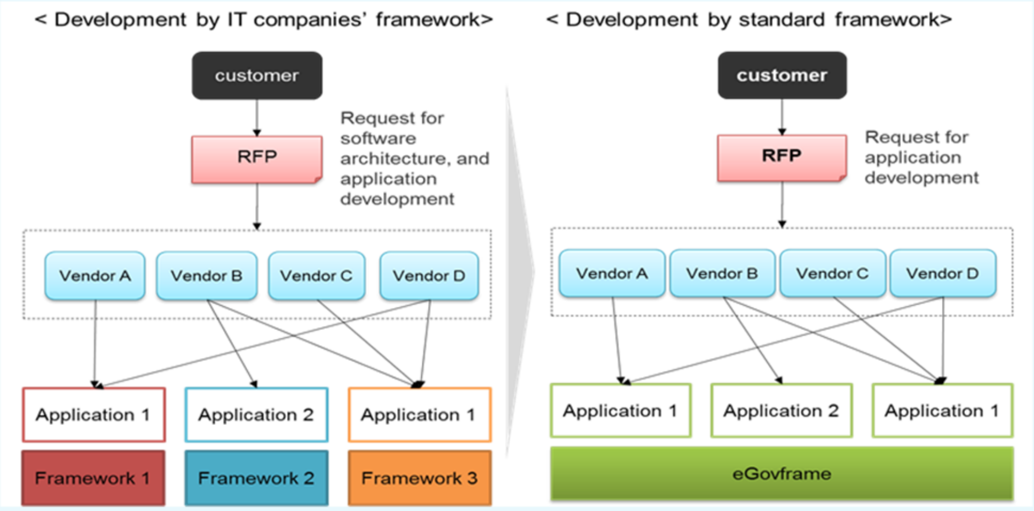
Open Outputs '09. 6.

- Collected extensive opinions from over 500 stakeholders
- Ran over 20 public-private meeting

Open Processes '08~'10

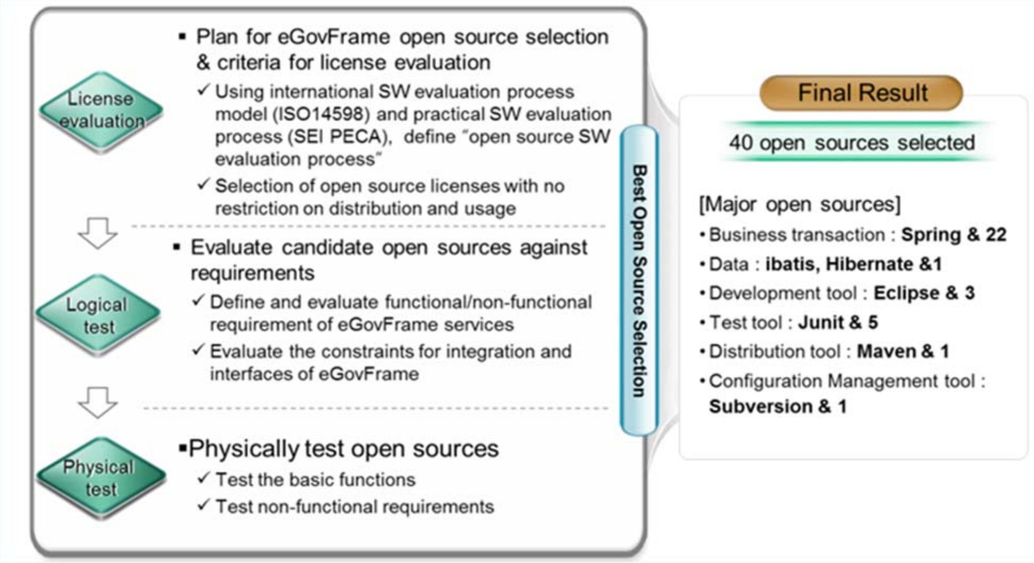
为了统一使用 eGovFrame，我们就五套主要的 IT 公司框架开展了环境和功能性分析，并围绕每家利益攸关方进行调查和深入访问。由此，我们总结得出四个包含十三家服务团体和五十四项服务功能的环境。为了避免各政务系统重复开发相同的功能，我们在 2004 到 2007 年间对一份有关六十七个电子政务项目的 31 114 项功能的分析报告进行了审议。用于提取各组件相同功能的标准可发现重复开发的高度可能性、政务系统的可复用性和标准可采用性。在完成五个提取程序之后，我们共发现了 219 个相同部件。

图3：即将开发完成的eGovFrame图像



为了减弱对主要 IT 公司的依赖性，我们选取了经过验证的知名开放源。我们利用国际软件评估程序模型（ISO 14598）以及实用软件评估程序（SEI PECA），确定了 eGovFrame 的开源软件评估程序。在首轮逻辑测试中，共有一百七十五套开源软件经过评估，评估标准侧重于 eGovFrame 的整合与接口的限制因素。在第二轮物理测试中，我们围绕基础功能和非功能性要求对首轮逻辑测试得出的八十五套开源软件开展评估。经过测试评估，我们选取了四十套开源软件组成 eGovFrame 框架。基于开源的 eGovFrame 框架拥有多方面的优点，既可轻松采用日新月异的技术，又可应用于国外的电子政务应用中。

图4：开放源评估与最终选取



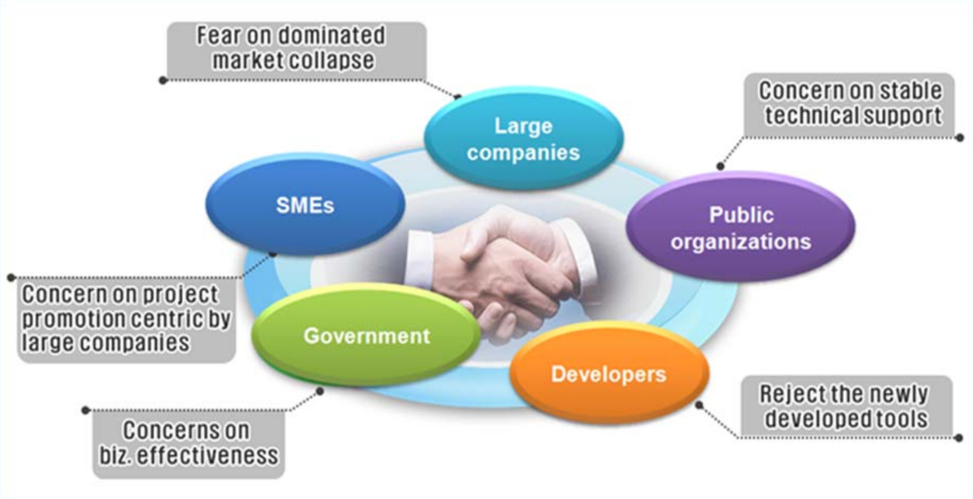
- Plan for eGovFrame open source selection & criteria for license evaluation
  - ✓ Using international SW evaluation process model (ISO14598) and practical SW evaluation process (SEI PECA), define "open source SW evaluation process"
  - ✓ Selection of open source licenses with no restriction on distribution and usage
- Evaluate candidate open sources against requirements
  - ✓ Define and evaluate functional/non-functional requirement of eGovFrame services
  - ✓ Evaluate the constraints for integration and interfaces of eGovFrame
- Physically test open sources
  - ✓ Test the basic functions
  - ✓ Test non-functional requirements

[Major open sources]

- Business transaction : **Spring & 22**
- Data : **ibatis, Hibernate &1**
- Development tool : **Eclipse & 3**
- Test tool : **Junit & 5**
- Distribution tool : **Maven & 1**
- Configuration Management tool : **Subversion & 1**

开发流程完全向公众开放，成功创建起可面向 500 多家利益攸关方收集广泛意见的环境。除此之外，我们举行了 20 次公共-私营会议，促使众多利益攸关方达成相互谅解和一致意见。

图5：eGovFrame的众多利益攸关方


Fear on dominated market collapse
Large companies
Concern on stable technical support
SMEs
Public organizations
Concern on project promotion centric by large companies
Government
Developers
Reject the newly developed tools
Concerns on biz. effectiveness

开放输出成果

包括源代码、实体关系（ER）图在内的所有输出成果均向公众开放，可从 eGovFrame 网站（www.egovframe.go.kr）自由获得，从而创建了一个有利环境，可鼓励开发者、提供商及政府官员主动参与实施过程。此外，我们还开展了免费培训课程，共计 1,236 名开发者获得认证。

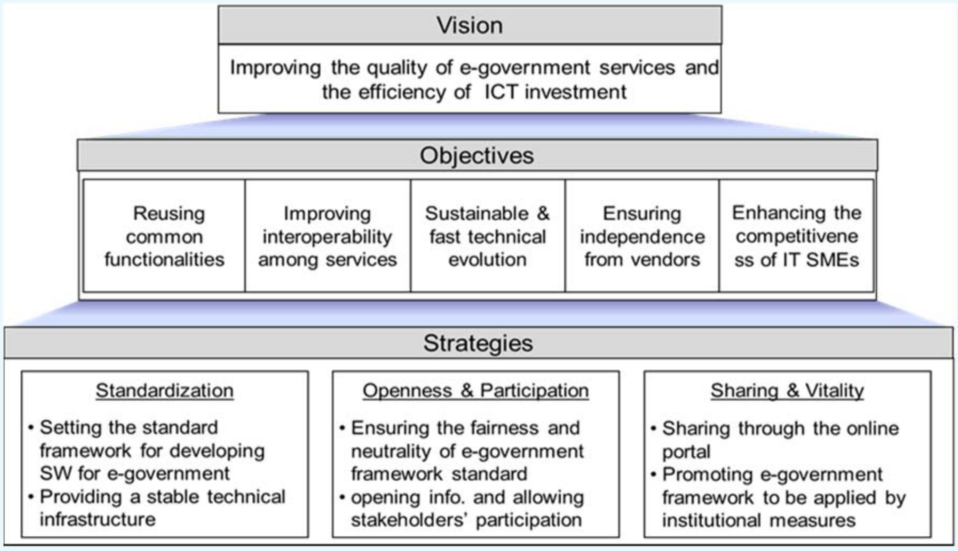
开放生态系统

我们与大型及中小企业共同成立了一个开放社区，并建立起公共-私营合作中心，成为推动 eGovFrame 全球化、提供可靠的技术支持和实现持续进步的重点设施。该开放社区以及按季度举行的专家会议和公共-私营合作伙伴开放论坛将对 eGovFrame 做出持续的改进和提高。在上述努力基础上，我们成功建立了 eGovFrame 的开放生态系统。

4.3.4 eGovFrame 的变化和好处

该项目旨在提供一套标准化软件工具 – eGovFrame，用于开发和运行电子政务应用程序，进而提高 ICT 投资的效率及电子政务服务的质量。该框架侧重于改善电子政务应用程序的可重复使用性和互操作性，具体措施包括在建立起一套用于开发电子政务软件的标准框架的同时，通过采用开放、中立的软件确保不对 IT 公司过分依赖，并借助多种渠道进行工具共享，从而提高 IT 中小企业的竞争力。

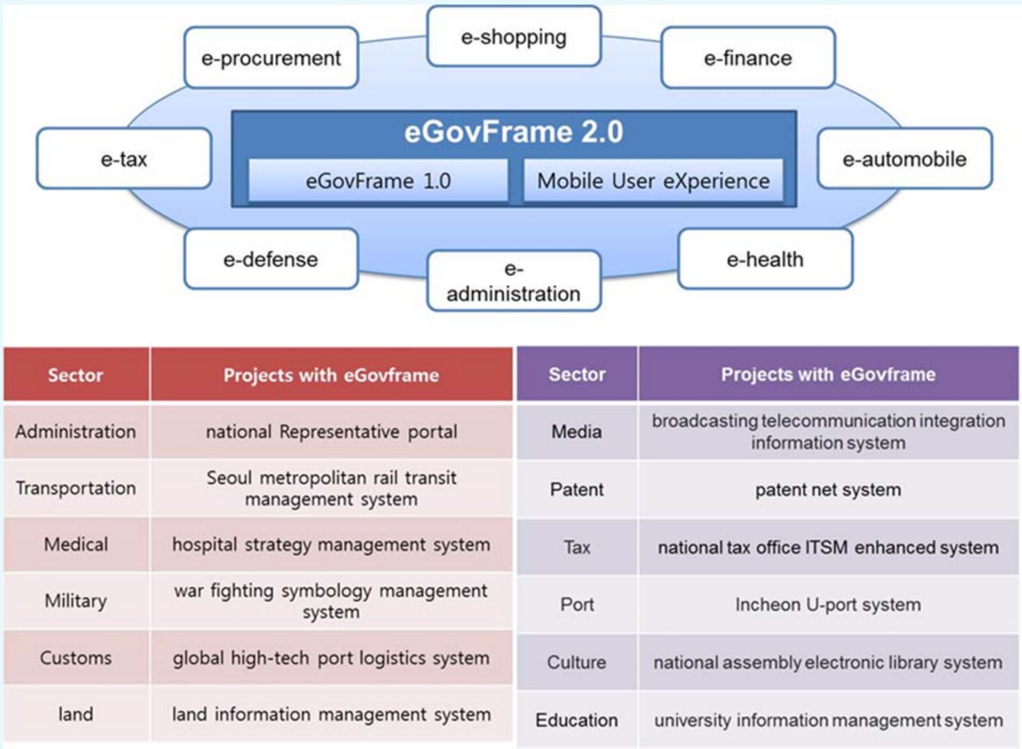
图6：eGovframe的愿景与战略


Vision
Improving the quality of e-government services and the efficiency of ICT investment
Objectives
Reusing common functionalities
Improving interoperability among services
Sustainable & fast technical evolution
Ensuring independence from vendors
Enhancing the competitiveness of IT SMEs
Strategies
Standardization
• Setting the standard framework for developing SW for e-government
• Providing a stable technical infrastructure
Openness & Participation
• Ensuring the fairness and neutrality of e-government framework standard
• opening info. and allowing stakeholders' participation
Sharing & Vitality
• Sharing through the online portal
• Promoting e-government framework to be applied by institutional measures

eGovFrame 源自经过验证的知名开源软件，所有源代码均通过在线门户网站向每位利益攸关方开放。该框架包含四个软件环境：应用程序的运行时环境、应用开发者的开发环境、框架管理者的管理环境和应用运营者的运营环境。

在应用开发阶段，应用 eGovFrame 框架可以节省大约百分之三十的开发成本和工作。这意味着 eGovFrame 可以在某一具体类型的基础设施使用多种应用程序的过程中发挥“缓冲”作用，也可以作为开发相同功能的共同基础。于近期研发得出的 eGovFrame 2.0 版本已在去年十月份连同移动用户体验部件共同推出，具体情况如图 7 所示。

图7：eGovFrame 2.0版本



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 移动 eGovFrame 的扩展和未来

伴随着智能手机、平板电脑等高级移动设备的广泛使用，公共和私营领域的移动服务需求正在不断增长。为了满足新的需求，并提高移动服务的质量和效率，加入了 HTML 5 和新用户界面等特征的 eGovFrame 2.0 版本于 2011 年底推出。该版本可与至少三类移动浏览器（谷歌 Chrome 浏览器、苹果 Safari 浏览器和火狐浏览器）兼容。目前，大韩民国已经利用 eGovFrame 2.0 版开发了大量移动电子政务服务，具体内容如图 7 所示。

为了充分利用移动设备的诸多功能，例如震动、相机控制、指南针等，eGovFrame 2.0 版将引入部分新组件，支持创建移动应用程序。这一举动有望鼓励软件开发者开发出大量移动网络服务及移动应用程序。

4.3.6 其它国家的机遇

在本国取得的有益经验基础上，大韩民国政府还在为国际范围内更大规模的信息化进程做出积极贡献。对于那些希望解决某些供应商公司的垄断经营问题或希望强化开源软件作用的国家而言，韩国推出的标准化框架令他们非常感兴趣。如表 1 所示，eGovFrame 框架已经在多个国家应用实施。

表1：采用了eGovFrame的国家

国家	项目	相关机构	项目时间
保加利亚	索非亚大学行政管理系统	索非亚大学	11/2011~10/2012
厄瓜多尔	单一窗口系统	厄瓜多尔海关	01/2011~03/2013
越南	投资升级和扩大供水系统项目	资源环境部（MONRE）	09/2010~12/2013
蒙古	国家注册系统	国家注册总局	07/2011~06/2012
突尼斯	电子采购系统	国家公共采购监督局	11/2011~11/2012

其他发展中国家对学习韩国在电子政务领域特别是 eGovFrame 方面的经验抱有强烈需求。对此，韩国政府通过多种渠道帮助其他国家改进其电子政务服务，其中还包括与国际组织开展积极合作。为了鼓励其他国家采用 eGovFrame 框架，英文版的框架源代码可以从 eGovFrame 的门户网站（http://eng.egovframe.go.kr）自由下载，同时，韩国政府还提供在线技术支持。除此之外，韩国政府还通过韩国 IT 学习（KoIL）计划和信息技术合作中心（ITCC，该中心旨在推进大韩民国和其他合作伙伴国家在 IT 领域的相互合作）提供 eGovFrame 教育课程。

5 发展中国家受益的应用范围

5.1 确定应用范围的导则

在当今技术驱动的世界中，ICT 迅速成为政府现代化项目的核心。这不仅体现在发达国家。在发展中国家，新技术对变革政府运作的方式所具有的潜力越来越普遍得到认识。当政府使用 ICT（电子政务）已成为政府开展工作不可分割的一部分时，我们有必要制定指导原则，以确定应用领域并为发展中国家的利益确定轻重缓急。制定指导原则应强调以下问题：

1) 每个发展中国家的独特性（经济和社会条件）；

2) 每个国家的需求和当前能力；

3) 对发展中国家价值最大的应用重点；

4) 考虑将移动和无线平台用于政府与公民之间的活动，以获取政府信息并提供公共服务。

电子政务开发早期采用的应用可根据以下原则予以选择：

- 项目与公民日常生活关系最为密切，使他们感觉到从所引入的电子服务中获得的最大利益；
- 项目主要实现跨组织边界的业务流程的整合；
- 扩大政府各机构分享信息的可能，以消除在记录收集和管理方面的重复工作；
- 促进 ICT 的使用以便通过业务流程重组（BPR）的成熟方式精简行政流程。

按照上述原则确定应用领域的过程中，我们需要考虑到开展电子政务所缺乏的国家资源，特别是发展中国家，以及通过电子政务实施推动各国发展的迫切性。为满足需求，必须制定战略，有所选择并集中精力，一些电子政务项目是按原则“挑选出来的”， 将有限的资源集中在挑选的项目上。

5.2 基础设施

- 更新电子政务和安全的法律体系；
- 培训 ICT 人力并重组 ICT 管理方式；
- 电子认证系统。

5.3 G2G

- 将电子文件系统与政府工作系统（如公共采购系统、本地政府系统、税收系统）相连接；
- 本地政府系统；
- 公共金融管理系统（国家和本地）；
- 信息共享系统。

5.4 G2C 和 G2B

落实用户友好服务的经验教训、公共服务的综合化和个性化、采用多种渠道、在用户需求基础上改进服务质量、电子政务服务的宣传、保护个人数据以及电子政务业务的安全

- 用于公民公共服务提供的门户系统；
- 互联网税收系统；
- 政府电子采购系统。

6 确保电子政务活动取得成功的因素

6.1 总统的领导（政治支持）

- 国家 IT 项目，尤其是电子政务项目通常涉及多个机构。这意味着，他们之间在很多问题上可能存在分歧。正常制定过程可能因部委之间的官僚性竞争而常常被终止。
- 在网络部署和应用系统实施过程中实现相关机构之间的协调可能是电子政务举措实施中面临的最大挑战。各机构具有的水平和面临的风险不同，要考虑的激励机制也不同。因此用一种方案满足各机构的需求令人质疑。为缓解该问题，部委间需成立高层指导委员会，以解决政府机构之间的争议。委员会活动的有效性取决于总统的支持，这是活动协调的真正力量所在。
- IT 项目需要大量投资，而投资回报价值并非立等显现，因为 IT 举措需要长时间产生实际价值。此外，由于 IT 项目并非显而易见，很难将 IT 项目的成就显示给负责签署为政府项目分配国家资源的人们。

- 虽然很多人认识到使用 IT 的潜力及其对效率和能力的影响，但负责政府预算分配的人们无法看到足够的现金证据以便对 IT 的好处深信不疑。总统通过认识到 IT 潜力所发挥的领导作用对克服这种困境具有重要影响。例如，韩国总统决定打破正常预算程序，专门为 1987 年 IT 项目的使用划拨大笔专项资金。体现了韩国总统对 IT 举措早期发展所发挥的强有力的领导作用。

6.2 有关电子政务服务的供需平衡

- 通常，国家 IT 总体规划配备优先发展政策，主要侧重于供应一方。政府在开发首先提供给公民的应用服务中发挥必要的领导作用以便带动需求。但是，我们应注意到有关需求方的问题，如哪类服务值得为电子政务项目进行大笔投入。该问题的提出是因为，我们可能创建了一个昂贵的解决方案，但是没有相应的问题。

- 重视供应方的想法并不排除考虑某项电子政务服务潜在需求的重要性。一种困境是，IT 项目似乎产生了需求但无法在供应之前预测需求的大小。重要的是，IT 战略应与如何在 IT 系统实施后通过培训该系统的潜在用户使他们充分利用 IT 的实际优势带动需求。

- 为平衡有关电子政务的供需，潜在服务的方方面面均应考虑在内。例如，审核政府和公民之间脱机交易是我们确定在电子举措中提供哪些服务时所要考虑的需求问题。这将弥补需求预测的不足，因为我们可以想象，脱机交易越多，在线服务需求就越大。

6.3 深入了解电子政务

- 电子政务的重点是在“政府”，而不是“电子”。电子政务的核心是变革公共行政管理，以便在 IT 的辅助下实现内部和外部的创新。电子政务问题应置于国家公共管理改革和良治举措范畴内。政府创新问题自 IT 应用引入公共行政早期一直作为追崇的目标，对现实世界中政府工作流程的实际影响却异常缓慢。

- 与其侧重于引入 IT，政府应决定、指导并控制行政程序的变革，使 IT 为流程的重组充分发挥潜力。

- 电子政务预期将引发政府内部业务和公民服务的深入而全面的变革。变革将基于 IT 的性质，特别是互联网，使政府得以综合开展业务。通过信息在政府组织各部门之间的普遍共享实现共同职能和相同服务的整合。多数电子政务项目经过了业务流程重组（BPR），然后才进行实际的实施。BPR 通常经过若干步骤，如分析业务流程以便实现各组织目标，取消多余流程，精简工作方式并简化复杂程序。

- 取消重复工作或精简业务流程意味着削减工作机会，从而招致利益攸关方的反对。那些习惯于传统工作方式的人们没有顺应变革的积极性。我们需为政府雇员制定激励机制并为在某一程序中相关的各政府机构之间的协调搭建结构。激励机制包括按工人意愿对其进行再培训和再安排。更具责任心和有效的政府将取消不必要的程序，简化复杂程序并在削减的情况下统一程序。

6.4 鼓励公民参与

- 公民对政府制定政策程序的参与愿望随着政府和公民之间互动的机遇的增加迅速提高。这部分得益于民主进程的压力以及方便人们访问各政府组织的互联网的广泛使用。我们应注意技术如何使每个人得到倾听而不被遗忘在大众辩论中。举例而言，政府应对个人意见做出适当响应 。

- 成功的在线参与需要公民尽可能了解公众问题信息，而政府官员应了解互联网为公民参与政策制定的机会和限制。

6.5 信息资源管理（IRM）创新

电子政务项目将政府各部门的 IT 资源积累起来，我们需要确定这些资源的管理方法，从而避免 IT 财产的浪费，IRM 需要各政府组织相互协作从而使 IT 资源尽可能在最大程度上得到分享和集成。

IRM 方法，如企业机构（EA）将目前和所期待的业务流程之间的关系以及 IT 资源记录在案，从而确保信息共享的安全和整个组织内的流程整合。EA 还能消除政府各机构 IT 资源的重复采购，从而提高投资的有效性。

EA 活动侧重于如何将信息共享和 IT 投资的改进通过指导原则和参考模式转化为现实。参考模式旨在促进通用的身份识别、使用和数据的适当共享、业务流程、SW 应用以及 SW 机器。指导原则针对信息资源的有效管理，以在业务重点和技术实施变化的情况下最不可能变革的元素为基础。

6.6 隐私保护和系统安全

- 随着各机构维护的信息在电子政务举措发展的过程中得到相关各方的共享，电子政务潜在用户担心个人信息得到不当使用或过量使用。个人数据的保护和为加速政府服务电子应用而进行的信息共享之间有必要进行权衡，促进相关机构的信息共享与开发保护隐私的手段之间的平衡至关重要。

- 随着电子政务的成熟，我们将体验到 IT 应用的不良影响，因此应加强隐私保护措施，在两个极端之间达成平衡。电子政务系统永远面临政府外的攻击，有时也有来自政府内部的攻击。因此，应为防止黑客、造假和欺诈采取各种技术、法律和机构性措施。

6.7 接受电子服务的战略

- 尽管电子服务广为提供，公民对这些服务的采用和业务是另一个问题。公民不希望接受电子政务系统，除非他们真正感觉到电子服务的优势。通常，在电子政务系统落实的初期，电子服务的使用率较低。资金投入的价值没有完全体现出来，导致就电子政务举措是否应进展下去开展强烈辩论。

- 政府工作的互联网应用应得到监督，以便了解如何更新，使人们得以实际感受到这些应用的方便性。接入渠道应便于接入，超级链接数量较少，无法登录一般公民所需要的政府信息和服务的正确网址。

- 与其关注所有应用，不如将注意力集中在重要的应用之上，使人们与政府进行真正的互动。在我们选择所更新的电子政务应用时，有必要选择公民需求量最大的服务，从而使人们感受到系统带来的好处。

7 鼓励电子政务活动和确定发展中国家电子政务应用领域的指导原则

7.1 范围

这些指导原则涉及有关鼓励发展中国家电子政务活动和确定电子政务领域的问题。

7.2 指导原则的目标

这些指导原则旨在发展中国家了解为取得电子政务活动的成功需考虑的因素以及为了发展中国家的利益应确定的电子政务的领域。

指导原则提供了：

– 为确定有利于发展中国家的电子政务应用领域的指导。各国条件不同，因此需要不同的电子政务应用领域；

– 我们应考虑到的因素，从而使针对发展中国家的电子政务举措取得成功。

7.3 为了发展中国家利益确定应用领域指导原则

电子政务中有很多应用领域，因为几乎所有政府工作可以通过实施信息通信技术完成。

在确定发展中国家的应用领域时，我们应研究以下因素：

– 每个发展中国家的独特性（经济和社会条件）；

– 每个国家的需求和当前能力；

– 对发展中国家价值最大的应用重点；

– 考虑将移动和无线平台用于政府与公民之间的活动，以获取政府信息并提供公共服务；

– 形成组织和行政简化以及政府部门间进行协作的战略和机制，如电子政务术语中的 G2G 领域；

– 落实用户友好服务的经验教训、公共服务的综合化和个性化、采用多种渠道、在用户需求基础上改进服务质量、电子政务服务的宣传、保护个人数据以及电子政务业务的安全，如 G2C 和 G2B。

7.4 确保电子政务活动取得进展的指导原则

为确保电子政务活动取得适当进展，发展中国家应能营造有利于有效落实电子政务举措的环境。

一些成功的因素是基于各国先进的电子政务系统经验确定的。这些因素应在实施电子政务系统中得到考虑：

– 有效协调和强有力的政治领导：实现相关机构在网络部署过程和应用系统实施过程中的协调可能是电子政务举措面临的最大挑战；

– 平衡电子政务服务的供需：典型的国家 ICT 总体规划一般具备优先发展政策，侧重于供应方。政府在开发首先提供给公民的应用服务中发挥必要的领导作用，以便带动需求。但是，我们应注意到有关需求方的问题，如哪类服务值得为电子政务项目进行大笔投入。该问题的提出时因为，我们可能创建了一个昂贵的解决方案，但是没有相应的问题。

– 明确和准确理解电子政务概念：电子政务的重点是在“政府”，而不是“电子”。电子政务的核心是变革公共行政管理，以便在 IT 的辅助下实现内部和外部的创新。电子政务问题应置于国家公共管理改革和良治举措范畴内。政府创新问题自 IT 应用引入公共行政早期一直作为追崇的目标，对现实世界中政府工作流程的实际影响却异常缓慢。

– 鼓励公民参与：公民对政府制定政策程序的参与愿望随着政府和公民之间互动机遇的增加迅速提高。这部分得益于民主进程的压力以及方便人们访问各政府组织的互联网的广泛使用。我们应注意技术如何使每个人得到倾听而不被遗忘在大众辩论中。举例而言，政府应对个人意见做出适当响应。

– 有效监督和评估以及适当的反馈系统：电子政务项目的良好开端不能说明成功。最重要的是完成、业绩和结果。在努力衡量 ICT 投资的好处的同时，应注意监督和评估电子政务举措，从而了解用户的需求以及他们对电子服务的态度。根据这些测量元素评估系统的结果应纳入反馈机制。

– 创新和有效 IRM（信息资源管理）：由于电子政务项目将政府各个部门的 ICT 资源累积起来，我们需要制定一种管理方法以避免 ICT 资产的浪费。IRM 需要每个政府组织相互合作从而在最大程度上分享并整合 ICT 资源。

– 保护个人信息：随着各机构维护的信息在电子政务举措发展的过程中得到相关各方的共享，电子政务潜在用户担心个人信息得到不当使用或过量使用。个人数据的保护和为加速政府业务电子应用而进行的信息共享之间有必要进行权衡，促进相关机构的信息共享以及开发保护隐私的手段之间的平衡至关重要。

– 让公民接受电子政务服务的战略：尽管电子服务广为提供，公民和企业对这些服务的采用是另一个问题。公民不希望接受电子政务系统，除非他们真正感觉到电子服务的优势。通常，在电子政务系统落实的初期，电子服务的使用率较低。资金投入的价值没有完全体现出来，导致就电子政务举措是否应进展下去开展强烈辩论。

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**

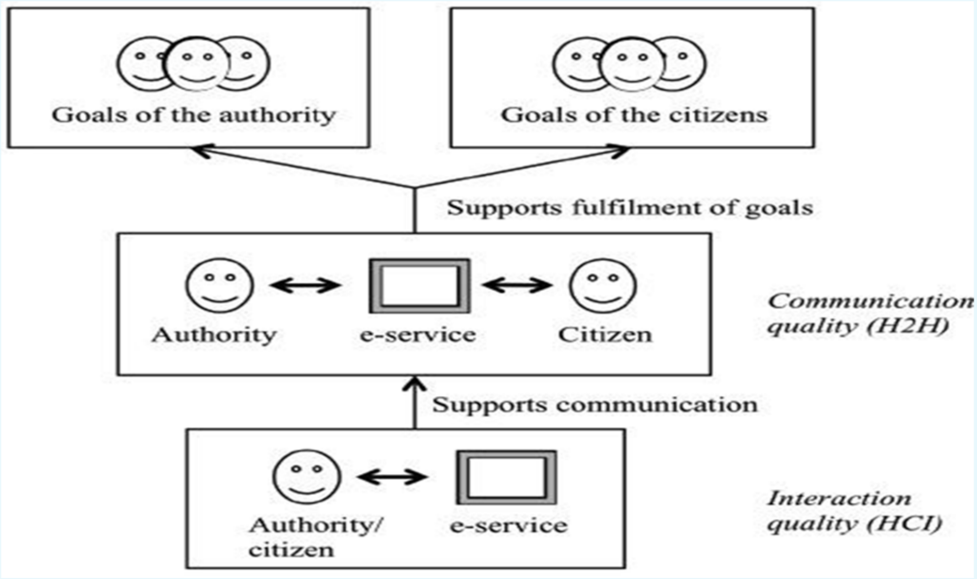
Operators at service

- 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	<u>UN Public Service Award</u> 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	<u>Best Case for Effects on the Private Sector</u> The OECD reported that Korea's e-Procurement contributed towards the dissemination of IT in the private sector, and reached the level of "no further action required"	April 2004

Table 6: Global recognition for KONEPS

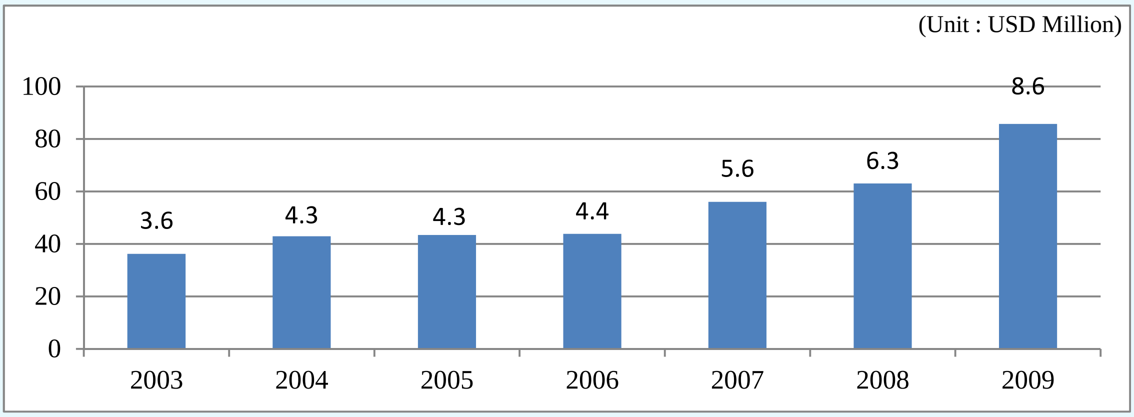
Awarding Organization	Award	Date
UN	Best Practice Model in e-Procurement KONEPS was selected as one of the best 23 practices in the world in the UN Global E-government Readiness Report 2004	November 2004
UN	KONEPS process reflected in UN/CEFACT standards KONEPS process was reflected in UN/CEFACT standards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

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

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

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

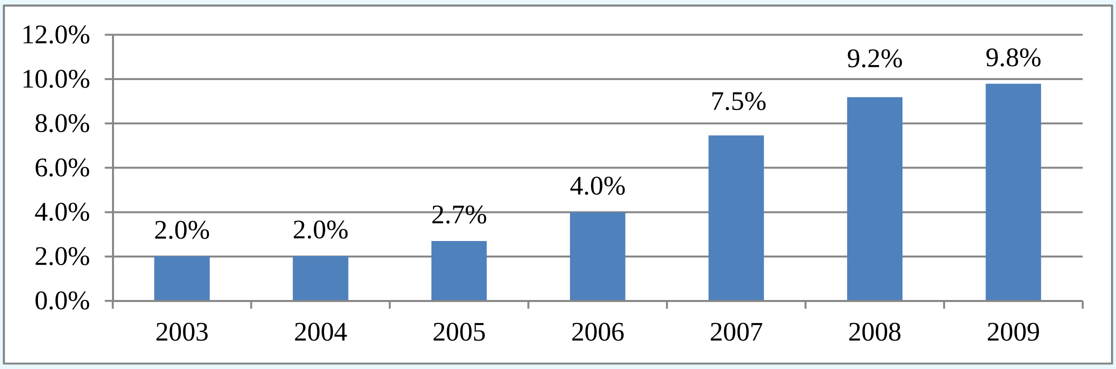
Figure 1: Transactions via KONEPS



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

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

Figure 2: Use ratio of e-Contracting



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

5) Challenges and success factors

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

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

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

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

6) Next steps

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

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

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

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

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

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

1) Background

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

2) Development of e-Government infrastructure

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

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

3) Legal framework

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

4) e-Government framework

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

a) Citizen-centric

b) Accessibility and choice

c) Trust, confidence and security

d) Better governance

e) Collaboration and integrity, and

f) Accountability

5) Public e-Government initiatives

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

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

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

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

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

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

6) Private e-Government Initiatives

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

a) Payment of utility bills using mobile phones

b) Money transfers using mobile phones

c) Payment of school fees using mobile phones

d) Checking of commodity prices using mobile phones

e) E-banking and mobile banking

7) Future envisaged applications

a) e-Procurement

b) e-Document sharing in government

c) Electronic passport processing

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

e) e-Education between urban and rural areas

8) Challenges

f) Cyber crime and cyber terrorism

g) Undefined cross-border jurisdiction for cyber litigation

h) Reliance on imported hardware and software

i) Reliance on foreign funding

j) Un-harmonised ICT Policies and Strategies

k) Inadequate Infrastructure

l) Adverse cultural beliefs and languages

m) Inadequate funding for ICT Projects

n) Inadequate human resources

o) Inadequate Public Private Partnerships (PPPs) frameworks

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

1) Introduction

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

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

2) Uganda's universal access policy framework

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

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

a. Objective

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

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

b. Broadband policy implementation

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

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

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

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

3) Expected benefits

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

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

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

4) Conclusions

Internet penetration, access and usage in Uganda, is still very low and is estimated at (5%) users of the total population. This is also largely confined to urban commercial centres owing to commercial considerations by the private service providers. Although Uganda's previous policy had supported the installation of Internet points of presence in all the underserved districts, the internet bandwidth speeds and quality of service issues (outages) has been of major concern by the end users.

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

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

1) Country overview

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

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

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

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

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

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

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

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

2) Background of e-government initiatives

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

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

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

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

a. Analysis of the existing Governmental Information Systems and Databases

Nowadays, there is a satisfactory level of computerization within the public administration bodies of the Kyrgyz Republic and especially in the central government agencies. In most of the ministries that operate with huge information data there are special dedicated servers to host databases, e-mail systems, Internet access and other services or even departments responsible for data processing and management. Many ministries and government administrations are developing their own local networks and information systems with access to Internet. As a result, there are many different types of information systems, databases, types of data, telecommunication infrastructure used, etc. that may block or hamper the future opportunities for the inter-agency information exchange. Some of these systems are very old and are very difficult to maintain and develop further. Even within the institutions there are different types of technologies and data types that are making the future integration even more complicated. That is why the process of integration of state computer data and systems is very timely and should not be further procrastinated.

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

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

c. Overview of the legal framework

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

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

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

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

3) Objectives and strategies

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

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

Kyrgyzstan has already recognized the importance of providing access to modern technologies and services for all citizens and businesses. The E-Government and E-Services will provide the opportunities to the state administration to use information technologies for providing better services to citizens, businesses, and other actors of the governance. As a result, the administrative environment in the country will be improved in several key directions:

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

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

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

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

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

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

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

Component A: Coordination of the E-Government implementation process

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

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

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

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

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

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

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

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

Component B: E-Government architecture and standardization

CCICT will provide support to the development of the:

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

- back-office inter-exchange gateway/s and mechanisms for interoperability between the government organizations;
- mechanisms for introduction of e-services and support for their implementation;

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

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

Component C: Creation of the Population Register

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

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

4) Activities implemented

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

- "Transparent budget" (http://budget.okmot.kg) - an automatic system for providing data on revenues and expenditures of the central and local budgets. It is for the first time in the country's history the ordinary citizens and legal entities have free access to the detailed data on implementation of the state budget. The presented data consist of information detailed from the level of individual recipients to the government agencies and the regions. The data is updated on-line through the electronic interconnection with Central Treasure Data Base;
- State e-procurement (http://zakupki.okmot.kg) – an automatic system for state procurements, including on-line registration, bid participation and other related information and actions
- On-line economic mapping (http://map.okmot.kg) –an electronic map of the Kyrgyz Republic, visualizing all socio-economic data for each geographical location of the country;

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

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

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

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

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

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

a. Local self-governance area

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

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

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

b. Support to election processes (2011-2012)

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

Developed software platform with user generated content allows for the use of mobile phones to report and e-map incidents of violence via SMS (to short number 4414), e-mail or web. During the pre- and after election period about 5000 SMS were received, 2917 from them were processed and data uploaded and mapped.

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

c. Support to State Registration Service (SRS)

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

5) Changes and outcomes achieved

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

6) Challenges and success factors

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

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

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

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

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

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

Success factors are the following:

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

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

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

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

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

7) Lessons learned and next steps

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

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

1) Introduction

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

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

2) Overview

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

Based on such program, MIC conducted the "Project Promoting Cooperative Business Administration Systems (Verification of Ways of Improving User-Friendliness for Mobile Phones as Means of Access)" in 2011, based on a survey and research results from the "research and study of the diversification of means of access to electronic administrative services, etc. (research and study of technology for mobile phones to access electronic administrative services, etc.)" in 2009.

3) Objectives and strategy

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

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

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

4) Implementation

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

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

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

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

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

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

5) Outcomes

The outcomes achieved in response to such issues are below.

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

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

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

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

Examples of the utilization image of mobile access systems are: (1) writing ID information for certificates to Android terminal-tamper resistant devices, (2) applying for a certificate with an Android terminal online, (3) holding an Android terminal over the ministerial kiosk terminal (multi copy machine) installed at convenience stores and administrative bodies to receive a printed certificate.&#12288; 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 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 &#8213; GSB will provide integration platform and access to shared government services, like shared data, security, payment services, and notification engine. Later phases of the GSB will provide advance services, like service orchestration, registry and e-Forms integration

Case 11: MWANA (Zambia)

1) Introduction

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

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

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

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

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

2) Country overview

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

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

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

3) Objectives and strategies

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

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

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

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

4) Activities implemented

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

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

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

d. Scaling the project nationally between 2011and 2015.

5) Technologies and solutions deployed

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

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

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

6) Changes and outcomes achieved

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

7) Challenges and success factors

a. Challenges

- Ownership of the project prior to initiation, and coordination among the partners
- Sustainability of the project after scale up and when cooperating partners hands over the project
- Lack of investment in research and development in ICT

- Digital gap between the Urban and the rural areas
- Socio-economic disparities

b. Success Factors

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

8) Lessons learned and next steps

a. Government leadership

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

b. Locally sourcing

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

c. Cost control

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

d. Co-creation

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

e. Next steps

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

Case 12: eGovernment Service in Montenegro

1) Introduction

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

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

2) Country overview

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

3) Objectives and strategies

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

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

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

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

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

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

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

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

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

Analysis of eGovernment development

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

EU cooperation

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

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

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

4) Technologies and solutions deployed

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

eGovernment Portal

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

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

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

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

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

Electronic Document Management System – eDMS

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

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

5) Lessons learned and next steps

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

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

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

- Cooperation between public administration institutions;
- Exchange of information in order to fulfil legal conditions, or political obligations;
- Exchange and re-using of information to increase administrative efficiency and reduce administrative burdens on citizens and businesses;

and leads to:

- Better provision of public services to citizens and businesses on the principle of “one-stop shop” (one-stop government)
- Reducing costs for public administrations, businesses and citizens through the efficient and effective provision of public services.

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

1) Introduction

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

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

2) Goal and objectives

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

Main objectives of the National program are:

- ICT infrastructure development with advance capabilities required to satisfy growing needs of citizens, business and state. Creation of environment for e-services implementation, development of e-government resources and providing universal access to such services;
- creation and development of state system of e-services;
- improving quality of health care services;
- improving quality of social and employment services;
- e-learning development and capacity building;
- e-commerce promotion in order to faster economic development;
- increasing government, business and civil society online presence;
- security systems development in order to provide safe ITC usage;
- providing appropriate conditions for IT-industry growth.

3) Subprograms

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

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

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

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

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

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

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

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

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

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

4) E-government subprogram

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

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

Subprogram uses the following KPIs to evaluate its progress:

- UN e-government readiness index;
- Percentage of organizations using digital signature;
- Percentage of organizations using Internet to perform information exchange with Government;
- Percentage of information systems, integrated into unified e-government system;
- Percentage of state authorities using outsourced professional services of information systems support and maintenance.

5) Challenges

- Informatization processes are still fragmented, and there is lack of proper coordination between state authorities;
- There are not enough e-services provided for citizens, services are decentralized. Exceptions are banks and cadastral agencies;
- Digital signature is not widely adopted and is not in demand. It needs to be improved;
- There is lack of process coordinator, who has enough experience and credentials to link involved authorities into singe productive team.

6) Lessons learned

- Changes should be overall, fearless but with prior active consulting with civil society and business;
- Changes must be implemented step by step. We should use positive experience from previous changes in future ones;
- Business likes changes and generally supports them;
- E-government implementation should be fully transparent and must be based on multi-stakeholder approach;
- Processes should be simplified prior to automation;
- Sometimes we should be able to implement changes one-sided instead of spending unlimited amount of time searching for mutual understanding.

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

Introduction

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

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

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

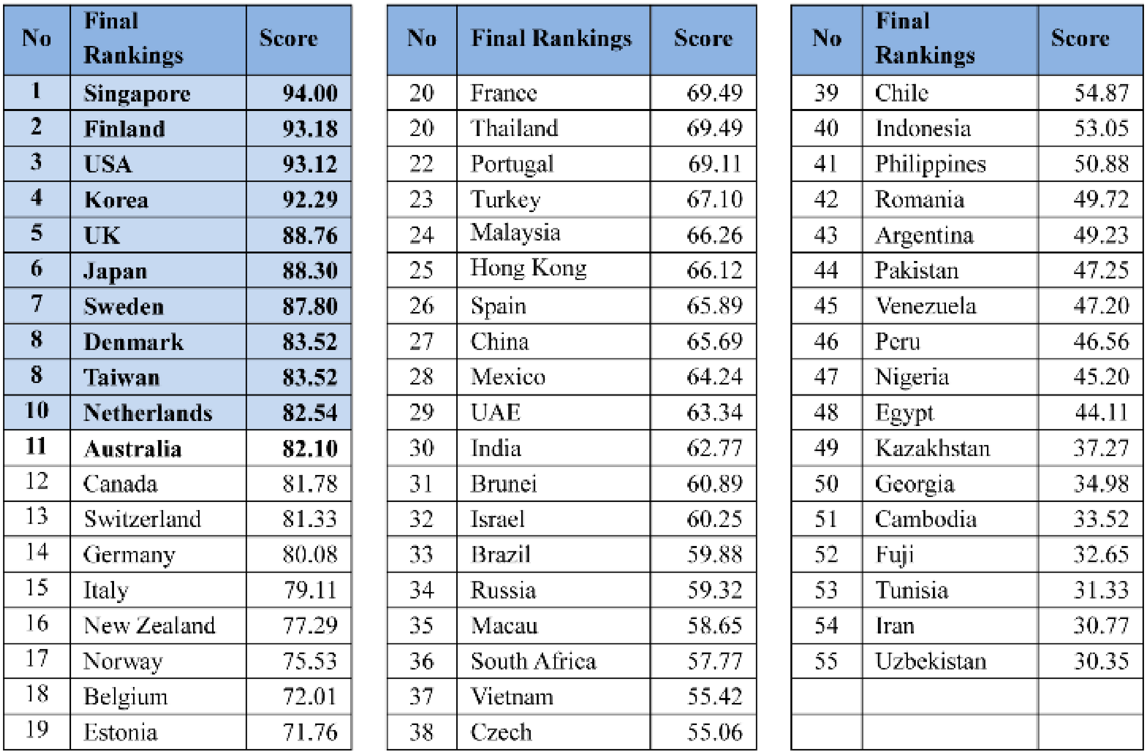
Most developing countries receive low score since there is no strong evidence on CIO mandate, CIO Presence as well as CIO development programs

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

Country overview

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

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



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

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

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

Technologies and solution deployed

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

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

Objectives and strategies

- Develop and implement information technology policy.
- Coordinate information technology investment strategy and capital planning.
- Develop and implement Enterprise Architecture.
- Implement Data Management program.
- Identify and oversee business process improvement opportunities.
- Develop and implement information technology performance measures.
- Oversee the Department's Reports Management Program, including the Information Collection Budget.

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

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

Table of contents

0 Introduction

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

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

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

1 E-Government Delivery Models – Use of Mobile Terminals

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

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

- Not every citizen owns a personal computer, but usually almost everybody owns a mobile phone (According to the ITU report "Trends in Telecommunication Reform 2012", by the end of Y2011 there were 6 billion mobile subscribers and almost twice less Internet users all over the world);
- Mobile phones are always with their owners and always on-line;
- In some cases mobile communication may be the only available way of communication;
- Mobile communications are not less secure than the Internet.

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

- m-Powering Development
- m-Health for NCDs (jointly with WHO)

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

- Government-to-Government (G2G)
- Government-to-Business (G2B)
- Government-to-Employees (G2E)
- Government-to-Citizens (G2C)
- Obviously, G2C is the most widely used model and this model, in particular, can play an important role in world-wide spread of m-services.

2 G2C Activities

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

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

- Usually, four types of G2C activities take place: governance, e.g. online polling, voting, and campaigns.
- one-way communication, e.g. regulatory services, general holidays, public hearing schedules, issue briefs, notifications, etc.
- two-way communication between the Agency and the Citizen. In this model, users can engage in dialogue with agencies and post questions, comments, or requests to the Agency.
- financial transactions, e.g. payments, lodging tax returns, top-ups, fines.

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

Two-way communication between the Agency and the Citizen

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

Financial Transactions

The service of carrying out financial transactions should be universal. This will allow to process non-cash payments with state institutes, trading companies, service providers and between citizens, including cross-border payments, which means not only G2C, but also B2C and C2C transactions. Along with these services the option to initiate a payment by either party should be available. Sources of payment may be national or international bank cards, clients' bank accounts, and even personal accounts of mobile network subscribers, or so-called "electronic money". In this proposal Mobile Payment System (MPS) becomes a part of national Retail Payment System being under the government control. While processing cross-border transactions, it is important that national payment systems of various countries should be compatible with each other. That is impossible to fulfil without following common standards. ITU, as an international organisation and under aegis of UNO, should carry out coordination and standards settling.

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

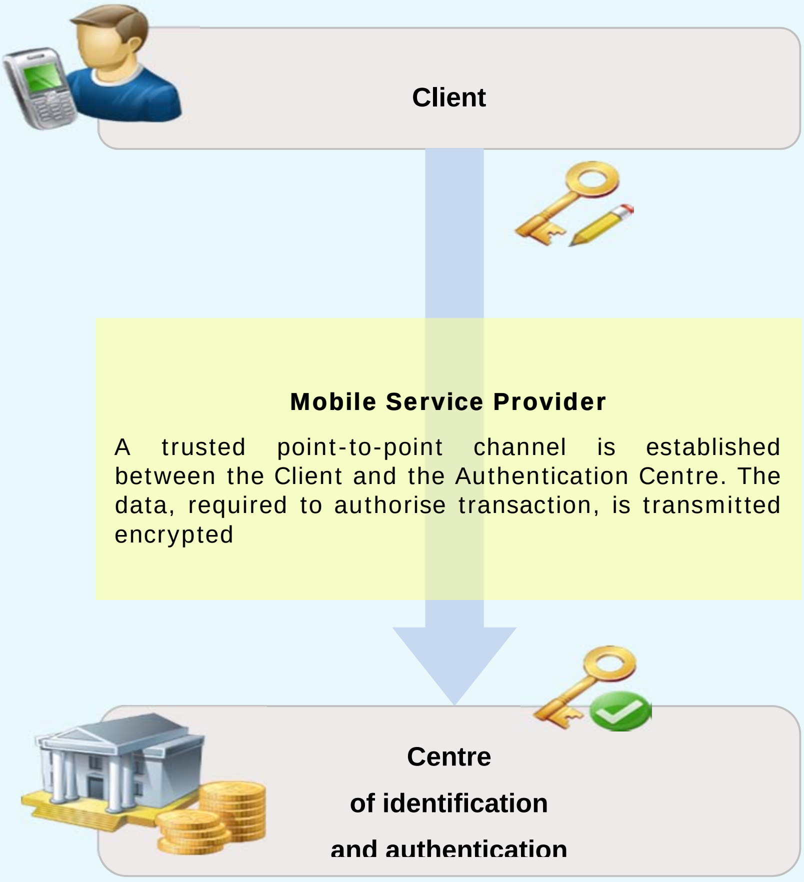
3 General Principles for Secure Mobile Services

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

3.1 Identification and authentication

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

Figure 3: Infrastructure of secure data transmission



A trusted point-to-point channel is established between the Client and the Authentication Centre. The data, required to authorise transaction, is transmitted encrypted

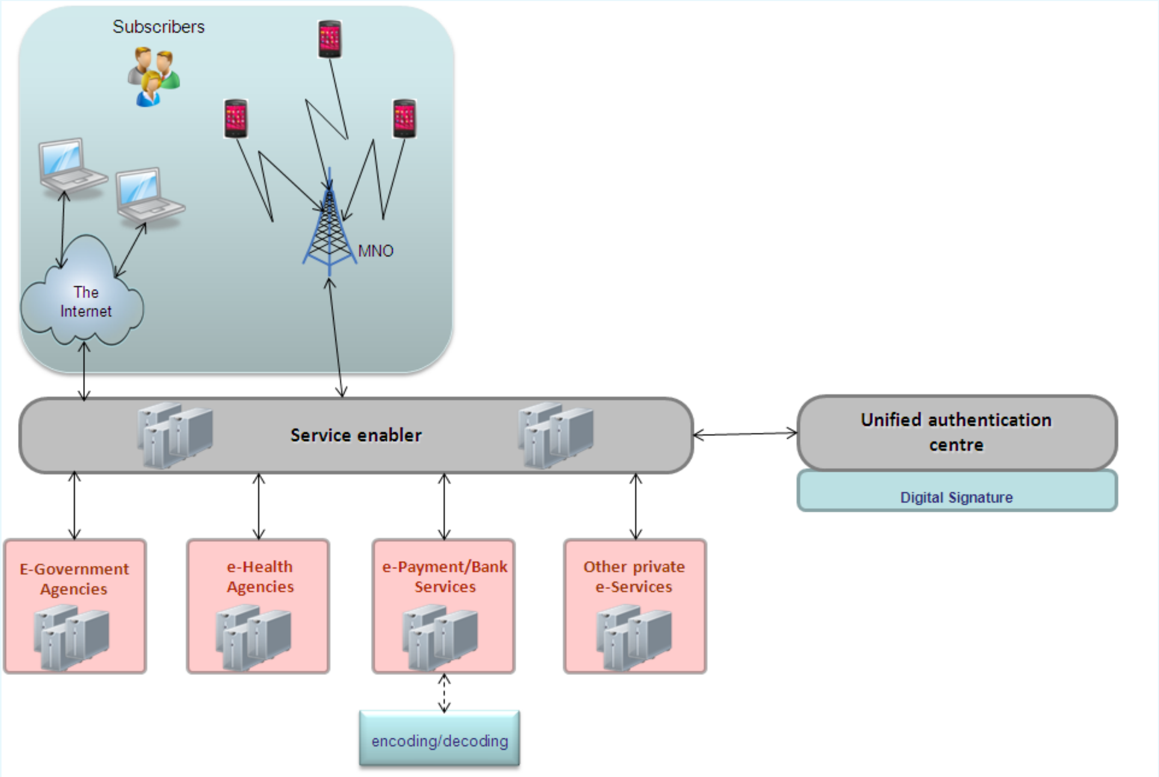
Existing mobile payment systems have already implemented their own security procedures, where security requirements are determined by agreements between service providers and their customers. Obviously, e-government requires a security system, controlled by the State and compliant with national law regulations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

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

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

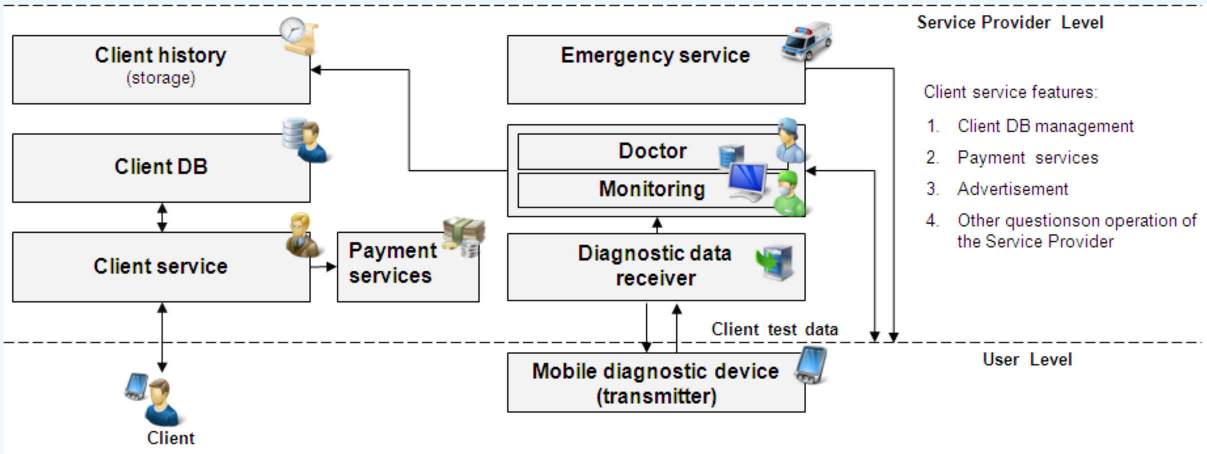
All identification and authentication centres must comply with the same allocation rules and regulations for global identifiers of mobile clients (mID), registered in a central System Directory to ensure message delivery to customers.

Figure 4: Unified authentication model with additional cryptography



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

Figure 5: The structure of a separate medical service provider



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

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

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

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

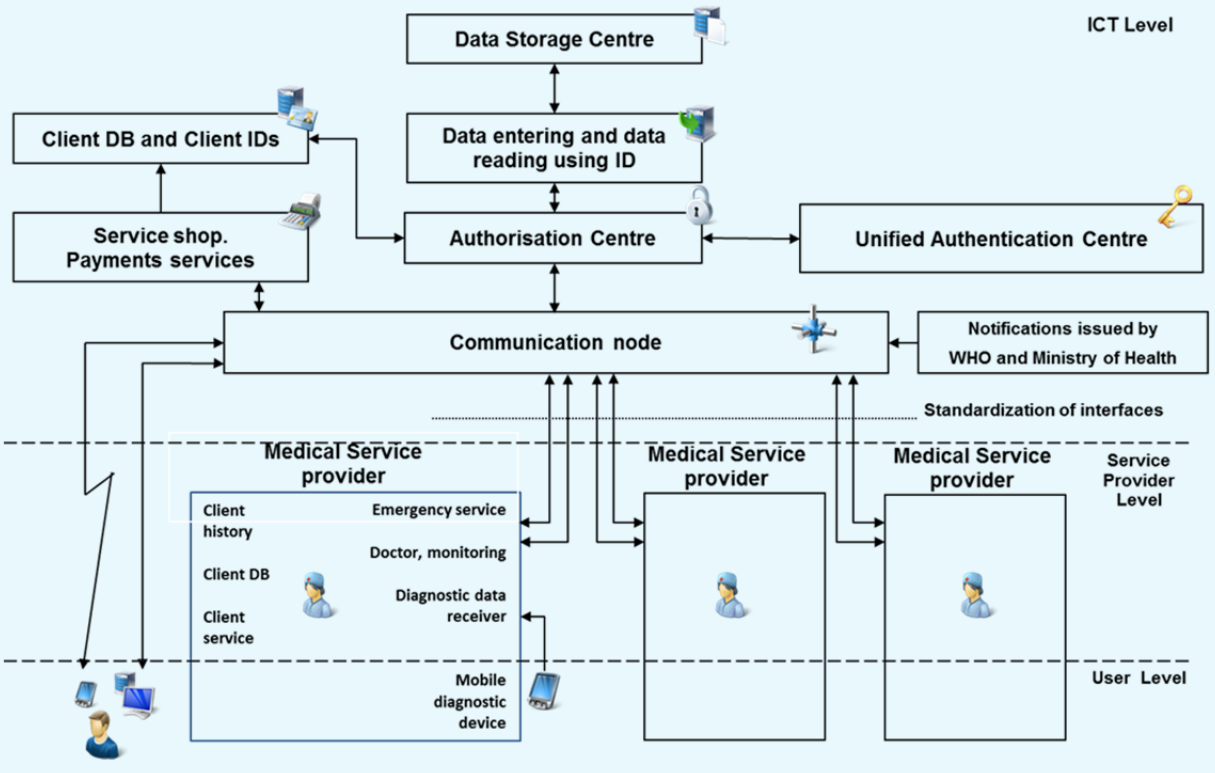
4) Insufficiency of authentication and protection of personal data

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

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

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

Figure 6: Proposed structure of the State healthcare system



3.2 Keys administration

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

Asymmetric key cryptography applies public-key infrastructure (PKI) to link two different keys which belong to one individual: "public" key, with publicly available identity, and "private" key that is securely stored and protected from unauthorized access (for example, in SIM card or specially protected smart card). Mathematical interaction between keys is managed in such a way that an action committed with one key can be "linked" to another key, without disclosing the private key data. This is particularly useful for creating an electronic signature, since the signing action completed by the private key identifies the private key owner only due to the relationship with the associated public key - the identity of the latter is known. The most important task of PKI technology is, on one hand, to ensure "privacy" of private keys, and on the other hand - to verify the relationship between open and private keys. This is achieved by careful management of registration process when keys are issued, and certification process, confirming the identity of the public key. These elements are managed respectively by entities known as "Registration" and "Certification" Authorities, (i.e. RA and CA). In relation to mobile signature, their primary function is to acknowledge the unique relationship between private key usage and the registered identity of the Citizen by virtue of his/her ownership of the associated public key.

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

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

– The application is loaded onto mobile device from an open source together with the public key of the System.

– During the activation process, the application generates a random symmetric session key.

– The application sends this session key encrypted using the public asymmetric key of the System.

– The System decrypts the session key using System’s secret key and stores it at the Hardware Security Module.

– This session key is used by both the System and the Application for all subsequent activities.

4 Mobile Payment System (MPS)

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

4.1 MPS participants and their Roles

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

– MPS Operator

– Mobile Operator

– Banks (for typical MPS)

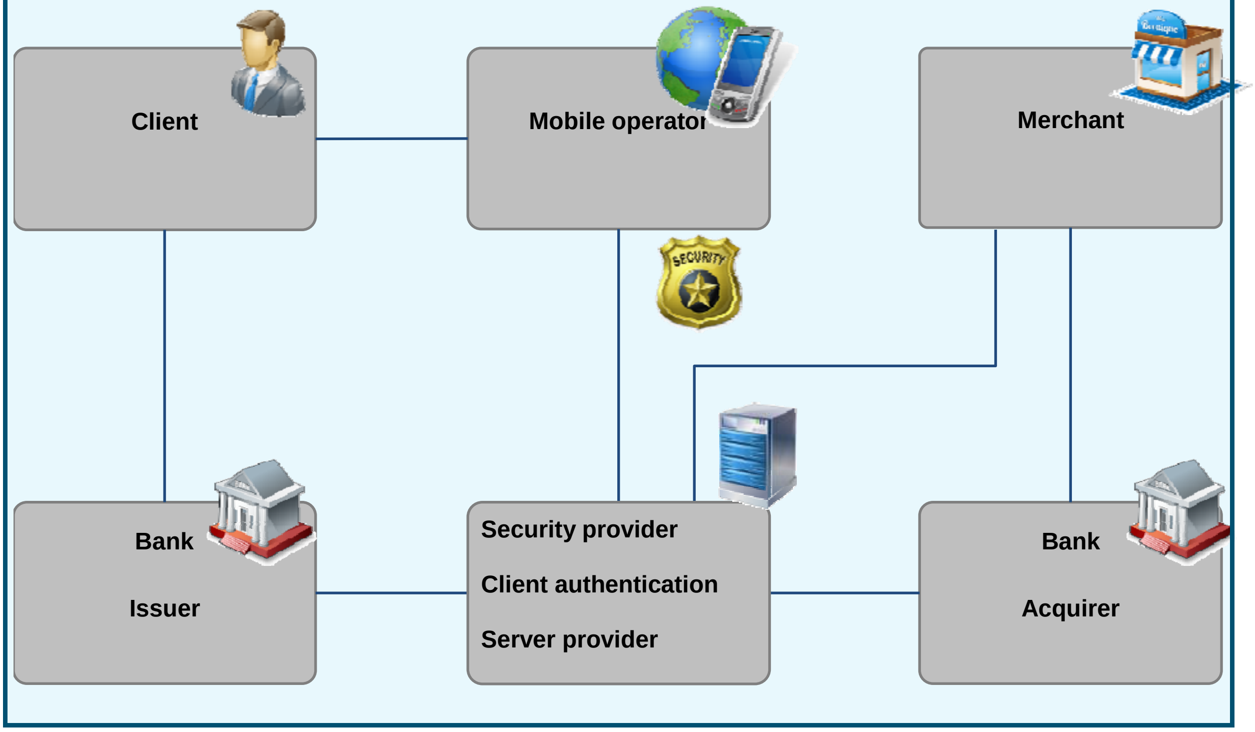
  - Clients’ Bank (bank issuer)
  - Acquiring bank, accepting payments and providing access to Clients’ banks for merchants or service providers
  - Settlement Bank (interbank settlements)

- Clients (mobile Operator subscribers, using Mobile Payment System and owning payment card or bank account)
- Client application – a special program downloaded to a mobile terminal of the Client, or to special hardware security module, for example, SIM card, which allows to perform registration, select payment means, interact with authentication agent, perform financial transactions, and also to set up payment details.
- Issuers of Client applications
- Merchants (legal entities, clients of Acquiring Banks)
- Authentication agent (Client authentication)

4.2 Typical System Architecture

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

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

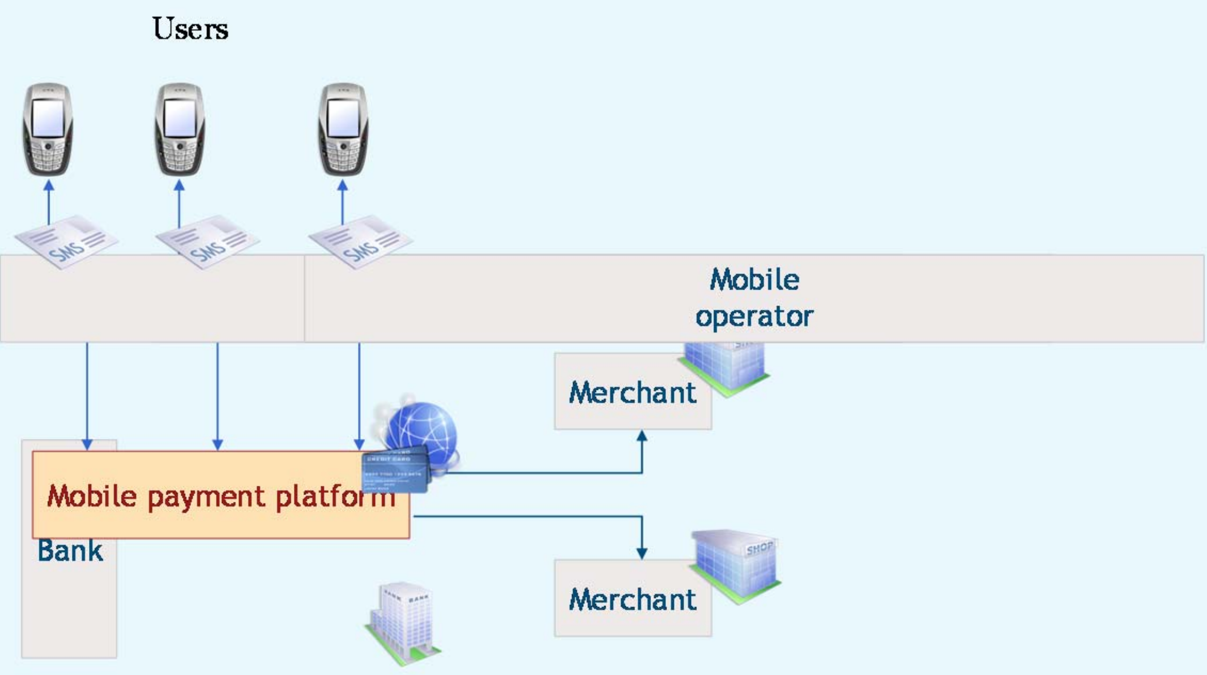


4.3 MPS Models

Different MPS models exist:

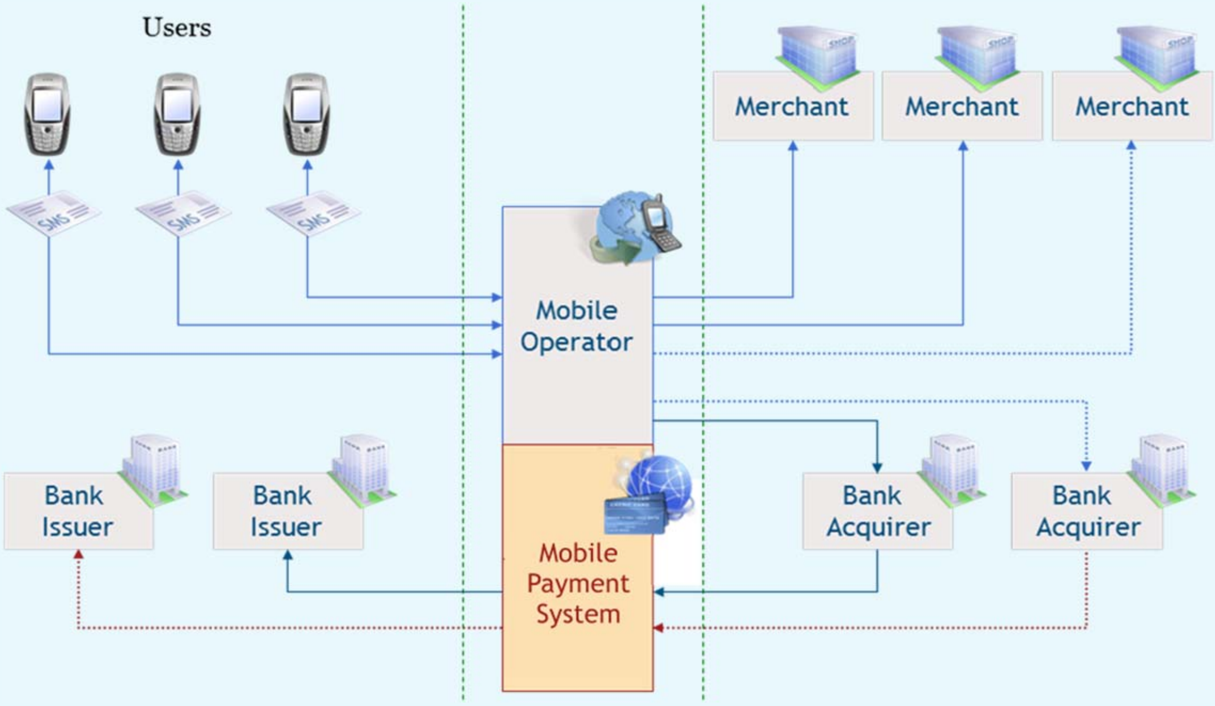
- Bank-oriented model (Figure 8), where bank offers mobile payment services with many mobile operators.

Figure 8: Bank-oriented MPS model



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

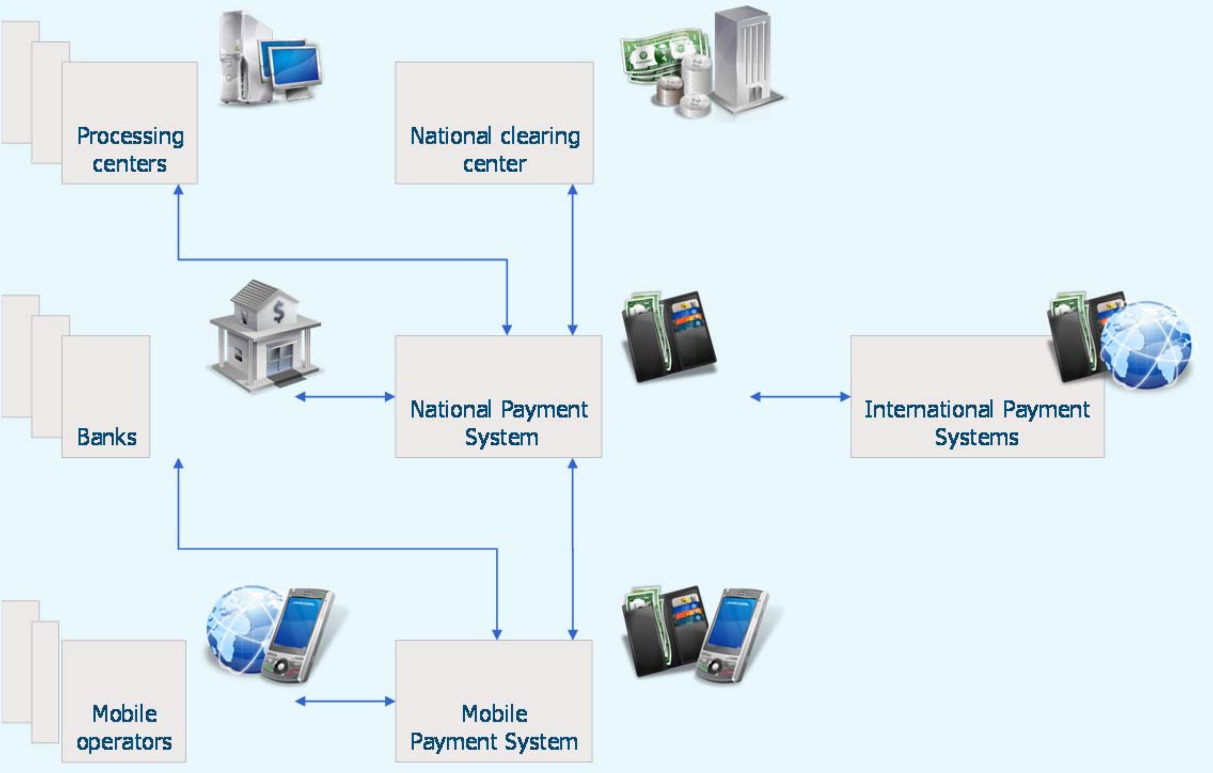
Figure 9: Operator-oriented MPS model



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

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

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



4.4 Available payment means

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

- Bank account
- Bank cards issued by local or global payment systems
- MNO subscribers personal accounts
- E-money

4.5 Payment arrangement

Two operation types are available in MPS:

- Operations initiated by the Client
- Operations initiated by the Merchant

4.5.1 *Operations initiated by the Client*

Transactions initiated by the Client may contain the following steps:

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

4.5.2 *Operations initiated by the Merchant*

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

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

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

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

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

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

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

g) Authentication of the Client;

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

i) The operation result is sent to the Client;

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

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

4.6 Near Field Communications (NFC)

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

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

- Mobile Device with NFC Chipset or Secure Element of NFC Chipset containing the logic and interfaces to communicate with card readers.
- Mobile Network Operator (MNO)
- One or many Service Providers
- Trusted Service Manager or broker providing a point of contact between service providers and MO

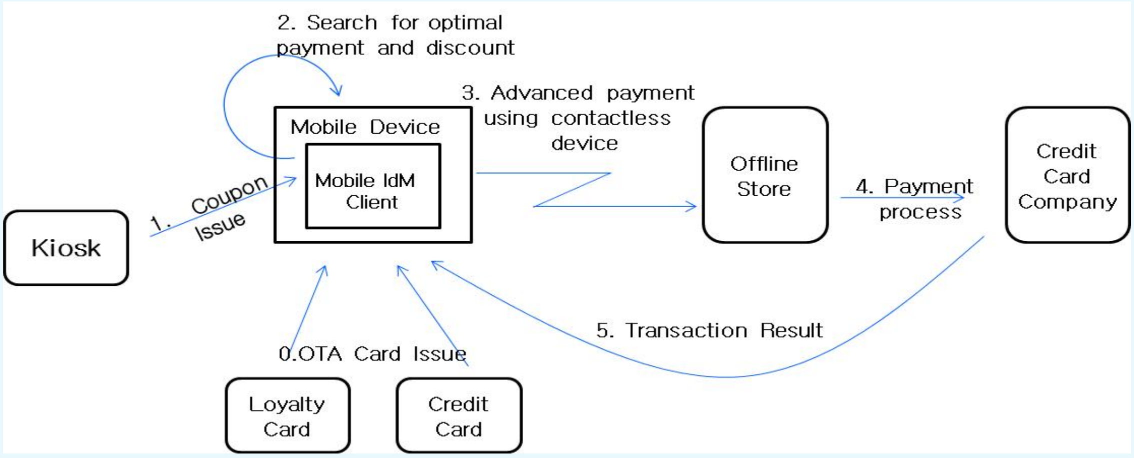
It is considered, that NFC payment systems can use credit cards as payment means for interactive shopping purchases via contactless NFC devices. After the payment transaction is processed successfully, result is stored in the system and sent to subscriber's handset. The use case is depicted in Figure 11 below. In order to actualise the scenario described above, following requirements are needed:

– User Authentication Communication security

– Protection of information stored, if mobile device is lost or stolen

– System storage to accumulate and process transaction records

Figure 11: Interactive shopping



NFC systems, due to its features, have become the most popular when carrying out the sale of consumer goods, and also within the transport sector, allowing for a reduction in the time spent to purchase tickets and significantly reducing lines for customers. Also, NFC-based systems can be successfully applied for authentication purposes instead of paper ID. Despite the differences, the main security methods for NFC operations remain the same as for remote services.

5 Security

The most important requirement for payment systems, as well as e-government and e-health, including their mobile variations, is security, which is provided by meeting recommendations of the ITU Telecommunication Standardization Sector, which issued a manual entitled "Security in telecommunications and information technologies[6]". This manual provides an overview of existing ITU-T Standards and their practical application in secure telecommunications. ITU-T Standards are required to follow, they stay as recommendations, but compliance with recommendations is essential to ensure compatibility and consistency of telecommunication systems of different countries.

Since these systems include many players, security considerations can be divided in multiple categories that include:

a) End-point Security

b) Mobile Application Security

c) Mobile Network Security

d) Identification of the requesting party that includes proper identification of the individual that is requesting the financial transaction.

Prior to the era of smart phones, management of mobile applications by operators on mobile phones was relatively easy. Basically, operators used to control which application can be downloaded onto device and their security characteristics. Management of mobile applications becomes more complicated with the advent of smart phones and ability to freely download third party applications. Nowadays, it is almost impossible to be completely certain that every application that is executing on a mobile device originated from a trusted source. As a result, mobile users are subject to additional threats such as identity theft, phishing, and loss of personal data.

The term "security" is used in the sense of minimising vulnerabilities of assets and resources. An asset is anything of value. Vulnerability is any weakness that could be exploited to violate a system or information it contains. A threat is a potential violation of security. The ITU-T Recommendation X.805 "Security Architecture for Systems Providing End-to-End Communications[7]" (Figure 10) of defines set of eight so-called "Security dimensions" – set of means that protect against all major security threats, described in the ITU-T Recommendation X.800 "Security architecture for Open Systems Interconnection for CCITT applications"[3]*:*

– destruction of information and/or other resources;

– corruption or modification of information;

– theft, removal or loss of information and/or other resources;

– information disclosure;

– service interruption.

Security dimensions are not limited to the network, but extend to applications and end user information as well. In addition, security dimensions apply to service providers or enterprises offering security services to their customers. The security dimensions are:

1) Access control;

2) Authentication;

3) Non-repudiation;

4) Data confidentiality;

5) Communication security;

6) Data integrity;

7) Availability;

8) Privacy.

Properly designed and implemented security dimensions support security policy that is defined for a particular network and facilitate the rules set by the security management.

The access control security dimension protects against unauthorized use of network resources. Access control ensures that only authorised personnel or devices are allowed to access network elements, stored information, information flows, services and applications. In addition, Role-Based Access Control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to, and perform operations on, network elements, stored information, and information flows that they are authorised for.

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

The authentication security dimension serves to confirm identities of communicating entities. Authentication ensures validity of claimed identities of entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication.

The non-repudiation security dimension provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It provides evidence that can be presented to a third party and used to prove that an event or action has taken place.

The data confidentiality security dimension protects data from unauthorized disclosure. Data confidentiality ensures that the data content cannot be understood by unauthorized entities. Encryption, access control lists and file permissions are methods often used to provide data confidentiality.

The communication security dimension ensures information flows exchange only between the authorised end points (information is not diverted or intercepted as it flows between these end points).

The data integrity security dimension ensures correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.

The availability security dimension ensures that there is no denial of authorised access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category.

The privacy security dimension provides protection of information that might be derived from the observation of network activities. Examples of this information include web sites visited by a user, user geographic location, and IP addresses and DNS names of devices within service provider network.

In order to provide an end-to-end security solution, security dimensions must be applied to a hierarchy of network equipment and facility groupings, which are referred to as security Layers and security Planes. The Recommendation X.805 defines three security layers build on one another to provide network-based solutions:

– Infrastructure security Layer, consisting of network communication means and individual network elements (routers, switches, servers, communication lines);

– Services security Layer to protect service providers and their clients (both basic services – connection to resources, DNS, and additional services – VPN, QoS, etc.);

– Applications security Layer, includes 4 potential targets: application user, service provider, application provider, bounding software.

Security layers represent a series of interrelated factors that contribute to ensure network security: Infrastructure security layer allows to use Services security layer and Services security layer allows to use Applications security layer. Security architecture takes into account that each layer has different security vulnerabilities, and provides flexibility in reflexion of potential threats in the most appropriate way for a particular security layer.

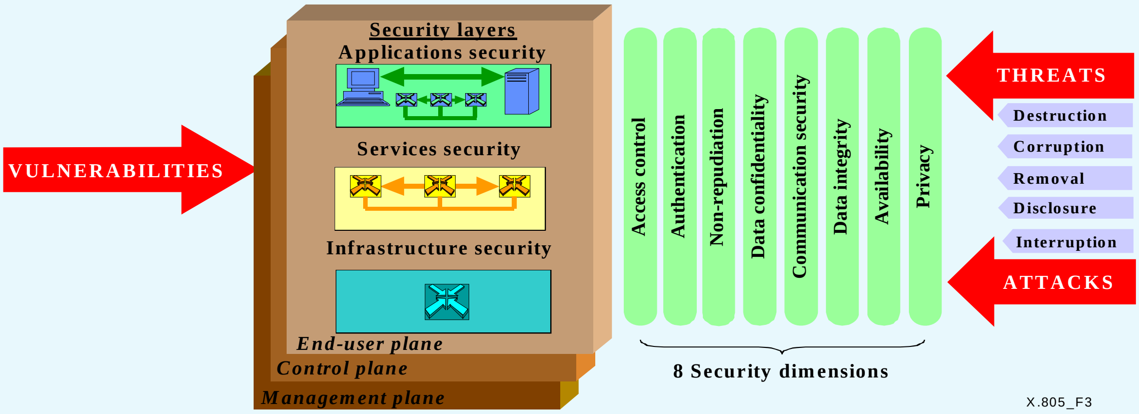
Each of these security Layers consists of three security Planes, representing a specific type of network operation, protected by Security dimensions:

– End-User Plane;

– Control Plane;

– Management Plane.

Figure 12: X.805 – Security architecture for end-to-end network security



According to this Recommendation the security architecture logically divides the System in question into separate architectural components. This separation assumes a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing solutions. The security architecture addresses three essential questions with regard to the end-to-end security:

1) What kind of protection is needed and against what threats?

2) What are the distinct types of system equipment and facility groupings that need to be protected?

3) What are the distinct types of system activities that need to be protected?

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

– Required security should be based on the use of:

– Means of identification and authentication of participants;

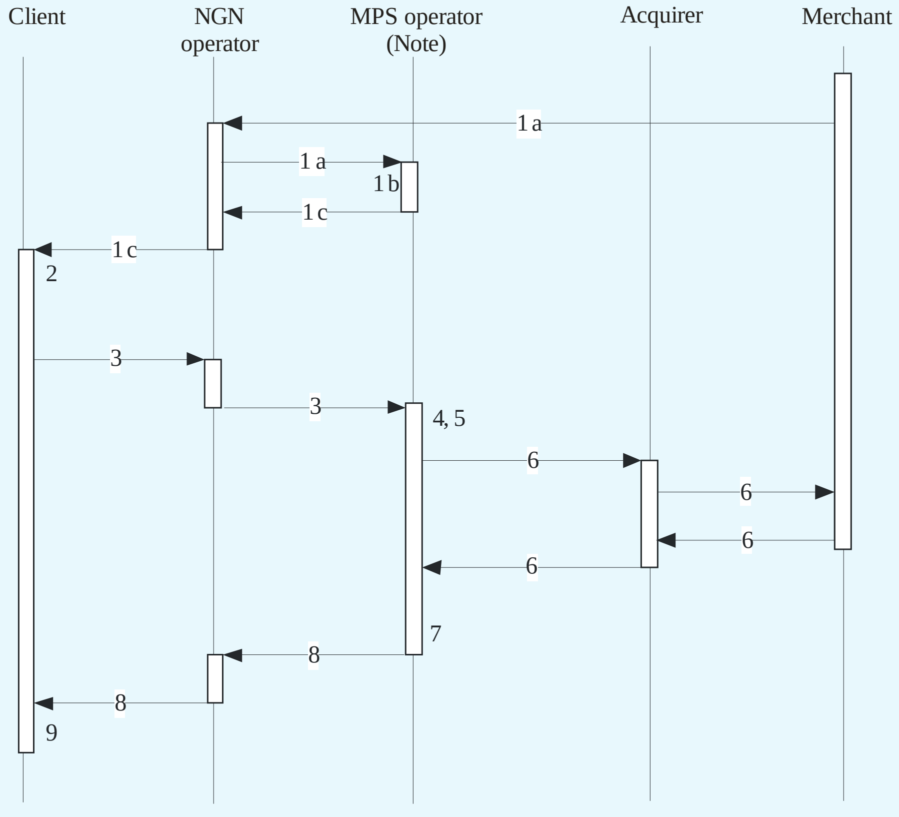
– Encryption of data transmitted through communication channels;

– Physical and administrative means to ensure the safety of information transmission and storage.

The ITU Recommendation X.1122[9] applies when using asymmetric cryptography, and provides guidelines for creation of secure mobile systems based on Public Key Infrastructure (PKI). This standard describes generation of public and private keys, certificate applications, as well as issuance, activation, use, revocation and renewal of the certificate.

The ITU Recommendations Y.2740 and Y.2741 describe security requirements and architecture of secured mobile financial transactions. These recommendations, though made for mobile remote financial transactions in NGN, are fully applicable to ensure security for m-Payment, m-Health and m-Government Systems in 2G, 3G and 4G mobile networks. The Recommendation Y.2741 describes the system architecture (Figure 5) and possible interaction scenarios. The example of such scenario for Merchant initiated payment is shown in Figure 11.

Figure 13: Performing payments initiated by merchant



NOTE – Security provider, client authentication provider, service provider.

ITU-T Y.2741(11)_F04

The basic steps of the scenario are as follows:

1. a) the Merchant generates a payment offer and sends it to the MPS operator;

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

   c) the request is sent to the client over the mobile operator channels.

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

3. The request is transmitted via the mobile operator channels;

4. The MPS operator receives the client's response;

5. Authentication of the client;

6. The required financial operation (remittance/payment) is performed using the client's payment instrument details;

7. The operation result is sent to the client;

8. The response is transmitted via the mobile operator channels;

9. The client receives the result of the financial operation.

The Recommendation Y.2740 defines four levels of system security and its provision. Security Level is determined by the extent to which security dimensions are implemented in the System. According to this Recommendation system participants should be aware of the Security Level, which should be stipulated in the participants' agreement if it is not contrary to the law. Service providers can further reduce the risks by organizational means - to restrict the transfer of some information, to limit service for users with a low level of loyalty, etc. The System security is entrusted upon every participant of the System and is achieved by the physical and administrative facilities of security assurance at data transfer, processing and storage. Implementation of security dimensions are required to be executed by all the participants in respect of data involved in information exchange. Thus the subscribers are responsible for maintaining the secrecy of their PIN codes, for the safe storage of their mobile terminals, as well as for confidential information related to a bank account or plastic payment card secure parameters. In turn, service providers are liable for the logging of performed transactions, security of transmitted and stored sensitive information, user authentication, etc.

Security Levels defined in the ITU-T Recommendation Y.2740 "Security requirements for mobile remote financial transactions in next generation networks":

Security Level 1

System can rely on authentication provided by the NGN operator. Data confidentiality and integrity at their transfer are ensured by the data transfer environment (communications security), and at their storage and processing – by the data storage mechanism and System access control facilities. The privacy is ensured by the absence of sensitive data in the messages being transferred as well as by the implementation of the required mechanisms of data storage and the System access control facilities. The System components must not have latent possibilities of unauthorized data acquisition and transfer.

Security Level 2

Authentication when using the System services can be executed by using only one authentication factor and thus can be implemented without the application of cryptographic protocols. One-Time Password is used for authentication. One-Time Password is generated by means of various tokens (Single Factor OTP Device, Single Factor Cryptographic Device, etc.). Data confidentiality, integrity and privacy are ensured similarly to Level 1.

Security Level 3

Multifactor client authentication must be used to access System services. The Client shall use more than one authentication factor. Data confidentiality, integrity and privacy at message transmission must be ensured by using additional message encryption together with data transfer protocols that ensure the security of the data being transferred by the interoperation participants (including data integrity verification); at data storage and processing their confidentiality, integrity and privacy are ensured by additional mechanisms of encryption and masking, together with well-defined distribution of access in accordance with privileges and permissions.

To meet security requirements at this level, System shall use software modules installed in Clients' handsets. These modules shall implement at least two-factor authentication and ensure both encryption and decryption of transferred data. Each authentication shall require entry of the password or other activation data to activate the authentication key and the unencrypted copy of the authentication key shall be erased after each authentication (Multi-factor Software Cryptographic Token).

All System interoperation participants shall use security facilities that ensure the System against break-in. In the Level 3 solutions the security of data transferred over the communications channels shall be ensured by means of strong cryptography. The strength of a cryptographic method depends on the cryptographic key being used. Effective key size shall meet minimal length recommendations to suffice protection.

Security Level 4

This is the highest System security assurance level. To meet security requirements at this level, clients' mobile terminals shall be equipped with hardware security modules. Implementation of other security dimensions shall fully correspond to level 3. Both symmetric and asymmetric cryptographic algorithms may be applied to message encryption. To prevent interception or corruption of information between mobile terminal elements (e.g. CPU and display, CPU and keyboard), some security measures shall be taken to ensure the integrity of data exchange on the Client's device (Trusted Execution Environment).

Security dimensions that are equally implemented at all Security Levels:

– access control,

– non-repudiation,

– communication security,

– availability

The following security dimensions have different implementation at different Security Levels:

– authentication,

– data confidentiality,

– data integrity,

– privacy

From Table 1 it follows that the implementation of the first and second levels of security can be achieved without installation of any special applications on the mobile device or special security element of mobile device; but to implement the third and fourth security levels, it is necessary to install custom applications that provide client authentication, encryption and decryption of data transmitted.

Table 8: Security implementation degree - (Y.2740) subject to Security Level

Security Dimension	Security Level			
	Level 1	Level 2	Level 3	Level 4
Access Control	The access to every system component shall be granted only as provided by the System personnel or end-user access level.			
Authentication	Authentication in the System is ensured by the NGN data transfer environment	Single-factor authentication at the System services usage	Multi-factor authentication at the System services usage	In-person connection to services where personal data with obligatory identification is used. Multi-factor authentication at the System services usage. Obligatory usage of Hardware Cryptographic Module.
Non-repudiation	The impossibility of a transaction initiator or participant to deny his or her actions upon their completion is ensured by legally stated or reserved in mutual contracts means and accepted authentication mechanisms. All system personnel and end-user actions shall be logged. Event logs shall be change-proof and hold all actions of all users.			

Table 8: Security implementation degree - (Y.2740) subject to Security Level

Security Dimension	Security Level			
	Level 1	Level 2	Level 3	Level 4
Data confidentiality	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.		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.	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).
Data integrity				
Privacy	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.			
Communication	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.			
Availability	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			

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:

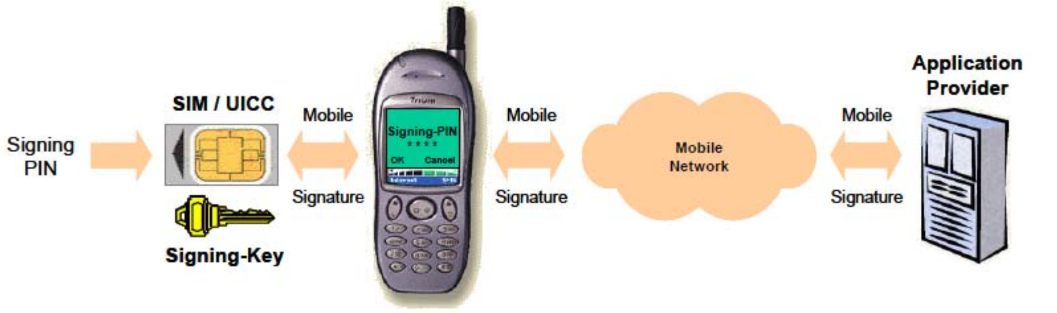
– ETCI TR 102 203[4]
"Mobile Commerce (M-COMM); Mobile Signature; Business & Functional Requirements"

[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.

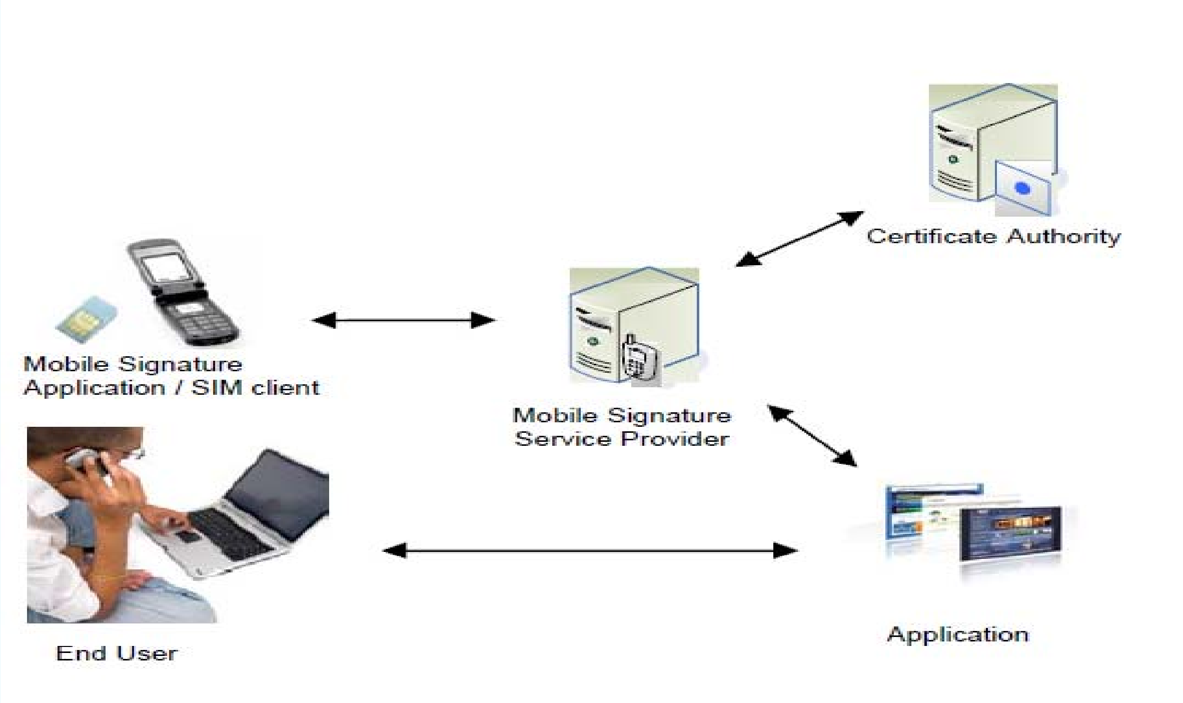
– Mobile application sends Mobile Signature to MSSP.

– 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"


Certificate Authority
Mobile Signature Application / SIM client
Mobile Signature Service Provider
End User
Application

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.

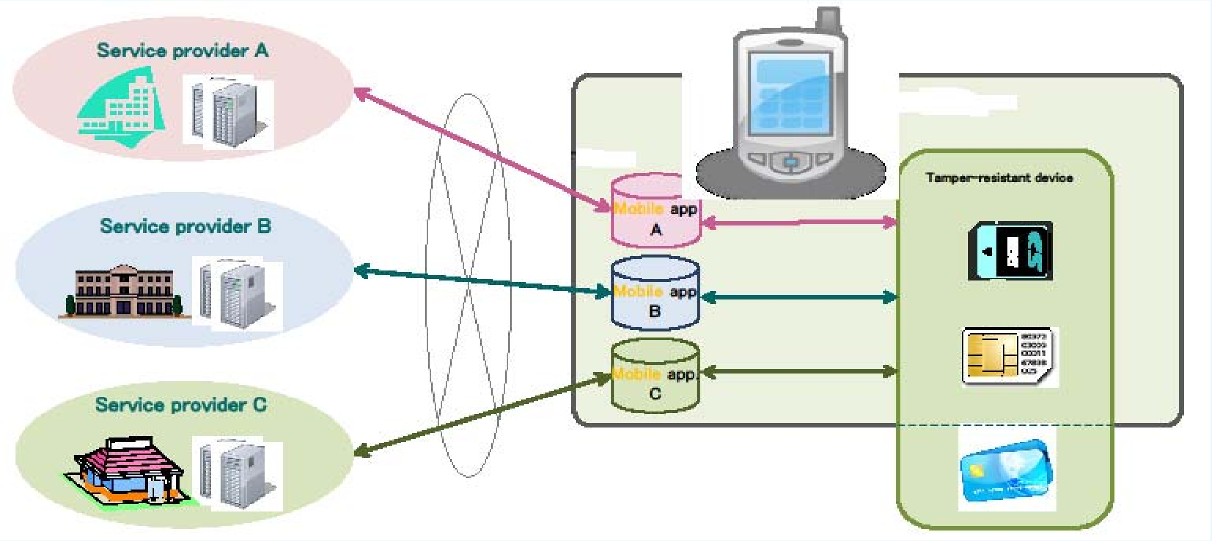
In addition, spread of smartphones has been progressing rapidly. Smartphone shipments in Japan in FY 2011 amounted to 23.4 million units (2.7 times increase year-on-year), accounting for 55.8 % of total shipments of mobile phone terminals[16]. Furthermore, since FY 2012, mobile phone terminals with NFC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

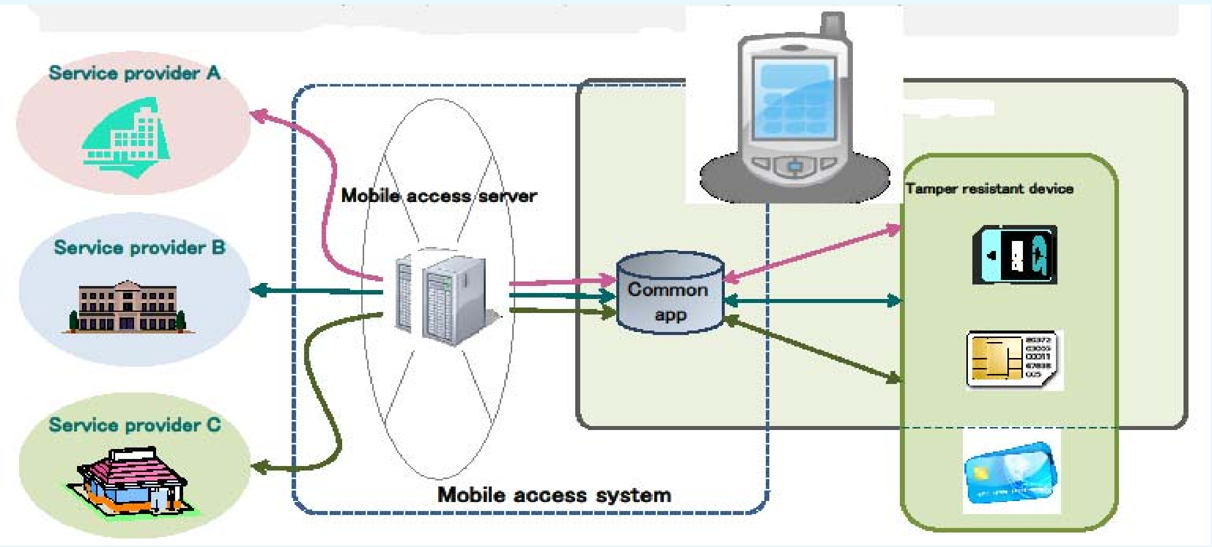
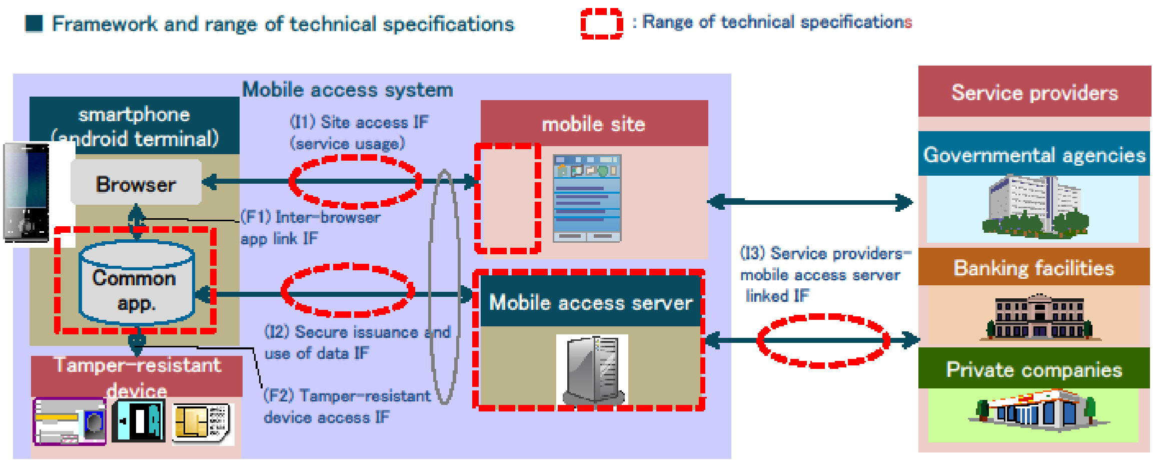


Figure 17: Common application and unified mobile access server for all service providers. Further, verification by experimentation with technical specifications etc. was studied. In other words, **A:** Examination of technical specifications for a mobile access system realising online storage and use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


Framework and range of technical specifications
: Range of technical specifications
Mobile access system
smartphone (android terminal)
Browser
Common app.
Tamper-resistant device
(I1) Site access IF (service usage)
(F1) Inter-browser app link IF
(I2) Secure issuance and use of data IF
(F2) Tamper-resistant device access IF
mobile site
Mobile access server
(I3) Service providers-mobile access server linked IF
Service providers
Governmental agencies
Banking facilities
Private companies

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.

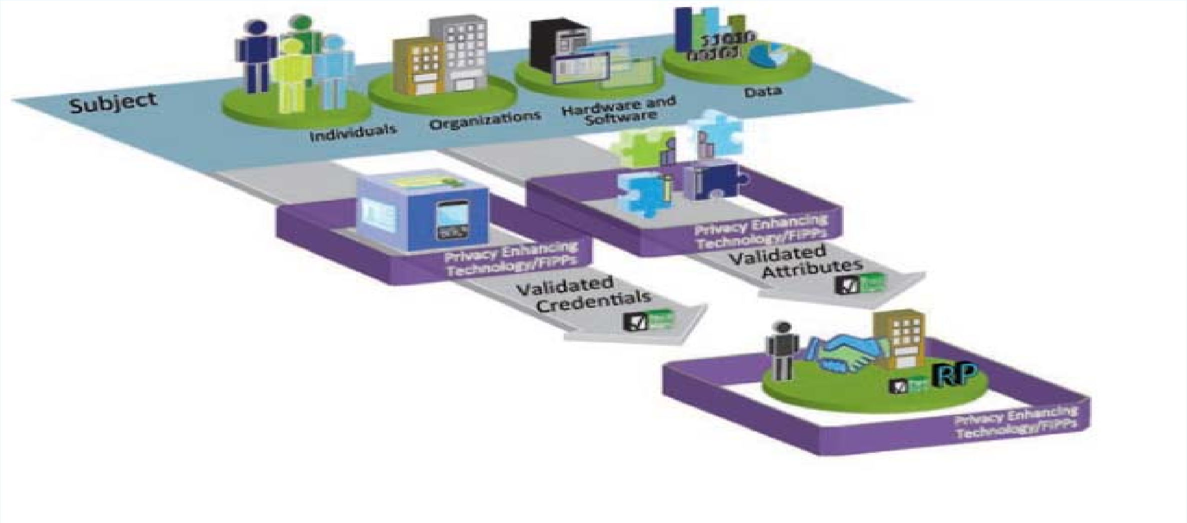
In order to realise the services above, further experimental studies for overcoming technical difficulties will be conducted. The main topics for consideration in the future in light of the technology are methodologies of authentication of the issuing terminal when storing the ID information, such as 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


Subject
Individuals
Organizations
Hardware and Software
Data
Privacy Enhancing Technology/FIPPs
Validated Credentials
Privacy Enhancing Technology/FIPPs
Validated Attributes
RP
Privacy Enhancing Technology/FIPPs

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)

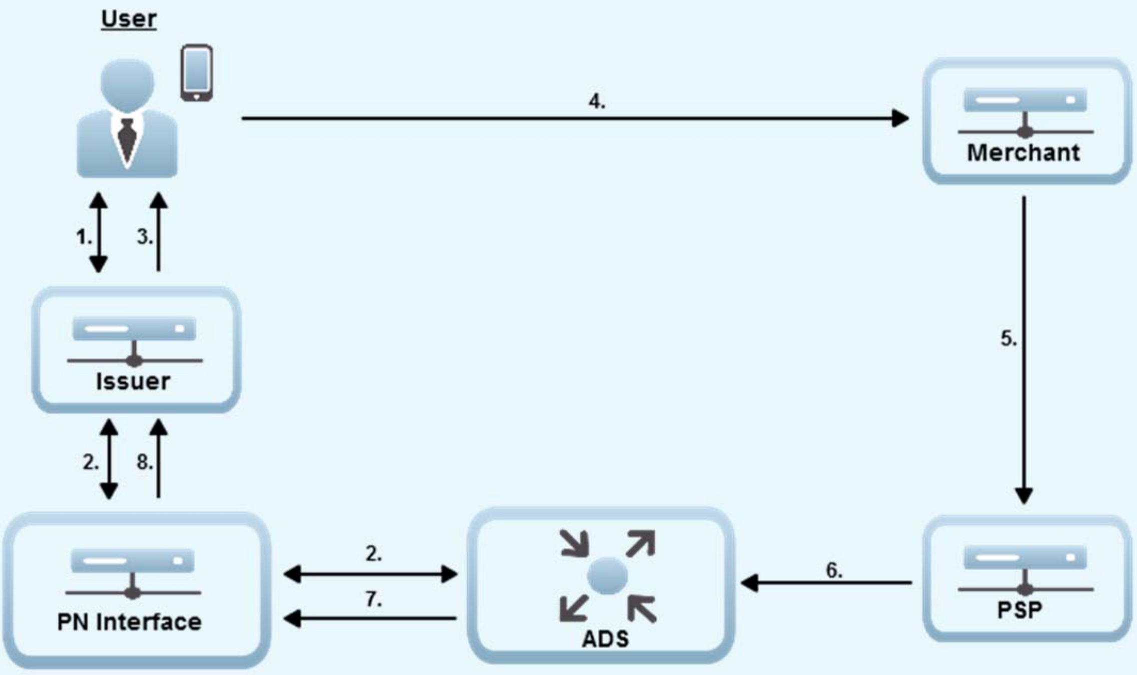
1. Open mobile payment app (can be set with or without PIN)
2. Choose pay and for example swipe mobile at POS-terminal (an OTT is shown on the mobile and transferred to the merchant)
3. Approve payment in app with PIN (can be set without need of OK or OK+PIN for low value transactions)
4. Receipt printed

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

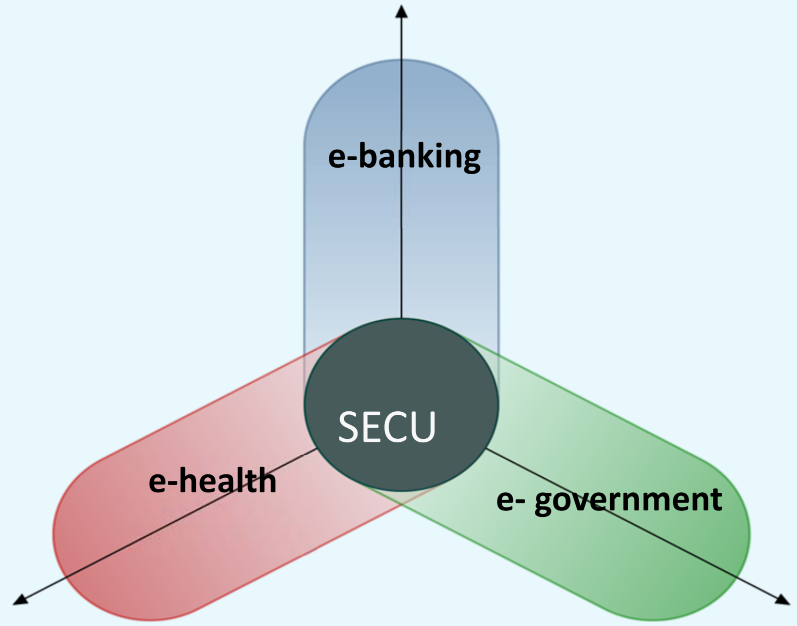
As shown in implementation cases described in chapters 6-9 above, development and usage of mobile devices for *m-Government, m-Health, m-Payment, m-Learning and so on* are at different levels in various countries, however, in today's global world the penetration of technology innovations increases drastically,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

国际电信联盟（ITU）
电信发展局（BDT）
主任办公室
Place des Nations
CH-1211 Geneva 20 – Switzerland

电子邮件：	bdtdirector@itu.int
电话：	+41 22 730 5035/5435
传真：	+41 22 730 5484

副主任
兼行政和运营协调部负责人（**DDR**）

电子邮件：	bdtdeputydir@itu.int
电话：	+41 22 730 5784
传真：	+41 22 730 5484

基础设施、环境建设和
电子应用部（**IEE**）

电子邮件：	bdtiee@itu.int
电话：	+41 22 730 5421
传真：	+41 22 730 5484

创新和
合作伙伴部（**IP**）

电子邮件：	bdtip@itu.int
电话：	+41 22 730 5900
传真：	+41 22 730 5484

项目支持和
知识管理部（PKM）

电子邮件：	bdtpkm@itu.int
电话：	+41 22 730 5447
传真：	+41 22 730 5484

非洲

埃塞俄比亚

国际电联
区域代表处
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia

电子邮件：	itu-addis@itu.int
电话：	+251 11 551 4977
电话：	+251 11 551 4855
电话：	+251 11 551 8328
传真：	+251 11 551 7299

喀麦隆

国际电联
地区办事处
Immeuble CAMPOST, 3^{e} étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroon

电子邮件：	itu-yaounde@itu.int
电话：	+ 237 22 22 9292
电话：	+ 237 22 22 9291
传真：	+ 237 22 22 9297

塞内加尔

国际电联
地区办事处
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4^{e} étage
B.P. 50202 Dakar RP
Dakar – Sénégal

电子邮件：	itu-dakar@itu.int
电话：	+221 33 849 7720
传真：	+221 33 822 8013

津巴布韦

国际电联
地区办事处
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

电子邮件：	itu-harare@itu.int
电话：	+263 4 77 5939
电话：	+263 4 77 5941
传真：	+263 4 77 1257

美洲

巴西

国际电联
区域代表处
SAUS Quadra 06, Bloco “E”
11º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

电子邮件：	itubrasilia@itu.int
电话：	+55 61 2312 2730-1
电话：	+55 61 2312 2733-5
传真：	+55 61 2312 2738

巴巴多斯

国际电联
地区办事处
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

电子邮件：	itubridgetown@itu.int
电话：	+1 246 431 0343/4
传真：	+1 246 437 7403

智利

国际电联
地区办事处
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

电子邮件：	itusantiago@itu.int
电话：	+56 2 632 6134/6147
传真：	+56 2 632 6154

洪都拉斯

国际电联
地区办事处
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

电子邮件：	itutegucigalpa@itu.int
电话：	+504 22 201 074
传真：	+504 22 201 075

阿拉伯国家

埃及

国际电联
区域代表处
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

电子邮件：	itucairo@itu.int
电话：	+202 3537 1777
传真：	+202 3537 1888

亚太

泰国

国际电联
区域代表处
Thailand Post Training Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

邮寄地址：
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

电子邮件：	itubangkok@itu.int
电话：	+66 2 575 0055
传真：	+66 2 575 3507

印度尼西亚

国际电联
地区办事处
Sapta Pesona Building, 13th floor
JI. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

邮寄地址：
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

电子邮件：	itujakarta@itu.int
电话：	+62 21 381 3572
电话：	+62 21 380 2322
电话：	+62 21 380 2324
传真：	+62 21 389 05521

独联体国家

俄罗斯联邦

国际电联
地区办事处
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

邮寄地址：
P.O. Box 25 – Moscow 105120
Russian Federation

电子邮件：	itumoskow@itu.int
电话：	+7 495 926 6070
传真：	+7 495 926 6073

欧洲

瑞士

国际电联
电信发展局（BDT）欧洲处（EUR）
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland

电子邮件：	eurregion@itu.int
电话：	+41 22 730 5111

国际电信联盟
电信发展局
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

瑞士印刷
2014年，日内瓦

01/2014