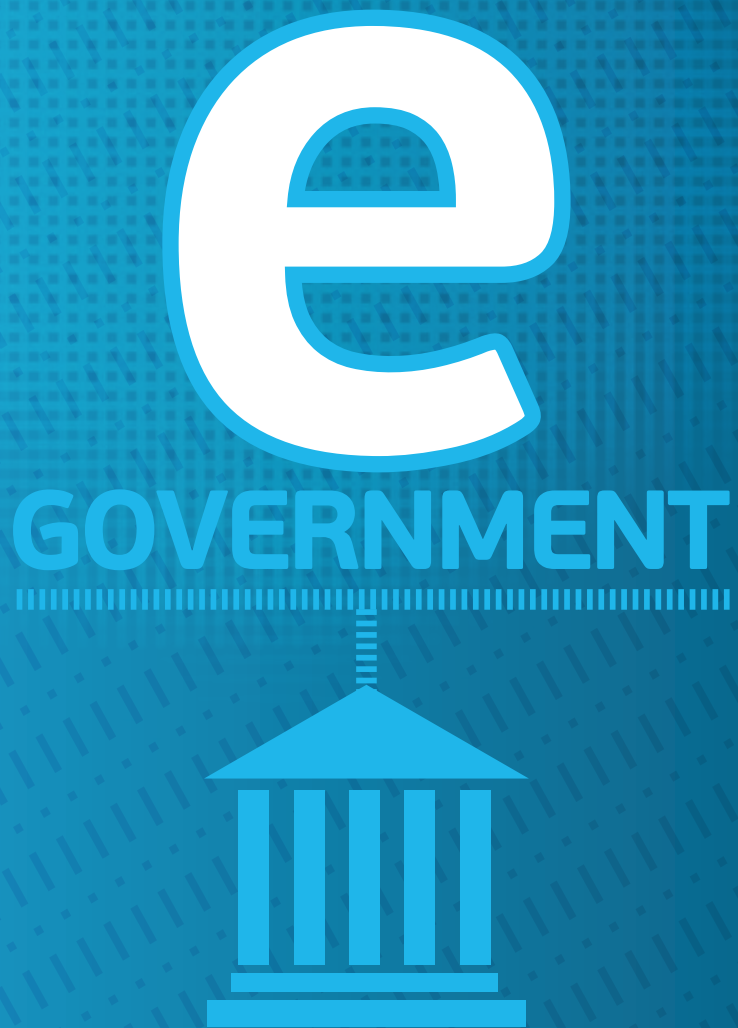
ЗАКЛЮЧИТЕЛЬНЫЙ ОТЧЕТ

**МСЭ-D 2-Я ИССЛЕДОВАТЕЛЬСКАЯ КОМИССИЯ**

# ВОПРОС 17-3/2

## ХОД ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА И ОПРЕДЕЛЕНИЕ ОБЛАСТЕЙ ПРИМЕНЕНИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА В ИНТЕРЕСАХ РАЗВИВАЮЩИХСЯ СТРАН




5-Й ИССЛЕДОВАТЕЛЬСКИЙ ПЕРИОД 2010-2014 Г.

Сектор развития электросвязи

**СВЯЖИТЕСЬ С НАМИ**

| | |
|---|---|
| Веб-сайт: | www.itu.int/ITU-D/study_groups |
| Электронный книжный магазин МСЭ: | www.itu.int/pub/D-STG/ |
| Электронная почта: | devsg@itu.int |
| Телефон: | +41 22 730 5999 |

# ВОПРОС 17-3/2:

## *Ход деятельности в области электронного правительства и определение областей применения электронного правительства в интересах развивающихся стран*

**Исследовательские комиссии МСЭ-D**

Для обеспечения выполнения программы по обмену знаниями и созданию потенциала Бюро развития электросвязи исследовательские комиссии МСЭ-D оказывают поддержку странам в достижении ими своих целей развития. Выступая в качестве катализатора в создании, применении знаний и обмене знаниями в области ИКТ в целях сокращения масштабов нищеты и обеспечения социально-экономического развития; исследовательские комиссии МСЭ-D помогают стимулировать создание в Государствах-Членах условий для использования знаний для более эффективного достижения целей развития.

**Платформа знаний**

Результаты работы, согласованные в исследовательских комиссиях МСЭ-D, и соответствующие справочные материалы используются в качестве исходных документов при реализации политики, стратегий, проектов и специальных инициатив в 193 Государствах − Членах МСЭ. Эти виды деятельности служат также для укрепления базы совместно используемых знаний Членов МСЭ.

**Платформа для обмена информацией и знаниями**

Обмен темами, представляющими общий интерес, осуществляется путем участия в очных собраниях, на электронном форуме, а также путем дистанционного участия в атмосфере, благоприятной для открытого обсуждения и обмена информацией.

**Хранилище информации**

Отчеты, руководящие указания, примеры передового опыта и Рекомендации разработаны на основе вкладов, поступивших для рассмотрения членами комиссий. Информация собрана путем обследований, вкладов и исследований конкретных случаев и доступна для Членов, использующих средства управления информационными ресурсами и веб-публикаций.

**2-я Исследовательская комиссия**

ВРКЭ-10 поручила 2-й Исследовательской комиссии исследование девяти Вопросов в области информационно-коммуникационной инфраструктуры и развития технологий, электросвязи в чрезвычайных ситуациях и адаптации к изменению климата. Основными направлениями работы стали исследования методов и подходов, которые в наибольшей мере соответствуют предоставлению услуг при планировании, разработке, внедрении, эксплуатации, техническом обслуживании и поддержке услуг электросвязи/ИКТ и дают наилучшие результаты, а также повышают ценность этих услуг для пользователей. В этой работе особое значение придается широкополосным сетям, подвижной радиосвязи и электросвязи/ИКТ для сельских и отдаленных районов, потребностям развивающихся стран в управлении использованием спектра, использованию ИКТ/электросвязи для смягчения воздействия изменения климата на развивающиеся страны, электросвязи/ИКТ для смягчения последствий стихийных бедствий и оказания помощи, проверке на соответствие и функциональную совместимость и электронным приложениям, причем основное внимание уделяется приложениям, поддерживаемым сетями электросвязи/ИКТ. Кроме того, работа была сосредоточена на внедрении информационно-коммуникационных технологий с учетом результатов исследований, проводимых МСЭ-R и МСЭ-T, и приоритетов развивающихся стран.

2-я Исследовательская комиссия совместно с 1-й Исследовательской комиссией МСЭ-R участвует в работе по Резолюции 9 (Пересм. ВКРЭ-10) "Участие стран, в особенности развивающихся стран, в управлении использованием спектра".

Настоящий отчет подготовлен многочисленными добровольцами из различных администраций и организаций. Упоминание конкретных компаний или видов продукции не является одобрением или рекомендацией МСЭ. Выраженные мнения принадлежат авторам и ни в коей мере не влекут обязательств со стороны МСЭ.

# Содержание

*Стр.*

*Стр.*



**Рисунки и таблицы**

# ВОПРОС 17-3/2

# Ход деятельности в области электронного правительства и определение областей применения электронного правительства в интересах развивающихся стран

## 1 Введение

### 1.1 Революция в сфере ИКТ и экспансия интернет-приложений

"Интернет меняет все". Это выражение в приближенном виде отражает основные изменения, вызванные применением ИКТ, в частности интернет-технологий. Развитие ИКТ и их широкое распространение и применение оказывают влияние на все аспекты жизни общества. Это называют революцией в сфере ИКТ. Общество, изменившееся в результате революции в сфере ИКТ, называют информационным обществом. Фактическое содержание революции в области ИКТ заключается в процессе преобразования, в формировании информационного общества, а также в том влиянии, которое она оказывает на различные сферы деятельности, включая деятельность коммерческих предприятий и государственных служб. Интернет полностью преобразил форму услуг государственных органов, предоставляемых государственным и глобальным коммерческим предприятиям. То внимание, которое уделяется на национальном уровне приложениям на базе ИКТ во многих странах, отражает веру правительств и граждан в то, что ключевые технологии для электронного правительства станут мощной силой, обеспечивающей эффективное административное управление и надлежащее предоставление услуг населению, создавая конкурентное преимущество в информационном обществе.

### 1.2 Электронное правительство и 2-я Исследовательская комиссия в МСЭ

В рамках Программы 3 МСЭ-D были предприняты исследования, касающиеся приложений электронного правительства, включая современные системы, обеспечивающие предоставление и оплату услуг, в сотрудничестве и партнерстве с частным сектором, а также с другими организациями системы ООН. Для того чтобы воспользоваться потенциальными преимуществами приложений электронного правительства, развивающимся странам необходима информация о стратегиях, передовой практике, источниках знаний и финансовой поддержки, а также о типах приложений электронного правительства и технологических платформ, которые обеспечивали бы максимальные преимущества для их граждан, исходя из потребностей и текущих возможностей каждой страны.

В МСЭ было принято решение об учреждении новой исследовательской комиссии по вопросам электронного правительства, основным исследовательским вопросом которой является оценка прогресса, достигнутого в мире в деятельности, связанной с электронными правительствами, а также определение областей, представляющих наибольшую ценность для развивающихся стран, включая применение мобильных и беспроводных платформ для предоставления и оплаты услуг в сельских и отдаленных районах.

Источниками, обеспечивающими вклад в это исследование, являются: прогресс в ходе исследований по Вопросам, относящимся к данному предмету (аутентификация, секретность и т. д.), проводимых соответствующими исследовательскими комиссиями МСЭ-Т (например ИК13, ИК17), прогресс в реализации инициатив БРЭ, предпринятых совместно с другими организациями

системы ООН и с частным сектором, по услугам и приложениям в области электронного правительства, с акцентом на участие развивающихся стран, прогресс в ходе осуществления любой другой деятельности, осуществляемой Генеральным секретариатом МСЭ или БРЭ, поступающие от Государств – Членов Союза и Членов Сектора отчеты о ходе работы и результаты исследований конкретных ситуаций, касающиеся разработанных инициатив, приложений или технологий, которые могли бы использоваться для предоставления приложений электронного правительства.

МСЭ опубликовал Комплект материалов по внедрению электронного правительства, структуру оценки готовности электронного правительства (2009 г.). В этом комплекте материалов рассматриваются ключевые аспекты среды электронного правительства, чтобы помочь директивным органам в определении приоритетных направлений деятельности, исходя из уровня их готовности и стратегий национального развития. МСЭ также рассмотрел мобильные технологии, чтобы определить последствия для быстро реагирующих правительств и соединенных обществ, и опубликовать отчет "Мобильные услуги правительства" совместно с ДЭСВ ООН и ОЭСР (2011 г.). Отчет, в котором освещаются вопросы обеспечения крайне важного потенциала мобильных технологий для совершенствования государственного управления, содержит углубленный анализ условий для внедрения мобильных услуг правительства, их основных преимуществ и проблем, цепочки создания стоимости и основных заинтересованных сторон, а также контрольный список конкретных мер, направленных на обеспечение того, чтобы политики постоянно контролировали и совершенствовали свои знания в области обеспечения мобильных услуг правительства.

## 1.3 Сравнительные исследования по вопросы электронного правительства в международных организациях

Вопросы электронного правительства рассматриваются в качестве важной программы для обеспечения устойчивого развития развивающихся стран в большинстве международных организаций, включая ООН, ОЭСР, МСЭ, Всемирный банк и региональные банки развития, такие как Азиатский банк развития (АБР) и Африканский банк развития (АФБР). ДЭСВ ООН (Департамент по экономическим и социальным вопросам) с 2001 года проводит регулярные обследования уровня развития национальных электронных правительств, обеспечивая информацию о степени готовности электронного правительства в каждом государстве-члене. В этих целях ООН разработала модель развития электронного правительства, включающую пять основных этапов, каждый из которых характеризуется соответствующими показателями.

В начале 2000-х годов ОЭСР учредила рабочую группу по электронному правительству и опубликовала несколько книг, таких как "Электронное правительство − веление времени" ("E-government Imperative") в 2003 году и "Электронное правительство для лучшего государственного управления" ("E-government for Better Government") в 2004 году, в которых рассматриваются многие основополагающие вопросы, касающиеся электронного правительства. За этими книгами последовало проведение исследований по развитию электронного правительства в отдельных странах, в том числе в Финляндии (2003 г.), Мексике (2004 г.), Норвегии (2005 г.), Венгрии (2007 г.), Нидерландах (2007 г.) и Турции (2007 г.), в рамках которых рассматривались уровень развития электронного правительства и усилия, предпринимаемые каждой страной в этом направлении, а также предлагались рекомендации по политике. Исследование проблемы электронного правительства в рамках ОЭСР было продолжено за счет проведения тематических исследований, на основе которых были подготовлены такие материалы, как "Управление реализацией выгод" ("Benefits Realization Management") и "Электронное правительство как инструмент преобразований" ("E-Government as a Tool for Transformation") в 2007 году, "Экономические основы для оценки затрат и выгод систем управления цифровой идентичностью для услуг электронного правительства" ("An Economic Framework to Assess the Costs and Benefits of Digital Identity Management Systems for E-Government Service") в 2009 году.

Деятельность Всемирного банка в области электронного правительства сосредоточена на оказании помощи странам-клиентам в создании необходимого институционального потенциала для

разработки приложений электронного правительства в целях улучшения показателей деятельности и подотчетности правительств, особенно с точки зрения предоставления государственных услуг. Департамент по глобальным ИКТ Всемирного банка проводит технические консультации и обеспечивает инвестиционную поддержку для разработки и развертывания решений и приложений в области электронного правительства. Это включает стратегические, политические, регламентарные и правовые аспекты, институциональные основы, архитектуру предприятий и стандарты функциональной совместимости, совместные инфраструктуру и службы, управление профессиональной подготовкой и изменениями, приложения в области электронного правительства и инновационные формы финансирования, включая партнерство государственного и частного секторов. Поддержка со стороны Всемирного банка оказывалась таким странам, как Тунис, Монголия, Гана и Руанда.

# 2 Принципы электронного правительства

## 2.1 Что такое электронное правительство?

Концепция электронного правительства появилась в начале 1990-х годов за счет сочетания двух весьма разнородных слов. Одно из них относится к чисто технической терминологии, а другое является весьма популярным в длительной истории системы управления. Хотя новый термин и не был принят легко сразу же после его появления, он вскоре стал обязательной целью большинства стран, пытающихся преобразовать правительство в современную и инновационную структуру. Преобразованное правительство по предположениям футуристов должно было привести к появлению революционной системы управления.

Международные организации, такие как ОЭСР и ООН, дают определение термину "электронное правительство". ОЭСР определяет электронное правительство как применение информационно-коммуникационных технологий (ИКТ), в частности интернет-технологий, в качестве инструмента, способствующего повышению эффективности работы правительства (ОЭСР, 2003 г.). ООН рассматривает его как правительство, применяющее ИКТ для внутренних преобразований и внешних отношений. Конечная цель электронного правительства заключается в том, чтобы обеспечить "надлежащее государственное управление", т. е. поставить правительство в как можно более эффективное и удобное положение, с государственной точки зрения. Его перспективная задача заключается в том, чтобы сформировать основы, на которых ИКТ служили бы одним из ключевых факторов успешного перехода к четкому, прозрачному и эффективному правительству.

Суть электронного правительства состоит в том, чтобы преобразовать государственные административные органы и обеспечить инновационные внутренние и внешние отношения с помощью электронных технологий, указывая на то, что в электронном правительстве акцент должен делаться скорее на "правительство", чем на "электронное", как отмечала ОЭСР (2003 г.). Следуя этой логике, вопросы электронного правительства ставятся в контекст реформы национального государственного управления и инициатив в области надлежащего государственного управления. Электронное правительство подразумевает не просто технические инновации, но и проведение реформы правительства, сосредоточенной на потребностях государственного сектора, с одной стороны, а также граждан и предприятий – с другой стороны, чтобы наверняка обеспечить использование ИКТ в интересах преобразования внутренних операций в рамках правительственных органов, а также методов взаимодействия государственного и частного секторов.

Поскольку электронное правительство направлено на преобразование внутренних процедур ведения деловой активности и поддержания внешних отношений с гражданами, его следует признать как процесс, обеспечивающий перемены по мере изменения функций правительства в соответствии с социальными преобразованиями.

## 2.2 Тенденции развития ИКТ для электронного правительства

### *2.2.1 Характеристики ИКТ для электронного правительства*

В современном технологически развитом мире ИКТ уже стали занимать центральное место в процессе правительственных преобразований. В настоящее время использование правительствами ИКТ носит вполне устоявшийся характер и стало неотъемлемой частью того, как правительства осуществляют свою деятельность. Информационная инфраструктура, в частности интернет-технологии, по своей природе обладают такими характерными особенностями, как открытость, обеспечение подключения, доступность и т. п. Поэтому на национальном уровне ИКТ уделяется внимание как одному из ключевых факторов, способствующих преобразованиям. Вопросы электронного правительства рассматриваются как преобразование правительственных структур и способ взаимодействия между правительственными ведомствами и гражданами. Кроме того, ИКТ являются мощным инструментом, содействующим привлечению граждан к формированию государственной политики. Устранение организационных барьеров, чему способствуют приложения ИКТ, имеет существенное значение для преобразования правительственных структур, чтобы упорядочить и упростить государственные административные органы, а иногда и устранить дублирование. ИКТ также повышают уровень доступности правительственных учреждений для населения, способствуя участию граждан в процессе принятия решений.

### *2.2.2 Сравнение фиксированной и подвижной связи*

В самом начале, когда ИКТ применялись для преобразования правительства, большинство инициатив в области электронного правительства строились на основе интернет-технологий с использованием фиксированной связи. Сделки через интернет осуществлялись в рамках сетей фиксированных линий связи, которые размещались под землей в качестве национальной информационной инфраструктуры. Услуги в области электронного правительства предоставлялись в ограниченных местах по месту жительства или на рабочем месте посредством проводных линий электросвязи. Однако по мере все более широкого распространения технологий подвижной связи[1], мобильный интернет и беспроводной доступ к государственным органам начали оказывать существенное воздействие на среду электронного правительства. Технологии подвижной связи расширяют потенциал государственного сектора, предусматривая использование ИКТ для совершенствования своей оперативной деятельности, а также для взаимодействия с гражданами и предприятиями. В результате этого электронное правительство стало расширяться и постепенно превратилось в мобильные услуги правительства, которые появляются в государственном секторе вместе с приложениями ИКТ нового поколения.

В развивающихся странах уровень доступа к фиксированной широкополосной связи ниже, чем доступ к технологии подвижной связи. Это объясняется высокой стоимостью проводных технологий и инфраструктуры, необходимой для интернета, строящегося на фиксированной широкополосной связи. За счет создания новых и расширенных каналов связи, технологии подвижной связи обеспечивают доступ в районах, где инфраструктура, требуемая для интернета, а также услуги проводной связи не являются экономически обоснованным вариантом (ОЭСР и МСЭ, 2011 г.). Дешевые и готовые к использованию устройства подвижной связи устраняют существующие барьеры для граждан в районах, где представление услуг интернета по линиям фиксированной связи имело весьма ограниченный характер.

[1] Доступ к сетям подвижной связи обеспечивается для 90% населения мира и для 80% населения, проживающего в сельской местности, а в странах ОЭСР темпы совокупного ежегодного роста абонентов широкополосной подвижной связи составили за период с 2007 по 2009 годы 20%. (ОЭСР и МСЭ, 2011 г.).

В то время как технология подвижной связи, с момента ее появления на основе технологии 2G, рассматривалась в качестве слабого средства для обеспечения доступа к широкому кругу информации и услуг, появление смартфонов в связи с созданием сетей 3G и 4G поколений обеспечивает беспрецедентные возможности с точки зрения предоставления государственных услуг гражданам и коммерческим предприятиям. Кроме того, технологии подвижной связи расширяют возможности для связи в реальном режиме времени между правительством и гражданами, что позволяет правительственным должностным лицам понимать потребности граждан и предлагать соответствующие решения с высоким уровнем реагирования. В то же время связь в режиме реального времени позволяет гражданам лучше понять государственные администрации, что расширяет их возможности для привлечения к процессу разработки политики.

### *2.2.3 Подвижная связь и технологии социальных сетей*

В процессе развития ИКТ в связи с инициативами в области электронного правительства, нам необходимо уделять внимание социальным технологиям, позволяющим правительствам активно запрашивать мнение граждан о государственной политике с целью ее совершенствования. Используя действующие в режиме реального времени каналы, такие как фейсбук, твиттер и т. п., которые регулярно посещают граждане, правительства напрямую взаимодействуют с гражданами, а также осуществляют мониторинг того, что говорят люди о проводимых государственных операциях и о предоставляемых услугах. Когда технологии социальных сетей сочетаются с устройствами подвижной связи, их воздействие на государственные администрации усиливается.

Вместо пассивного реагирования на запросы граждан государственные органы могут принимать участие в беседах посредством многочисленных социальных сетей и узнавать, что говорят люди о выполнении правительственных программ. Если в самом начале электронное правительство было представлено на правительственных веб-сайтах, посредством которых просто предоставлялась информация и давались ответы на запросы граждан, то в настоящее время от электронного правительства требуется нечто большее, чем просто пассивно ждать поступления запросов или жалоб со стороны населения. Новое направление прогресса в области ИКТ в сторону технологий социальных сетей открывает новые горизонты для инициатив в области электронного правительства.

### *2.2.4 Открытые правительственные данные как тенденция к повышению прозрачности, подотчетности, участия и сотрудничества правительств*[2]

В последние годы в ряде стран открытые правительственные данные становятся тенденцией. Эта тенденция направлена на создание общественных ценностей совместно с деловыми кругами, гражданским обществом и отдельными гражданами. Такая политическая парадигма строится на основе принципов прозрачности, участия и сотрудничества. Такие изменения культурного характера обеспечивают становление правительства, граждан и других заинтересованных сторон в обществе в качестве партнеров. Ключевые ценности открытых правительственных данных можно резюмировать следующим образом: i) прозрачность: правительство должно предоставлять гражданам информацию о том, чем оно занимается, чтобы обеспечить подотчетность правительства; ii) участие: правительство должно активно использовать знания и консультироваться со всеми слоями общества, чтобы оно могло разрабатывать политику на основе самой широкой информации; iii) сотрудничество: должностные лица правительства должны проводить работу совместно с гражданами и частным сектором и это должно составлять часть их работы, направленной на решение местных и национальных проблем.

[2] Из документа БРЭ.

Информационное общество меняет взгляды на социальные институты и их области подотчетности. Во всем мире правительства все шире раскрывают данные и делятся информацией с гражданами, средствами массовой информации и другими заинтересованными сторонами, реагируя на широко распространенные принципы надлежащего государственного управления, которые лежат в основе достижения целей мира и развития.

Открытые правительственные данные (ОПД) служат одной из основ стратегии открытого правительства. Этот термин означает, что правительственные ведомства предоставляют свои данные в режиме реального времени, чтобы люди могли ознакомиться с ними и обрабатывать их с помощью компьютеров (желательно в виде первичных данных или структурно оформленных данных в открытом формате, позволяющем их машинную обработку, а также с открытой лицензией, позволяющей повторно использовать эти данные третьими сторонами). Общественность может изучать и загружать эти данные и даже проводить новый анализ и создавать приложения на основе этих данных.

ОПД обеспечивают совершенно новые уровни гражданского участия и правительственной подотчетности и прозрачности, что в свою очередь способствует совершенствованию оказания государственных услуг и использования государственных ресурсов. Несмотря на различные вызовы, связанные с "цифровым разрывом" между "странами с различными уровнями развития, который оказывает воздействие на многие соответствующие приложения экономического и социального характера в таких областях, как государственное управление, деловые круги, здравоохранение и образование", правительства во всем мире все шире используют данные и обмениваются ими посредством интернета на национальном, региональном и местном уровнях.

Непреходящая ценность и потенциальные выгоды ОПД представляются достаточно ясными, хотя наше коллективное воображение можно расширить за счет активного обмена идеями и опытом. Это ставит задачи перед правительствами на каждом уровне (национальном, региональном, местном) с точки зрения проведения и поддержания инициатив в области открытых данных в связи с отсутствием понимания выгод со стороны директивных органов и заинтересованных сторон, а также из-за дефицита технических знаний.

Это требует укрепления потенциала государственных служащих, а также заинтересованных сторон в деловых кругах, научном и гражданском обществах, чтобы предпринимать, осуществлять и оценивать инновационные и устойчивые формы опубликования данных. Несмотря на наличие широкого консенсуса об общих благах для общества и демократии, обеспечиваемых повышением прозрачности, подотчетности, участия и эффективности правительств, проведенные недавно исследования также указывают на позитивные последствия для экономики в связи с появлением новых товаров и услуг за счет повторного использования открытых правительственных данных.

В настоящее время применяется широкий набор показателей для оценки деятельности правительства, особенно электронного правительства. Одна из проблем для правительства будущего заключается в разработке и внедрении новой системы показателей для сопоставительного анализа показателей деятельности государственных органов и обеспечения того, чтобы можно было осуществлять мониторинг и совершенствовать инициативы, связанные с участием граждан и открытыми правительственными данными. Настоятельно необходимо обеспечить сравнительный анализ "готовности к преобразованиям" государственных органов, а также совершенствование "общественной ценности" с точки зрения граждан. Инициативы в области открытых правительственных данных, которые в последние годы реализуются во всем мире, недвусмысленно подтверждают тот факт, что заинтересованным сторонам все еще не хватает четкого понимания потенциальных выгод, связанных с этим инструментом, с точки зрения обеспечения прозрачности и подотчетности деятельности правительств, а также содействия распространению этих благ на социальные и экономические результаты.

## 2.3 Компоненты электронного правительства

### *2.3.1 Портал, обмен информацией, безопасность*

Правительственный портал является ключевым компонентом электронного правительства с точки зрения предоставления гражданам и деловым кругам легкого доступа к информации и государственным услугам. Основная идея, связанная с созданием правительственного портала, заключается в том, чтобы обобщить информацию и услуги, которые предоставляются различными ведомствами, и создать единую точку доступа к каждой информации и услуге. Граждане и деловые круги получают более четкую информацию о том, какой сотрудник в каком департаменте и на каком уровне отвечает за ту или иную правительственную информацию и программу. За счет простого взаимодействия с правительством и получения доступа к официальным документам и административным процедурам граждане будут проявлять больше желания участвовать в процессах органов власти, ведущих к моделям более активного участия в государственном управлении, в рамках которого граждане будут принимать более широкое участие в соответствующих процедурах принятия решений. Этот портал служит мощным инструментом для отбора и интеграции значительного объема информации, которой располагает государственная администрация.

По мере эволюции технологий электронного правительства в технологии подвижной связи и технологии социальных сетей, этот портал преобразуется в место, в котором правительство активным образом запрашивает отклики граждан и консультируется со всеми слоями общества, чтобы оно могло принимать решения, отвечающие интересам всех. Государственные служащие могут получать информацию о том, что думают люди о политике правительства. Вместо пассивного реагирования на запросы со стороны, правительственные ведомства ощущают потребности людей, чтобы обеспечивать удовлетворение их требований.

Совместное использование информации представляет собой существенный компонент реализации электронного правительства, который позволяет пересматривать и интегрировать процедуры, обеспечивающие деятельность правительства. Основная идея, связанная с совместным использованием информации, заключается в том, чтобы с первого раза сохранять получаемую информацию, а не запрашивать одну и ту же информацию неоднократно для нужд различных департаментов и ведомств у граждан и предприятий. Граждане могут сокращать количество посещений государственных учреждений, а также количество проверок представляемых документов при обращении за какой-либо услугой.

Совместное использование информации направлено на то, чтобы на основе концепции разового сбора информации правительством у граждан и предприятий этой информацией могли затем пользоваться все департаменты и ведомства. Информация является жизненно важным ресурсом для эффективного управления, осуществляемого правительством. Часто происходит так, что информация об удостоверении личности граждан требуется различным ведомствам, например, для целей налогообложения или замены водительского удостоверения. Бремя, которое возлагается в этой связи на граждан и предприятия, было бы меньше, если бы при взаимодействии с новым департаментом в целях получения какой-либо услуги им пришлось бы лишь представлять дополнительную информацию. Вопросы совместного использования информации включают наличие соответствующей технологии, обеспечивающей такое использование, правовые и институциональные меры, а также организационную культуру, причем последней уделяется значительное внимание, так как нарушения в совместном использовании информацией являются результатом организационного эгоизма, когда информацию рассматривают как источник власти, что приводит к снижению готовности делиться информацией.

Один из наиболее деликатных вопросов, связанных с совместным использованием информации, заключается в возможности вторжения в информацию личного характера и в низком уровне безопасности сетей. В этой связи невозможно переоценить важность обеспечения защиты конфиденциальных данных и безопасности при развитии электронного правительства. Независимо

от того, насколько удобной и эффективной является система, если она не обеспечивает надежной защиты конфиденциальных данных, то она будет сталкиваться с сопротивлением со стороны пользователей, доверие которых будет трудно восстановить. Защита личных данных может быть обеспечена за счет технических, а также правовых, организационных и культурных мер. В то время как совместное использование информации является ключевым компонентом электронного правительства и обязательным условием для продвижения приложений ИКТ, защита информации представляет собой меру, направленную на борьбу со случаями утечки личных данных при совместном использовании информации.

### *2.3.2 Сети, человеческий потенциал*

Высокоскоростные сети представляют собой базовую инфраструктуру для правительственных должностных лиц, обеспечивающую им доступ к базам данных и различным приложениям. Они являются обязательным условием не только для обеспечения взаимного подключения между правительственными органами, например, между центральными и местными правительственными органами, а также между министерствами и ведомствами, но и для того, чтобы граждане и предприятия могли взаимодействовать с правительством для получения информации и услуг. Электронное правительство может оказывать государственные услуги, такие как охрана здоровья и образование, посредством широкополосных сетей. Системы электронного здравоохранения предоставляют дистанционные услуги людям в сельских районах, а системы электронного образования дают возможность учащимся получать дополнительные учебные материалы, которых не оказалось в школе.

Потенциал пользователей для работы с такими установленными системами имеет решающее значение для достижения максимальных выгод от электронного правительства. На раннем этапе внедрения электронного правительства довольно часто случалось, что уровень использования системы был настолько низким, что инвестиции в электронное правительство подвергались критике как расточительные. Есть ряд причин, которые лежат в основе такой критики, в том числе часто упоминалась неспособность граждан пользоваться системой. Обучение населения базовым навыкам работы в интернете, особенно населения отдаленных районов, является очень важным на раннем этапе внедрения электронного правительства. Этот вопрос рассматривался при обсуждении проблемы "цифрового разрыва". Разрывы в уровнях использования услуг электронного правительства иногда связывают с техническими причинами, такими как отсутствие доступного оборудования и подключений к широкополосному интернету, однако отсутствие подготовки человеческого потенциала представляет собой главное препятствие для извлечения максимальной выгоды из внедряемых систем. В любом национальном плане развития ИКТ, охватывающем услуги электронного правительства, содержится настоятельная рекомендация разработать учебные программы по ИКТ для государственных служащих, а также для граждан, особенно проживающих в отдаленных районах.

## 2.4 Виды деятельности в области электронного правительства

### *2.4.1 Приложения: G2G, G2C, G2B*

Сокращения G2G и G2C обозначают "правительство–правительство" и "правительство–граждане", соответственно. G2B обозначает "правительство–бизнес", что весьма близко по форме к G2C с точки зрения особенностей приложений электронного правительства. Приложение G2G представляет собой инициативы электронного правительства, касающиеся вспомогательных операций, в то время как G2C и G2B обеспечивают взаимодействие между правительствами и гражданами, а также деловыми кругами, т. е. основные операции.

Категория G2G содержит инициативы, основная цель которых заключается в обновлении рабочих процессов, таких как установление электронных рабочих процессов, расширение обмена административной информацией, а также реструктуризация процесса ведения деловой активности

на основе оказания услуг. Например, система электронной документации, финансовая система для местного и центрального правительств, система электронной ревизии и т. п. принадлежат к категории G2G.

Категории G2C и G2B включают приложения, обеспечивающие обновление услуг для граждан и деловых кругов. В Республике Корея услуга G4C (правительство для граждан) представляет собой именно этот тип приложения G2C. Кроме того, национальная система социального обеспечения, информационная система по вопросам продовольствия и лекарственных препаратов, а также информационная система по вопросам занятости и поиска рабочих мест служат примерами категории G2C. G2B или служба инноваций для бизнеса включает услугу делового портала, посвященного вопросам корпоративного управления, отраслевой информации, а также оказанию услуг для осуществления различных видов деятельности в течение всего жизненного корпоративного цикла, от начала работы предприятия до ее завершения и закрытия предприятия. Кроме того, информационная система, контролирующая потоки материально-технического обеспечения, иностранные предприятия и т. п., также относится к этой категории. Еще один тип приложения в рамках G2C представляет собой систему, стимулирующую участие граждан в процессе принятия государственных решений, что имеет существенное значение для темы электронной демократии. Эта система направлена на расширение каналов, позволяющих гражданам высказывать свои мнения по конкретным политическим вопросам и взаимодействовать с правительствами на различных уровнях.

### *2.4.2 Финансирование*

Объем средств, требуемых для реализации инициатив электронного правительства, настолько огромен, что для обеспечения их финансирования необходимо подготовить тщательно спланированную схему. Для того чтобы содействовать мобилизации ресурсов на проекты электронного правительства, многие развивающиеся страны опираются на политическое руководство, которое признает огромную важность электронного правительства. Это относится и к опыту Кореи на начальном этапе осуществления национальных проектов в области ИТ. Поскольку было крайне важно в связи с характером информационной технологии показать выгоды от инвестиций в ИТ, правительство Кореи решило откладывать определенную сумму денежных средств исключительно на проекты в области ИТ, осуществляемые на основе распоряжений, издаваемых президентом.

Вопросы финансирования проектов ИТ спровоцировали обсуждение факторов предложения в сравнении со спросом. В научных кругах прекрасно понимают, что с точки зрения стимулирования технологических новшеств и новых приложений политические меры в области спроса широко рассматриваются как более эффективные, чем меры в области предложения. Риск, связанный с нерациональным использованием правительственного бюджета, является высоким, при отсутствии понимания значения фактора спроса. Ключевой вопрос, подчеркивающий значение спроса в рамках проекта, заключается в следующем: какого рода услуги стоят тех громадных инвестиций, которые требуются для проектов электронного правительства? Этот вопрос возникает в связи с возможностью того, что мы можем создать дорогостоящее решение, для которого нет соответствующей задачи.

К сожалению, на этом этапе мы все-таки столкнулись с этой дилеммой. Ряд проектов, связанных с ИТ, создали спрос, который фактически не позволял прогнозировать его вплоть до появления предложения. В результате этой дилеммы первоначальным проектам в области электронного правительства было разрешено следовать в русле идей сторонников концепции предложения. Стратегия сторонников концепции предложения нашла свое отражение в механизме финансирования на раннем этапе разработки электронного правительства, в частности в Корее. Однако нацеленность на идеи концепции предложения не должна перечеркивать значение рассмотрения потенциального спроса на конкретные услуги электронного правительства. Например, при принятии решения о том, какие услуги следует включить в инициативы электронного

правительства, мы можем затронуть аспекты спроса, пересмотрев операции, совершенные между правительством и гражданами в офлайновом режиме.

### *2.4.3 Правовые и институциональные меры*

В процессе подготовки деятельности электронного правительства разработка соответствующего законодательства и нормативно-правовой базы является необходимым условием для успешного электронного правительства, поскольку работа государственной администрации осуществляется строго на основе законодательства. Например, если ранее управленческая деятельность правительства строилась на основе бумажных документов, имеющих юридическую силу, то после создания систем электронного правительства вместо них стали использоваться электронные документы для обеспечения государственной административной деятельности, что потребовало принятия правовых мер в отношении электронных документов. Меры, направленные на юридическое обеспечение, сопровождаются укреплением и координацией соответствующих функций правительства, которые ранее распределялись между различными правительственными учреждениями.

Для того чтобы создать институциональную основу для электронного правительства, необходимо внести изменения в законы и нормативные правовые акты, регулирующие гражданско-правовые вопросы, которые были приняты в офлайновой среде, чтобы обеспечить электронную обработку гражданско-правовых вопросов. Даже после технического внедрения систем электронного правительства методы работы и мышления государственных служащих и граждан не изменятся до тех пор, пока для них не будут разработаны законы и нормативные правовые акты, регулирующие функционирование систем электронного правительства.

Система управления на базе ИТ, обеспечивающая эффективное осуществление деятельности электронного правительства, является важнейшей частью институциональных мер, обеспечивающих укрепление организационной структуры. Поскольку большинство проектов электронного правительства обычно охватывают несколько ведомств, то они весьма уязвимы в связи с воздействием противоречивых вопросов, которые мешают нормальному процессу реализации электронного правительства. Для того чтобы обеспечить координацию действий между соответствующими ведомствами, формируется специальный комитет в целях разрешения разногласий между ними. Членами комитета являются не только представители соответствующих ведомств, но и независимые специалисты, которые, как ожидается, должны занимать нейтральную позицию с целью достижения координации.

# 3 Примеры передового опыта стран-участниц (вклады, представленные в МСЭ-D)

В течение последних трех лет третьего исследовательского периода (2010–2012 гг.) 12 конкретных ситуаций, связанных с инициативами электронного правительства, были представлены на совещании ИК в сентябре. Две конкретные ситуации в отношении Бангладеш были сведены в одну в связи со схожим характером их содержания. Версия с резюме каждого вклада представляется в хронологическом порядке его представления. Полный текст каждого вклада помещен в приложении в конце настоящего отчета.

## 3.1 Проект INV (Деревня, оснащенная информационной сетью) (Республика Корея)

Проект направлен на то, чтобы предоставить возможность населению в отдаленных районах получить доступ к богатому контенту в таких областях, как образование, медицинская информация, сельскохозяйственная квалификация, сокращая тем самым цифровой разрыв между городскими и сельскими районами. Он также обеспечивает потенциал для продажи местной продукции

напрямую клиентам и получения дополнительных денежных средств за счет местного производства. Таким образом, этот проект играет определенную роль в подъеме местной экономики и обеспечении сбалансированного регионального развития на национальном уровне. Предполагается, что обучение населения отдаленных районов базовым навыкам работы с интернетом должно расширить спрос на услуги электронного правительства[3].

- Построение широкополосной интернет-инфраструктуры в сельскохозяйственных и рыбацких деревнях, отдаленных районах и в других местах, далеких от информационной революции, для устранения разрыва между городскими и сельскими районами. Существовала надежда обеспечить прочную основу для электронного правительства и электронной демократии.
- Создание информационного контента, включая онлайновый рынок сбыта местной продукции, для получения практической выгоды и восстановления местной экономики в целях равномерного национального развития.
- Он был также направлен на предоставление местным жителям более легкого доступа к информации об образовании, медицине, культуре и знаниям по сельскому хозяйству путем обеспечения возможности пользоваться интернетом в повседневной жизни.
- В каждой деревне был организован "Комитет по управлению Проектом INV". Комитет определял ключевые вопросы в отношении функционирования информационной деревни. Также поощрялись инициативы по созданию бизнес-модели, которая позволила бы Комитету действовать в качестве самофинансируемой организации даже без правительственной поддержки. Модели деревни, оснащенной информационной сетью, были тщательно разработаны с учетом уникальных местных особенностей и потребностей, а после комплексной оценки их внедрение было распространено на всю страну.
- Одним из важнейших факторов успешной реализации данного проекта является обучение тому, каким образом использовать информационные системы в рамках проекта INV.
- Настоящая программа предусматривает проведение различных мероприятий для повышения понимания общественностью сути проекта INV.
- Проект INV сосредоточен на повышении потенциала местных жителей в области информационных технологий, чтобы они были приспособлены к жизни в условиях быстро меняющегося информационного общества. Например, одна из целей проекта INV заключается в предоставлении местным жителям государственных услуг в онлайновом режиме посредством местного проекта электронного правительства.
- В результате реализации проекта INV были достигнуты следующие результаты. Во-первых, осуществление упомянутых выше инициатив содействовало устранению цифрового разрыва за счет улучшения условий для пользования интернетом такими лицами, страдающими от отсутствия информационного обеспечения, как сельские жители.
- Жители отдаленных районов получили возможность пользоваться этими услугами электронного правительства в результате обучения, которое было обеспечено усилиями проекта INV.
- Кроме того, был подготовлен ряд стимулов, чтобы привлечь людей к проекту INV, таких как включение программы электронной торговли в проект INV, чтобы лица, торгующие товарами посредством электронной торговли, могли получать дополнительную прибыль.

[3] Представлено 14 сентября 2010 года на 1-м собрании ИК2.

- Проект INV, направленный на сужение "цифрового разрыва" в бедных с точки зрения информации областях, таких, например, как сельскохозяйственные и рыбацкие деревни, взят за основу другими государствами.
- Участвующим деревням рекомендуется устанавливать братские отношения с частными компаниями, заинтересованными в развитии деревень посредством проекта INV.
- Во время посещения деревни, оснащенной информационной сетью, представитель Компании Intel (крупнейший производитель микросхем в мире) назвал корейский проект INV беспрецедентным примером распространения цифровых технологий в сельскохозяйственных и рыбацких деревнях.

## 3.2 Корейская онлайновая система проведения электронных закупок (KONEPS), (Республика Корея)

В системе KONEPS в онлайновом режиме осуществляется обработка всех процессов закупок: от объявления тендера, определения победителя, заключения контракта и до осуществления оплаты. Благодаря доступу к государственным системам обмена данными, в системе KONEPS отсутствует необходимость подачи документов в бумажном виде, таких, как свидетельство о регистрации предприятия и свидетельство об уплате налога. В системе переведено в цифровую форму более 160 официальных форм документов для электронной обработки, включая тендерные заявки, контракты, запросы на проверку, запросы на оплату. Поскольку в системе KONEPS предусматривается осуществление оплаты в онлайновом режиме, включая обработку отчета о доставке, а также запросов на проверку и оплату, она может существенно уменьшить время задержки платежей. Это достигается благодаря тому, что каждый отдел, ответственный за договорную работу, осуществление проверок и оплаты, вводит соответствующие индивидуальные задачи в общую систему, оптимизируя, таким образом, процессы оплаты.

Было принято решение о том, что отдельным департаментам не следует разрабатывать отдельную систему электронных закупок. Вместо этого, было предложено разработать стандартную систему с возможностью адаптации под индивидуальные потребности в процессе реализации. В июне 2001 года была принята "Инструкция по предотвращению дублирования разработок" во избежание бюджетных растрат. В процессе внедрения проектов в области электронного правительства пересмотр нормативно-правовой базы играет не менее важную роль, чем процесс построения самой системы электронного правительства[4].

- Технология построения инфраструктуры системы KONEPS предусматривает использование электронной подписи, основанной на инфраструктуре открытых ключей (PKI), применение технологии обеспечения безопасности документации, внедрение стандартов обмена электронными данными, а также построение крупномасштабной веб-службы.
- В системе KONEPS в электронном виде публикуется тендерная информация, поступающая от всех государственных учреждений, таким образом, она выступает в качестве единого окна в сфере государственных закупок.
- Система KONEPS также подключена к казначейской системе правительства, что позволяет учреждениям-заказчикам осуществлять администрирование платежей через фонд электронных платежей.

[4] Представлено 11 сентября 2011 года на 2-м собрании ИК2.

- Служба государственных закупок (PPS) продолжила разработку системы мобильных закупок на основе мобильных телефонов. Учитывая большую популярность смартфонов, спрос на мобильные услуги на рынке закупок вырастет.
- Система KONEPS значительно повысила прозрачность процесса проведения государственных закупок.
- Во время ВКМЭ PPS была названа государственным учреждением, предоставляющим лучшие инновационные услуги с использованием информационных технологий.
- Для того чтобы разработать комплексную систему закупок, был осуществлен пересмотр системы KONEPS с различных точек зрения, таких как услуги, данные и техническая архитектура.
- Кроме того, система KONEPS будет интегрирована с рабочей системой PPS (Службы государственных закупок), чтобы государственные служащие в рамках PPS могли в полной мере воспользоваться преимуществами инициатив в области электронного правительства.
- В настоящее время данные обрабатываются в индивидуальном порядке в зависимости от типа предоставляемых услуг и рабочих процедур в рамках структур PPS.
- Наконец, на основе интеграции услуг в области закупок и приведения в соответствие данных, получаемых в результате операций системы KONEPS, будет осуществлен анализ ее структуры и будет перепроектирована сама система в соответствии с eGovFrame – структурой разработки для стандартов электронного правительства.

## 3.3 Путь Уганды к электронному правительству (Уганда)

Правительство Уганды твердо убеждено, что у ИКТ есть потенциал не только для революционизирования механизмов осуществления правительством своей деятельности, но и для улучшения отношений между правительством и гражданами, правительством и деловыми кругами, а также внутри правительства между правительственными органами. Путь Уганды к электронному правительству берет свое начало с разработки ИКТ-стратегии в 2003 году, в которой основное внимание уделялось необходимости построения ИКТ-инфраструктуры на национальном уровне. После принятия ИКТ-стратегии в 2004 году было проведено общегосударственное исследование по электронной готовности. В 2005 году национальное исследование по электронной готовности было проведено непосредственно в отношении правительства.

В 2006 году при поддержке правительства Китая Уганда начала внедрение инфраструктуры электронного правительства по всей стране. Первый этап охватил все центральные министерства правительства в городах Кампала и Энтеббе, а также в городах Бомбо, Джинджа и Муконо. Возможность использования сети предоставила министерствам доступ к базовым голосовым услугам, а также услугам по проведению видеоконференций и информации.

Предоставление услуг одним министерством другому в настоящее время осуществляется на бесплатной основе. На сегодняшний день такое сотрудничество проводится между четырьмя министерствами в рамках пилотных проектов. Такое сотрудничество предполагает использование ими платформы с одинаковым программным обеспечением. Второй этап охватит восточную, северную и западную части Уганды и будет проводиться до конца 2011 года. Частный сектор также по всей стране развивает ИКТ-инфраструктуру, которая может быть использована для обеспечения функционирования электронного правительства[5].

[5] Представлено 11 сентября 2011 года на 2-м собрании ИК2.

- Были приняты законы, регулирующие киберпространство, а именно: Закон об электронных транзакциях, Закон об электронной подписи и Закон о неправомерном использовании компьютеров. Они должны вступить в силу до конца года.
- Имея необходимую инфраструктуру, Уганда разработала рамочный план по внедрению электронного правительства, в соответствии с которым у всех районных органов власти в стране есть веб-сайт, разработанный в рамках Программы развития сельских коммуникаций (RCDP). Информация о государственных инициативах, инвестиционных и других бизнес-возможностях публикуется на веб-сайтах, несмотря на сложности, с которыми сталкиваются районные органы власти в связи с необходимостью периодически обновлять веб-сайты и осуществлять оплату услуг по веб-хостингу и предоставлению интернета.
- Веб-портал правительства Уганды будет служить в качестве пункта доступа к государственным услугам со ссылками на разделы, которые еще находятся в стадии разработки.
- Министерство ИКТ в сотрудничестве с ЮНИДО открыло пилотные центры бизнес-информации в шести районах (Митяна, Иганга, Лира, Рукунгири, Карнвенге и Бусиа) для улучшения доступа населения к ИКТ-услугам.
- Был построен Национальный центр информации для содействия хранению, пользованию, обмену и обеспечению безопасности информации правительства.
- Большинство инициатив частного сектора основаны на мобильной телефонии, поскольку уровень проникновения мобильной телефонии в Уганде выше уровня проникновения компьютеров или интернета.

## 3.4 Подход Уганды к внедрению широкополосной связи в недостаточно обслуживаемых районах (Уганда)

Комиссия Уганды по коммуникациям (UCC) учредила Фонд развития сельских коммуникаций (RCDF) для стимулирования предоставления услуг электросвязи в сельских и недостаточно обслуживаемых районах. Вышеуказанный фонд предназначен для управления инвестициями в коммуникационную инфраструктуру и услуги в сельских и недостаточно обслуживаемых районах страны.

Это стало признанием того факта, что несмотря на либерализацию этого сектора и открытие его для конкурентной борьбы, некоторые районы страны, остающиеся нежизнеспособными с коммерческой точки зрения, по-прежнему не могли привлечь частный капитал для инвестиций в инфраструктуру и услуги. Главные цели RCDF включают обеспечение доступа к базовым видам услуг в области коммуникации в разумных пределах с точки зрения расстояний; обеспечение эффективных инвестиций в развитие сельских коммуникаций, а также содействие использованию ИКТ в Уганде.

Стратегия Уганды по обеспечению общего доступа (2010 г.) была разработана во исполнение повестки дня по глобальному развитию, Декларации тысячелетия (ЦРТ), подписанной Угандой, а также своего собственного Национального плана развития (2010 г.), который изначально ассоциировался со стратегией национального видения, называвшейся "Видение 2025". Новая стратегия по обеспечению всеобщего доступа была разработана на основе предыдущей стратегии (2001 г.) и с учетом положений, предусмотренных национальными стратегиями в сфере ИКТ и электросвязи Уганды.

Одна из основных причин, по которой интернет не распространен в сельских районах, – это стоимость доступа, недостаточная ширина частоты полос, проблемы с энергоснабжением, а также более важные для сельских сообществ вопросы неграмотности и отсутствия соответствующего местного контента на родном языке. Поэтому новая стратегия ставит главной целью обеспечение предоставления широкополосного подключения и поддержку развития местного контента.

Главное препятствие для развития ИКТ-сектора в Уганде на сегодняшний день – это отсутствие сети широкополосной инфраструктуры, которая предназначена ускорить доступ и использование интернета в частности и внедрение ИКТ в целом. Данная проблема вызвана в основном необходимостью значительных капиталовложений, что не может быть возложено только лишь на частный сектор и, следовательно, требует особых мер со стороны правительства.

Правительство Уганды начало оказывать поддержку построению национальной магистральной информационной инфраструктуры, которая соединит столицы и главные города всех регионов для обеспечения предоставления пользователям широкого спектра экономически эффективных услуг в сфере ИКТ. Как ожидается, данный процесс будет способствовать созданию точек доступа к информации различных учреждений, в первую очередь профессионально-технических учреждений, высших учебных заведений и учреждений среднего общего образования, а также государственных учреждений здравоохранения IV и III уровней. Доступ к широкополосному интернету будет обеспечен на территории определенных субокругов для подключения их к высокоскоростной Национальной магистральной инфраструктуре. Данная инициатива рассматривается как решение "последней мили" для субокругов. В связи с этим проводится глубокое исследование для определения наиболее экономически целесообразных технологических решений (беспроводные, кабельные), которые можно будет реализовать в рамках каждого населенного пункта[6].

- **Электронное правительство**: Данный проект будет способствовать сбору информации, начиная с органов местного самоуправления и заканчивая центральными органами правительства. Информация станет неотъемлемой частью национальной статистики в сфере демографии и других социально-экономических сферах.
- **Электронное образование**: Проект будет способствовать реализации программ в сфере электронного обучения, которое уже становится все более популярным в стране. Так, у крупнейших университетов страны есть студенческие городки, оснащенные спутниковой связью и расположенные в глубине страны, где на сегодняшний день предлагается дистанционное и онлайновое обучение.
- **Электронное здравоохранение**: Проект будет способствовать обеспечению передачи данных, в том числе голосовых, из сельских районов в медицинские учреждения, далее в районные больницы и региональные лечебно-диагностические центры и, наконец, в общегосударственные лечебно-диагностические центры. Будет происходить и обратная передача данных, в том числе голосовых. Как ожидается, обмен данными будет происходить и между головным подразделением Министерства здравоохранения и его местными подразделениями, а также между министерством и медицинскими учреждениями.

Интернет-проникновение, обеспечение доступа к интернету и использование интернета в Уганде все еще находятся на очень низком уровне, покрывая, согласно оценкам, (5%) от общего количества населения. Более того, территория покрытия электросвязью в основном ограничивается городскими коммерческими центрами, что связано с коммерческими соображениями частных провайдеров соответствующих услуг. И хотя предыдущая стратегия Уганды предусматривала создание точек доступа к интернету во всех недостаточно обслуживаемых регионах, скорость и качество услуг широкополосной связи (отключение подачи электроэнергии) остается главной проблемой для конечных пользователей.

[6] Представлено 11 сентября 2011 года на 2-м собрании ИК2.

## 3.5 Информационная система органов местного самоуправления (LGIN)

В Конституции Республики Корея говорится: "Органы местного самоуправления занимаются делами, касающимися благополучия местного населения, управляют государственным имуществом и могут в рамках закона приводить в исполнение законодательные акты, относящиеся к автономности своего образования". На момент реализации проекта существовало 16 органов управления провинций (в том числе семь органов управления городов-метрополий и девять органов управления собственно провинций) и 234 органа местного самоуправления городского и районного уровней. Главы органов местного самоуправления осуществляют управление и контроль над административными вопросами, за исключением случаев, предусмотренных законом. Среди исполнительных функций органов местного самоуправления, делегированных центральным правительством страны, – управление государственной и муниципальной собственностью, эксплуатация и поддержание в надлежащем состоянии объектов инфраструктуры, определение налогооблагаемой базы и сбор муниципальных налогов, а также взимание платы за различные услуги. В состав органов управления провинций входят комитеты по делам образования, которые занимаются вопросами образования, детской и молодежной деятельности в каждом населенном пункте. Органы управления провинций в целом служат в качестве посредников между центральным правительством и органами местного самоуправления (города/района).

- Органы государственной власти испытывают серьезное давление со стороны избирателей, которые требуют снизить издержки на организацию работы государственных служб, улучшить качество потребительских услуг и более эффективно распространять информацию, находящуюся в компетенции соответствующего ведомства.
- Государственным служащим приходится работать в совершенно новой производственной среде в связи с внедрением такой новой системы, как LGIN.
- Стратегия охватывает конкретные ситуации, связанные с бизнес-процессами и службами приложений.
- Это обеспечивает возможность для обмена информацией между правительственными ведомствами, что способствует совершенствованию внутренней оперативной деятельности органов местного самоуправления и совершенствованию формата предоставления государственных услуг.
- Кроме того, отдельные органы местного самоуправления обмениваются друг с другом информацией, благодаря чему сокращается количество документов, необходимых для оказания государственных услуг.
- В результате внедрения системы LGIN упростились многие рабочие процессы, а также были устранены дублирующие друг друга процедуры и должностные обязанности, связанные с оказанием государственных услуг.
- Повышение эффективности работы государственных учреждений ведет к более эффективному оказанию государственных услуг, а также укреплению доверия к государственному аппарату.
- Система LGIN представляет собой информационную инфраструктуру, которая поддерживает все типы государственных услуг.
- Мобильные услуги предоставляются в ограниченных областях приложений.

Система LGIN является необходимой для полноценного функционирования внедряемых центральными органами власти приложений электронного правительства, поскольку разнообразные государственные услуги, предоставляемые на центральном уровне, предположительно будут распространяться по соответствующим каналам органов местного самоуправления.

Факторы, определившие успех вышеописанного проекта, можно считать главным уроком, который следует извлечь из нашего опыта по его реализации. Текущий уровень успеха был достигнут как следствие эффективного решения следующих проблем[7]:

- урегулирование разногласий относительно проекта между заинтересованными сторонами;
- финансирование проекта и распределение затрат между центральным правительством и органами местного самоуправления;
- минимизация психологической нагрузки на тех, кто работает с новой системой, и возможных страхов, связанных с негарантированной занятостью;
- предупреждение значительных убытков вследствие потенциального провала проекта в связи со сложностью реализации и общенациональным масштабом;
- получение поддержки со стороны политических и государственных лидеров с целью создания благоприятных финансовых условий и возможного пересмотра существующего законодательства и т. д.

## 3.6 Обзор услуг, осуществляемых на базе ИКТ, в Бангладеш

Бангладеш является одной из самых густонаселенных стран в мире, при этом занимая одно из последних мест среди стран Южной Азии по плотности сетей электросвязи. Традиционно, лишь сравнительно небольшая часть населения имеет доступ к средствам электросвязи. Еще 10 лет назад уровень плотности сетей электросвязи был ниже 1%, но эра мобильной телефонии изменила ситуацию, и на сегодняшний день плотность сетей электросвязи в Бангладеш составляет 46%.

Общая ситуация в Бангладеш улучшилась в некотором роде благодаря быстрой экспансии рынка услуг мобильной связи. Использование информационно-коммуникационных технологий (ИКТ) в деятельности правительства стало обычным явлением в последние годы.

На сегодняшний день применяются различные технологии для обеспечения возможности реализации уникальных свойств электронного правительства, в том числе обмен электронными данными, интерактивный голосовой ответ, голосовая почта, электронная почта, предоставление веб-услуг, виртуальная реальность, а также для обеспечения функционирования ключевых объектов государственной инфраструктуры.

Электронное управление предусматривает использование информационных технологий государственными секторами для предоставления услуг и информации, содействия демократическому участию граждан в процессе принятия решений путем увеличения открытости и усиления отчетности правительства. Для предоставления гражданам всей необходимой информации из различных правительственных министерств необходимо разработать хороший официальный веб-портал и хранилище информации. Гражданам должны быть доступны для загрузки любые заявления и формы, и для них можно ввести онлайновую систему подачи с целью минимизации бюрократических барьеров. Для обеспечения прозрачности и уменьшения уровня коррупции через данный веб-портал можно также проводить тендерные закупки, подачу налоговой отчетности и распределение земельных участков. Однако следует понимать, что когда речь идет о мобильных услугах правительства, то имеется в виду лишь один из способов электронной

[7] Представлено 17 сентября 2012 года на 3-м собрании ИК2.

коммуникации с правительством, который имеет смысл лишь в том случае, если электронное правительство уже существует[8].

- Электронное управление предусматривает использование информационных технологий государственными секторами для предоставления услуг и информации, содействия демократическому участию граждан в процессе принятия решений путем увеличения открытости и усиления отчетности правительства.
- Продукция и услуги должны продвигаться на глобальный рынок с использованием соответствующих ИКТ-ориентированных технологий в области маркетинговых стратегий.
- Чтобы стимулировать применение ИКТ представителями деловых кругов можно внедрить специализированную корпоративную сетевую линию.
- Онлайновая система биржевой торговли может привлечь большее количество трейдеров из различных секторов к осуществлению деятельности на рынке капитала.
- Правовая система и система здравоохранения также играют важную роль во всех сферах жизни общества.
- Надлежащая система управления отношениями между пациентом и врачом во всех государственных учреждениях здравоохранения улучшит качество услуг в сфере здравоохранения в отдаленных районах.
- Среда в этой "глобальной деревне" меняется, формируется и развивается в соответствии со скоростью интернета.
- Для того чтобы оставаться конкурентоспособным на глобальном рынке, Бангладеш настоятельно необходимо оставаться на этой скорости, реализуя электронное правительство.
- В Бангладеш электронное правительство только развивается, однако "шарик вертится" в сторону интернет-революции.
- В Бангладеш имеются широкие возможности для расширения деятельности электронного правительства.

Цифровая Бангладеш – это постоянный процесс развития. Устойчивая и надежная общенациональная сетевая инфраструктура ускорит процесс информатизации государства, и, таким образом, устранит "цифровой разрыв" между сельскими и городскими районами. Преимущества децентрализации и цифрового правительства могут быть доступны всем гражданам.

## 3.7 Реализация электронного правительства в Кыргызской Республике – опыт и дальнейшие шаги

Правительство Кыргызстана занимает весьма активную позицию, отмечая очень большое значение информационно-коммуникационных технологий (ИКТ) как одного из инструментов, обеспечивающих более высокие темпы развития страны. Среднесрочная стратегия национального развития (2012−2014 гг.) и Специальная программа правительства "Стабильность и достойная жизнь" четко указывают на высокий спрос на внедрение электронного правительства в стране для управления электронными преобразованиями, которые будут отвечать потребностям рядовых граждан. В настоящее время в органах государственной администрации Кыргызской Республики отмечается удовлетворительный уровень компьютеризации, особенно в ведомствах центрального правительства. В большинстве министерств, которые обрабатывают огромные объемы информации,

[8] Представлено 17 сентября 2012 года на 3-м собрании ИК2.

имеются специальные серверы, содержащие базы данных, системы электронной почты, обеспечивающие доступ к интернету и оказание других услуг, либо даже имеются департаменты, отвечающие за обработку данных и управление ими. Многие министерства и административные правительственные органы разрабатывают свои собственные местные сети и информационные системы с доступом к интернету.

Правовые рамки, связанные с электронным правительством в Кыргызской Республике, являются вполне достаточными и включают 16 законов в области ИКТ. Вместе с тем необходимо разработать и принять дополнительные законы, чтобы открыть дверь для дальнейшего обеспечения электронных услуг и обмена информацией в стране (например, Закон об электронной коммерции, обеспечение единых технических стандартов и требований).

В 2002 году Кыргызская Республика приняла Национальную стратегию и План действий "Информационно-коммуникационные технологии для развития Кыргызской Республики" на 2002−2010 годы. Оценка реализации этой стратегии, проведенная ПРООН в 2007 году, показала, что было достигнуто лишь 30% результатов.

Кыргызстан уже признал важность обеспечения доступа к современным технологиям и услугам для граждан и предприятий. Электронное правительство и электронные услуги предоставят возможность государственной администрации использовать информационные технологии для более качественного оказания услуг гражданам, коммерческим предприятиям и другим участникам процесса управления[9].

- **Министерство финансов** Кыргызской Республики выступило в 2012 году с рядом электронных инициатив, касающихся прозрачности бюджета (www.okmot.kg), таких как: "Прозрачный бюджет" (http://budget.okmot.kg) – автоматизированная система для представления данных о поступлениях и расходах в рамках центрального и местных бюджетов. Впервые в истории страны рядовые граждане и юридические лица получают свободный доступ к детальной информации о выполнении государственного бюджета. Представляемые данные включают подробную информацию, начиная с уровня отдельных получателей до правительственных ведомств и регионов. Эти данные обновляются в онлайновом режиме посредством электронного подключения к базе данных Центрального казначейства; электронной системе государственных закупок (http://zakupki.okmot.kg) – автоматизированной системе по государственным закупкам, которая включает услуги онлайновой регистрации, участия в торгах, а также другую соответствующую информацию и меры. Составление онлайновых экономических карт (http://map.okmot.kg) – электронная карта Кыргызской Республики, показывающая все социально-экономические данные по каждому географическому месту страны;
- **Национальный статистический комитет** Кыргызской Республики проводит активную работу по осуществлению электронного сбора и анализа статистических данных. Это ведомство разработало и утвердило свою корпоративную стратегию развития ИКТ до 2020 года.
- **Налоговый комитет, Управление таможенной и пограничной службы** представляют собой государственные ведомства, которые активно применяют в своей работе электронные инструменты (электронные декларации, межведомственный обмен электронными данными, и т. п.).
- **Социальный фонд, Фонд обязательного медицинского страхования**, **Министерство здравоохранения** и **Министерство социального развития** активно совершенствуют свои

[9] Представлено 17 сентября 2012 года на 3-м собрании ИК2.

отраслевые информационные системы и базы данных для оказания электронных социальных услуг и межведомственного обмена данными.

- **Министерство юстиции**, **Министерство внутренних дел** приступили к внедрению потока электронной документации в рамках министерств и инструментов программного обеспечения для своих систем управления людскими ресурсами.
- **Министерство иностранных дел** начинает процесс внедрения электронных виз и электронной документации.

Практический опыт внедрения различных отраслевых проектов электронных услуг показал, что правительство должно играть ведущую роль в содействии ИКТ для обеспечения развития страны на национальном уровне. Отсутствие координации усилий в этой области может стать причиной дублирования усилий и неэффективного использования ресурсов, предоставляемых донорами и самим правительством. Отсутствие надлежащей координации действий между ведомствами ведет к дополнительным трудностям в области электронного взаимодействия. Создание эффективного координационного органа по ИКТ и разработка национальных стандартов электронной функциональной совместимости, а также единообразной комплексной инфраструктуры для электронных услуг имеют решающее значение для успешного внедрения электронного правительства в Кыргызской Республике.

## 3.8 Деятельность по обеспечению более удобного доступа к административной хозяйственной системе с использованием мобильных терминалов при сотрудничестве служб в Японии

"Новая стратегия в области дорожных карт информационно-коммуникационных технологий (ИКТ), разработанная Стратегическим штабом по пропаганде передового общества информационно-коммуникационных сетей, представляет следующие цели, касающиеся программ диверсификации методов доступа к административным услугам относительно обновления правительственного портала и стимулирования населения к обращению к правительственным службам; в 2011 году разработка, испытания и демонстрация мобильного доступа к административным услугам при аутентификации посредством мобильных телефонов; в 2012–2013 годах, на основании демонстрации, внедрение, развитие и содействие распространению услуг частично в испытательных районах на основании вышеупомянутой демонстрации и постепенное развертывание в общенациональном масштабе; к 2020 году введение электронных административных услуг, чрезвычайно удобных в использовании, – "службы одного окна".

На основании этой программы Министерство информации и связи (MIC) осуществило "Проект по содействию развитию совместных хозяйственно-административных систем (проверка способов повышения удобства использования мобильных телефонов как средства доступа)" в 2011 году на базе результатов "Исследования и обследования диверсификации методов доступа к электронным административным услугам и т. д. (исследование и изучение технологии доступа к электронным административным услугам с помощью мобильных телефонов и т. д.)", проведенного в 2009 году.

Мобильные терминалы с функциями NFC (связь в ближнем поле) будут распространяться на коммерческой основе в 2012 году. Они дают возможность помещать в автономном и онлайновом режиме в устойчивые к взлому устройства личную информацию пользователей услуг, такую как логины/пароли, пункты и купоны, а также считывать эту информацию. Применение этих функций делает удобнее аутентификацию пользователей при доступе к услугам электронного правительства через мобильные терминалы, и все граждане, независимо от поколения, к которому они принадлежат, получают легкий и безопасный доступ к административным службам через мобильные терминалы.

В ходе проводившихся MIC в 2009 году исследований изучалась безопасность следующих мест хранения идентификационной информации, получаемой пользователями от поставщиков услуг в

качестве средства мобильного доступа к услугам электронного правительства: 1) открытая система карт с интегральной схемой (IC), используемая посредством помещения открытой идентификационной карты, выданной правительством, вблизи мобильного телефона, 2) открытая система карт для мобильных телефонов, используемая путем ввода соответствующих карт, выдаваемых правительством, в мобильные терминалы, 3) открытая система идентификационной информации, используемая путем занесения выдаваемой правительством информации в мобильные терминалы, и т. д. Устойчивыми к взлому устройствами считаются: 1) полномерные карты с интегральной схемой для открытой системы идентификационных карт; 2) устройства флеш-памяти, содержащие интегральные микросхемы для открытой системы карт для мобильных телефонов; 3) UICC (универсальная карта с интегральной схемой) для открытой системы идентификационных карт.

До проведения вышеуказанного исследования для хранения и использования идентификационной информации и пользовательской информации в устойчивых к взлому устройствах требовалось разработать и эксплуатировать приложение для мобильных телефонов (далее – мобильное приложение) для каждого поставщика услуг. К тому же пользователям нужно было загружать и устанавливать отдельные мобильные приложения, предоставляемые поставщиками услуг. Другими словами, при предоставлении устойчивого к взлому устройства неудобства испытывают и поставщики услуг, и пользователи. Для создания удобных для пользователей условий, в которых было бы несложно работать поставщикам услуг, мы рассмотрели технические спецификации для создания системы мобильного доступа.

Для преодоления этих трудностей мы изучили систему, которую могли бы совместно использовать и пользователи, и поставщики услуг. Другими словами, мы изучили технические спецификации системы мобильного доступа, которая состоит из серверов для хранения и безопасного прочтения, не относящихся к отдельным поставщикам услуг, и мобильного приложения, сообща используемого всеми услугами для хранения и использования идентификационной информации в устойчивых к взлому устройствах. Далее проводятся проверка опытным путем технических спецификаций, определение проблем в свете установки и эксплуатации, и изучаются варианты решения проблем.

Все больше людей в развивающихся странах приобретают мобильные терминалы, и в этих странах также растет число пользователей смартфонов. Для развивающихся стран также необходимо предусмотреть область оказания государственных услуг[10].

## 3.9 Электронное правительство в Ливане

В основе дорожной карты электронного правительства лежит твердая приверженность нашего правительства создать портал электронного правительства для совершенствования и упрощения доступа граждан к государственным услугам и общественной информации.

В концепции стратегии электронного правительства основное внимание уделяется достижению следующих стратегических целей: правительство, для которого главным являются граждане (а не бюрократия), которое ориентируется на результаты, опирается на рынок (активно содействуя инновациям), осуществляет благое управление, обеспечивает экономическое развитие и социальную интеграцию[11].

[10] Представлено 17 сентября 2012 года на 3-м собрании ИК2.

[11] Представлено 17 сентября 2012 года на 3-м собрании ИК2.

- Электронная реформа: открывает идеальную перспективу изменить структуру правительственных процедур, чтобы воспользоваться технологией и использовать ИКТ как направляющую силу процесса реформирования.
- Электронные граждане: объединяет все услуги, которые правительство в настоящее время оказывает гражданам Ливана и которые планируется предоставлять в электронном виде.
- Электронный бизнес: основное внимание уделяется тем правительственным услугам, которые важны для ливанского бизнес-сообщества и иностранных инвесторов. Более эффективное предоставление этих услуг будет содействовать росту частного сектора в Ливане и развитию национальной экономики.
- Электронное сообщество: широко признается, что ИКТ имеет ключевое значение для участия в возникающем обществе, основанном на знаниях, имеет огромный потенциал ускорения экономического роста, содействия устойчивому развитию, расширению прав и возможностей и сокращению масштабов нищеты.
- Инициатива электронного правительства в различных областях, таких как право, инфраструктура ИКТ, вертикальные приложения и различные национальные стандарты и направления политики.

Дорожная карта электронного правительства определяется как комплекс макромер и важнейших вех в различных областях, таких как правовая, административная, инфраструктурная, реструктуризации хозяйственных процессов, функциональной совместимости и портала электронного правительства. Эта дорожная карта будет поддерживаться планом создания потенциала, который даст государственным служащим возможность эффективно и действенно применять все проекты электронного правительства.

Следующим этапом будет подготовка различных законопроектов, решений и технических проектов, которые могло бы принять правительство Ливана, например:

- проект закона – электронные сделки;
- законопроект – закон о шкале заработных плат в сфере ИТ;
- принятие закона об электронных сделках;
- упрощение процедур.

## 3.10 Проект MWANA (Замбия)

Роль и влияние ИКТ в Замбии быстро растут благодаря социальным факторам и активному развитию технологий ИКТ. Согласно проведенному ZICTA обследованию использования ИКТ, в Замбии, население которой составляет 12 миллионов, 7,8 миллиона человек имеют доступ к подвижной связи, а 4 миллиона – к интернету. Повышение спроса населения на услуги и рост использования ИКТ побуждают правительство и частный сектор к инновациям и серьезным капиталовложениям в транзитные линии электросвязи[12].

- Укрепить потенциал ранней диагностики у младенцев с целью как увеличения числа матерей, уведомляемых о результатах, так и обеспечения более оперативного и эффективного доступа к матерям с использованием SMS-приложения (мобильное здравоохранение).
- Повышать показатели послеродового обслуживания, увеличивать число регистрации рождений по родам в клиниках и местных сообществах, при этом повышая число посещений

[12] Представлено 17 сентября 2012 года на 3-м собрании ИК2.

врача матерями посредством связи с медико-санитарными работниками местного уровня через приложение "RemindMi".

- Совершенствовать предоставление гражданам правительственных услуг.
- Сокращать бюрократическую волокиту и время, требующееся для предоставления правительственных услуг.

Применяемые технологии и решения:

- Технология SMS – мощная инновация, которая в Замбии позволила сократить задержки в получении результатов ранней диагностики детей младшего возраста (результаты анализов сухой капли крови на ВИЧ), улучшить связь между поставщиками услуг здравоохранения и добровольцами в местных сообществах, и, что еще важнее, стимулировать пациентов возвращаться в клинику за результатами анализов с бóльшим доверием.
- Технология RapidSMS – применяется для ранней диагностики ВИЧ у детей младшего возраста. Сообщения SMS используются для отправки результатов анализов на ВИЧ из лабораторий, где эти анализы обрабатываются, работникам клиник, где собираются образцы. Результаты поступают на телефоны в небольших клиниках и на SMS-принтеры в крупных клиниках. Система также отслеживает образцы и осуществляет мониторинг в режиме реального времени для провинциальных и районных служащих.
- RemindMI – позволяет отслеживать местоположение пациентов при послеродовом уходе. Сообщения SMS направляются располагающимся в местных сообществах агентам, которые вызывают матерей с младенцами и просят их посетить клинику через шесть дней, шесть недель и шесть месяцев после родов или в особых обстоятельствах, таких как получение клиникой результатов анализов.

Был разработан национальный план расширения деятельности, который начинается с подготовительного этапа, а затем переходит в итеративную фазу, в рамках которой происходит профессиональная подготовка работников клиник и включение их в систему, а также оценка проблем и результатов этого включения. Цель заключается в достижении общенационального охвата к 2015 году, при предоставлении учреждениями здравоохранения услуг по ранней диагностике детей младшего возраста. На подготовительном этапе основное внимание будет уделяться укреплению технической, физической, мониторинговой и человеческой инфраструктуры, чтобы дать системе возможность справиться с факторами масштаба. На протяжении всего процесса расширения будет вестись тщательный мониторинг проекта, чтобы обеспечить положительное воздействие системы на целевые задачи в сфере здравоохранения.

## 3.11 Услуги электронного правительства в Черногории

Понимая значение развития и применения ИКТ, Черногория в прошлом сделала значительные шаги в этом направлении. Это ясно показывает составленный Всемирным экономическим форумом рейтинг – Индекс сетевой готовности (NRI), в котором Черногория занимает 44-е место из 138 стран, располагаясь значительно выше других европейских стран в регионе. Проникновение пользователей сетей подвижной связи составляет почти 200%, а проникновение пользователей интернета постоянно растет, поэтому очевидно, что сектор ИКТ в Черногории активно растет[13].

- Устойчивость ИКТ – программы: основы ИКТ (технологические принципы, основы радиочастотного спектра, основы защиты потребителей), инфраструктура ИКТ, правовые и регуляторные рамки, информационная безопасность для совершенствования

[13] Представлено 17 сентября 2012 года на 3-м собрании ИК2.

инфраструктуры широкополосной связи, правовые и регуляторные рамки, предназначенные для создания конкурентоспособного и устойчивого сектора ИКТ.

- ИКТ для общества – программы: электронное образование, электронное здравоохранение, вовлечение в деятельность в электронной форме, с целью поощрения всех членов общества к использовании современной технологии.
- ИКТ в государственной администрации – программа: электронное правительство, в рамках которой основное внимание уделяется поощрению государственной администрации к инновационному использованию информационно-коммуникационных технологий для повышения качества услуг, предоставляемых органами государственной власти.
- ИКТ для экономического развития – программа НИОКР и инновационных ИКТ для развития научно-исследовательской деятельности с целью создания производительных и устойчивых систем ИКТ посредством составления базы данных кадрового потенциала, поощрения творческого начала и предпринимательства.
- Для внедрения электронного правительства в Черногории Министерство информационного общества и электросвязи осуществляет проект портала электронного правительства – www.euprava.me, далее именуемого "портал", посредством которого все учреждения государственной администрации и органы местного самоуправления будут в электронной форме предоставлять услуги частным лицам и предприятиям, а также другим учреждениям.
- eDMS (Система управления электронной документацией) – проект, основной целью которого является информатизация и электронизация хозяйственных подразделений в правительстве Черногории для повышения эффективности, экономии времени, сокращения затрат и повышения качества управления документацией.

В будущем усилия будут сосредоточены на Основах функциональной совместимости, которые по природе своей не являются техническим документом и предназначаются для тех, кто занимается определением, разработкой и предоставлением государственных услуг.

Хотя предоставление государственных услуг практически во всех случаях связано с обменом данными между информационными системами, функциональная совместимость представляет собой более широкое понятие и включает возможность организации совместной работы по имеющим общее положительное воздействие и взаимно согласованным целям.

# 4 Инструменты для передачи передового опыта

## 4.1 Комплект материалов для услуг на базе ИКТ с использованием подвижной связи

[14]В комплекте материалов по созданию услуг на базе ИКТ описываются использование подвижной связи для услуг электронного правительства и способы интеграции всех услуг на базе подвижной связи, которые требуют аутентификации и безопасного соединения, таких как мобильные услуги электронного правительства, мобильные платежи, мобильный банкинг и мобильное здравоохранение. В этой части отчета описываются общие принципы создания таких услуг и упоминаются Рекомендации МСЭ-Т, связанные с аспектами безопасности этого процесса.

[14] Эта часть представляет собой краткое изложение вклада компании Intervale, который полностью приведен в Дополнении.

- Подвижная связь, наряду со своей основной функцией – голосовой связью и передачей информации между пользователями, оказалась исключительно полезной для дополнительных приложений, таких как мобильная коммерция (m-commerce), мобильное здравоохранение (m-health), мобильные услуги правительства (m-government) и т. п., где "m" означает "mobile". Вместе с тем следует понимать, что мобильные услуги правительства – это лишь одна из различных форм электронной связи с правительством, и это же относится к мобильному здравоохранению, мобильному образованию, мобильной коммерции и мобильным платежам.

Хотя у мобильных телефонов небольшие дисплеи и клавиатуры, ожидается, что они будут широко использоваться для услуг электронного правительства. Происходящее в настоящее время стремительное развитие подвижной связи и ее существенные преимущества делают электронные услуги на базе мобильных терминалов, именуемые мобильными услугами (*мобильные услуги правительства, мобильное здравоохранение, мобильные платежи, мобильное обучение и т. п.*) весьма перспективными, поскольку:

- не у каждого гражданина есть персональный компьютер, но почти у всех есть мобильные телефоны (согласно Отчету МСЭ "Тенденции в реформировании электросвязи, 2012 год", к концу 2011 года в мире насчитывалось 6 млрд. абонентов подвижной связи, а пользователей интернета было почти в два раза меньше);
- мобильные телефоны всегда при своих владельцах и всегда включены;
- в некоторых случаях единственный вид связи – подвижная связь;
- подвижная связь защищена не хуже, чем интернет.

### *4.1.1 Мобильные принципы для безопасных мобильных услуг*

Мобильная система для предоставления защищенных дистанционных услуг, будь то мобильные услуги электронного правительства, мобильная медицина или мобильная коммерция, в целом должна обладать инфраструктурой для защищенной передачи блоков данных между пользователями мобильных терминалов и поставщиками услуг. Для гарантии безопасности эта структура должна обладать элементом, который обеспечивал бы аутентификацию и кодирование. Передаваемые блоки могут содержать конфиденциальную информацию, которая требует защищенного обращения. Обмен данных должен производиться только между имеющими допуск пользователями, быть недоступным третьим сторонам и должным образом заноситься в журнал учета, дабы избежать отказа от авторства. Аутентификация пользователей должна быть многофакторной.

### *4.1.2 Идентификация и аутентификация*

Для идентификации требуется подтвердить идентичность клиента и однозначно привязать мобильное устройство клиента к его учетной записи в базе данных поставщика услуг. После первоначальной идентификации клиента ему следует выдать "секретный ключ", который будет аутентифицировать пользователя при его взаимодействии с поставщиком услуг в будущем. Этот "секретный ключ", также называемый "мобильной подписью", является одним из факторов аутентификации. Мобильная подпись практически является уникальным криптографическим ключом, который может также использоваться для кодирования информации. Таким образом, использование ключей обеспечивает как кодирование данных, так и аутентификацию сторон. Вторым фактором многофакторной аутентификации может быть PIN-код или пароль пользователя, дающий доступ к установленным в телефоне приложениям. Этот PIN-код защищает от несанкционированного использования приложений.

В существующих системах мобильных платежей уже имеются процедуры обеспечения безопасности, и требования к безопасности определяются соглашениями между поставщиками услуг и их клиентами. Очевидно, что для электронного правительства требуется система

безопасности, которая контролировалась бы государством и соответствовала национальным правовым положениям, относящимся к электронным подписям. Эта система должна обеспечивать безопасную передачу конфиденциальной информации между государственными учреждениями и имеющими допуск пользователями, предоставляя при этом электронные подписи. Ту же систему можно использовать для услуг электронного здравоохранения и других созданных в последнее время услуг, требующих защиты данных. И хотя частные системы мобильных платежей, вероятно, будут иметь собственные средства защиты, не следует исключать сложных решений, обеспечивающих централизованную аутентификацию в едином центре, а некоторые поставщики услуг (скорее всего, финансовых) дополнительно используют собственные процедуры кодирования и проверки. Таким образом, в мобильных приложениях представляется разумным иметь несколько независимых блоков с различными наборами ключей. На Рисунке 2 показана единая модель аутентификации для мобильных устройств и интернет-устройств.

Несмотря на наличие множества центров идентификации и аутентификации, все они должны использовать единые правила выдачи глобальных мобильных идентичностей пользователя– mID, зарегистрированных в центральной директории системы для обеспечения надлежащего направления сообщений клиентам. У клиента может быть несколько mID, но они должны быть привязаны к его MSISDN.

Инструмент предоставления услуг обеспечивает технологическую поддержку и играет в этой структуре весьма важную роль. Помимо интеграции различных средств доступа, обеспечения функциональной совместимости с поставщиками услуг и центром аутентификации, инструмент предоставления услуг также снабжает пользователей приложениями для средств доступа (персональных компьютеров и мобильных терминалов).

Все центры идентификации и аутентификации должны соблюдать одни правила и нормы распределения для глобальных идентификаторов мобильных клиентов (mID), регистрируемых в центральной директории системы для обеспечения доставки сообщений клиентам.

### *4.1.3 Административное управление ключами*

Криптография может использоваться как с симметричными, так с асимметричными ключами для кодирования передаваемых данных и создания мобильных подписей. Преимущество симметричных ключей (стандарты 3DES, AES) заключается в использовании алгоритмов, которые легко применять в недорогих вычислительных устройствах. Генерация симметричных ключей является простой операцией, не требующей каких-либо специальных средств. В то же время по определению использование одного ключа совместно пользователем и поставщиком услуг (центром аутентификации поставщика) может привести к ситуации, когда пользователь оспорит совершенную сделку. Справедливо будет отметить, что в системах мобильных платежей успешно используется криптография с симметричными ключами, поскольку удалось создать надежные системы занесения сделок в журналы учета на случай споров.

При криптографии с асимметричными ключами применяется инфраструктура открытых ключей (PKI) для связи двух различных ключей, которые принадлежат одному лицу: "открытый" ключ с открытой идентичностью и "личный" ключ, который хранится в безопасности и защищен от несанкционированного доступа (например, на SIM-карте или специальной защищенной смарт-карте). Математическое взаимодействие между ключами осуществляется таким образом, что действие, совершаемое одним ключом, может быть "привязано" к другому ключу без раскрытия данных личного ключа. Это особенно полезно для создания электронной подписи, поскольку акт подписания, совершаемый личным ключом, идентифицирует владельца личного ключа только по взаимосвязи с соответствующим открытым ключом – идентичность последнего известна. Важнейшая задача технологии PKI заключается, с одной стороны, в обеспечении "конфиденциальности" личных ключей, а с другой стороны – в проверке взаимоотношений между открытыми и личными ключами. Это обеспечивается тщательным управлением процессом регистрации при выдаче ключей и процессом сертификации, подтверждающим идентичность

открытого ключа. Управление этими элементами осуществляется, соответственно, структурами, известными как органы "регистрации" и "сертификации" (RA и CA). Применительно к мобильной подписи их основная функция заключается в признании однозначного соотношения между использованием личного ключа и зарегистрированной идентичностью гражданина ввиду его собственности на соответствующий открытый ключ.

Для применения методов асимметричного кодирования требуются более дорогие вычислительные устройства, но они могут использоваться в различных схемах взаимодействия. Использование "двойного ключа" дает возможность большей масштабируемости и более простого разрешения конфликтов. Этот подход дает более эффективную модель доверия при упрощенном административном управлении и услугах (так, несколько различных приложений и схем взаимодействия могут поддерживаться одной асимметричной парой ключей). Вследствие этого документы, в которых говорится об основах глобальной функциональной совместимости для электронной подписи, почти всегда посвящены методам асимметричного криптографического кодирования.

### *4.1.4 Безопасность*

Наиболее важным требованием для платежных систем, как и для электронного правительства и электронного здравоохранения, в том числе их мобильных вариантов, является безопасность, обеспечиваемая при соблюдении Рекомендаций Сектора стандартизации электросвязи МСЭ, который выпустил пособие под названием "Безопасность в электросвязи и информационных технологиях". В пособии приводится обзор существующих стандартов МСЭ-Т и их практического применения в безопасной электросвязи. Стандарты МСЭ-Т не имеют обязательной силы и являются рекомендациями, но соблюдение рекомендаций необходимо для обеспечения совместимости и стабильности систем электросвязи различных стран.

Поскольку в этих системах участвуют множество субъектов, аспекты безопасности можно разделить на несколько категорий, которые включают:

a) безопасность оконечных точек;

b) безопасность мобильных приложений;

c) безопасность сетей подвижной связи;

d) идентификация запрашивающей стороны, включающая надлежащую идентификацию лица, запрашивающего финансовую сделку.

До наступления эры смартфонов операторам было относительно просто управлять мобильными приложениями на мобильных телефонах. По сути операторы контролировали то, какие приложения можно загрузить в устройство и каковы его характеристики безопасности. Управление мобильными приложениями усложняется с появлением смартфонов и возможности свободно скачивать приложения третьих сторон. Сейчас практически невозможно быть полностью уверенным, что все приложения, работающие в мобильном устройстве, происходят из заслуживающих доверия источников. В результате пользователи мобильных телефонов подвергаются дополнительным угрозам, например кражи идентичности, "фишинга" и потери персональных данных.

Должным образом разработанные и осуществленные измерения безопасности поддерживают политику безопасности, которая определена для конкретной сети, и упрощают выполнение правил, установленных управлением безопасностью.

Измерение безопасности – управление доступом – защищает от несанкционированного использования сетевых ресурсов. Управление доступом гарантирует, что только уполномоченному персоналу или устройствам разрешен доступ к элементам сети, хранимой информации, потокам информации, услугам и приложениям. Кроме того, управление доступом на основе ролей (RBAC) обеспечивает различные уровни доступа для гарантии того, чтобы люди и устройства могли

получать доступ и совершать операции только с теми элементами сети, с той хранимой информацией и с теми потоками информации, доступ к которым им разрешен.

Измерение безопасности – аутентификация – предназначено для удостоверения идентичностей поддерживающих связь объектов. Аутентификация гарантирует подлинность заявляемой идентичности объектов, участвующих в связи (например, человека, устройства, услуги или приложения), и гарантирует, что объект не пытается осуществлять подмену или неправомочно воспроизвести предыдущий сеанс связи.

Измерение безопасности – предотвращение отказа от авторства – обеспечивает средства для предотвращения со стороны индивидуума или объекта отрицания выполнения конкретного действия, связанного с данными, обеспечивая наличие доказательств совершения различных действий, связанных с сетью (таких как доказательство обязательства, намерения или готовности; доказательство происхождения данных, доказательство собственности, доказательство использования ресурса). Предоставляются данные, которые могут быть предъявлены третьей стороне и которые могут использоваться для доказательства того, что некоторое событие или действие имело место.

Измерение безопасности – конфиденциальность данных – защищает данные от несанкционированного раскрытия. Конфиденциальность данных гарантирует, что содержание данных не может быть понято объектами, которые не имеют к ним доступа. Кодирование, списки контроля доступа и разрешение доступа к файлам – это методы, которые часто используются для обеспечения конфиденциальности данных.

Измерение безопасности – безопасность связи – гарантирует, что информация передается только между уполномоченными оконечными точками (информация не изменяет направления и не перехватывается при передаче между этими оконечными точками).

Измерение безопасности – целостность данных – гарантирует правильность и точность данных. Данные защищены от несанкционированного изменения, удаления, создания и дублирования, а также обеспечивается обнаружение такой несанкционированной деятельности.

Измерение безопасности – доступность – гарантирует отсутствие какого-либо ограничения на санкционированный доступ к элементам сети, хранимой информации, потокам данных, к услугам и приложениям из-за событий, влияющих на сеть. В эту категорию включены варианты восстановления после аварий.

Измерение безопасности – секретность – обеспечивает защиту информации, которая могла бы быть получена, исходя из наблюдения сетевой деятельности. Примеры такой информации – веб-сайты, которые пользователь посетил, географическое расположение пользователя, IP-адреса и имена DNS устройств в сети поставщика услуг.

### *4.1.5 Мобильные технологии*

В настоящее время термин "подвижная связь" чаще всего связывается со стандартом GSM второго и третьего поколений. Эти системы подвижной связи используют различные подсистемы для передачи голоса и данных (с применением технологий коммутации с временным разделением каналов и коммутации пакетов) и представляют собой промежуточный шаг в развитии подвижной связи. Сети последующих поколений (СПП), которые уже появились на смену существующим сетям, обеспечивают абонентам широкополосный доступ и используют только пакетную коммутацию каналов.

СПП предоставляют услуги передачи голоса, изображений, текста и мультимедийных сообщений как различные приложения универсального процесса пакетной передачи данных. Вследствие этого технологии передачи данных SMS и MMS, широко используемые в настоящее время, могут уступить место новым технологиям. Пользователи могут даже не заметить этих перемен. Вместе с тем в

технологических решениях, разрабатываемых для мобильных услуг, следует учитывать процесс развития подвижной связи.

Широко применяются современные мобильные терминалы, но изначально они не предназначались для систем с высокой степенью аутентификации. Вследствие этого терминалы различных производителей и даже различные модели терминалов одного производителя могут использовать различные алгоритмы, что приводит к большей сложности, а в некоторых случаях и к невозможности создавать приложения, которые выполняли бы все требуемые системные функции. Например, приложение должно автоматически активироваться при получении сообщения от системы мобильных платежей (операции, инициируемые продавцом). К сожалению, это происходит не в каждом мобильном терминале.

Для упорядочения эксплуатации таких систем следует стандартизировать ряд дополнительных протоколов, и эту задачу решить может МСЭ вместе с производителями оборудования. Еще одна существенная проблема – расположение криптоприложения и администрирование доступа к этому приложению. Как показано в главе "Безопасность ", чтобы обеспечить наивысший уровень безопасности, эти приложения следует помещать в специальный модуль (элемент безопасности аппаратного обеспечения), который защищает хранимую информацию от несанкционированного доступа. Так, в качестве модуля может успешно использоваться карта SIM/UICC, при условии что будет решена проблема делегирования административных полномочий по доступу к SIM-карте, принадлежащей оператору подвижной связи. Эта проблема легко решается, если обе эти функции выполняются одной структурой; в противном случае возникают сложности. Создание мобильных терминалов, оборудованных дополнительным элементом безопасности аппаратного обеспечения, можно считать вариантом решения проблем, вызываемых совместным управлением SIM-картой. Это можно осуществить посредством встроенного модуля безопасности или специально установленной карты памяти, устойчивой к взлому.

В сетях подвижной связи имеются различные способы передачи информации, такие как CSD, SMS, USSD, GPRS, EDGE, LTE. Каждый из них обладает достоинствами и недостатками. Так, SMS – очень надежный и легко осуществимый способ, но длина сообщения ограничена. GPRS, напротив, не ограничен длиной сообщения, но менее надежен и требует верных коррективов для мобильного терминала, особенно в роуминге, который также очень дорог. Успех технологического прогресса привел к широкому применению услуг определения географического местоположения в смартфонах на базе систем GPS или ГЛОНАСС. Определение местоположения существенно расширяет функциональные возможности мобильных терминалов. Ввиду этого в последнее время услуги по определению местоположения широко применяются в приложениях для мобильных устройств (среди которых быстро растет доля смартфонов).

### *4.1.6 Выводы*

Как показано в случаях реализации в ЕС, Японии, США, России и т. д., приведенных в Дополнении, разработка и использование мобильных устройств для мобильных услуг правительства, мобильного здравоохранения, мобильных платежей, мобильного обучения и тому подобного находятся на разных уровнях в различных странах. Вместе с тем проникновение технологических инноваций в мире стремительно растет, что приводит к постепенному сближению уровней технологического развития и сокращает цифровую пропасть между развитыми и развивающимися странами. В настоящее время в развитых странах уже имеются полностью функциональные системы электронных платежей и мобильные услуги правительства, а в некоторых развивающихся странах даже простое использование SMS для передачи данных между медицинскими учреждениями дает реальные результаты, сокращая задержку с получением результатов анализов сухой капли крови на ВИЧ при диагностике детей младшего возраста, о чем говорится в описании проекта MWANA, осуществляемого в Республике Замбии. Это является доказательством того, что очень скоро технологический разрыв сократится. Сегодня наиболее передовые системы, базирующиеся на мобильных устройствах, предлагают полный комплекс услуг, который постоянно расширяется. Так, наряду с мобильными платежами и мобильными банковскими услугами широкое распространение

получили услуги, основанные на определении географического местоположения. Кроме того, как говорится в Белой книге по мобильным платежам, выпущенной Европейским советом по платежам в 2012 году, мобильный терминал должен стать "цифровым бумажником", обеспечивающим аутентификацию и цифровую подпись, которая заменит многочисленные пароли, идентификационные карты и карты постоянного покупателя в торговле.

Как и обычный бумажник, "цифровой" бумажник практически содержит идентификационные данные владельца, данные о средствах платежа, доступных владельцу, и в определенных случаях – персональные данные владельца (изображения, документы и т. п.). В нем может находиться идентификационная информация, цифровые подписи и сертификаты, информация об имени пользователя, адреса для получения и передачи счетов, а также информация о способах платежей. В нем могут также находиться другие приложения, например бонусные пункты, билеты или дорожные документы. После прохождения аутентификации в едином центре можно вносить личные торговые счета или социальные сети, такие как Facebook, LinkedIn и т. п., что очень удобно и снимает необходимость помнить или хранить в безопасности многочисленные пароли к различным счетам. В краткосрочной перспективе можно ожидать активного распространения мобильных устройств в качестве терминалов для электронного правительства и здравоохранения. Это подтверждается инициативами по использованию мобильных устройств, выдвинутыми на мероприятии Telecom-2012 МСЭ и ВОЗ.

Итак, стремительное развитие систем на базе мобильных устройств объясняется мерами безопасности, применяемыми к услугам. Обеспечение безопасности – это общая задача электронного правительства, финансовых служб и электронного здравоохранения, при следовании Рекомендациям МСЭ-Т по безопасности.

Благодаря этим Рекомендациям для аутентификации и кодирования передаваемых данных применяется криптография вместо одноразовых паролей, применявшихся в предыдущих системах, что значительно повысило безопасность мобильных устройств и в то же время увеличило удобство их использования, результатом чего стал рост популярности услуг на базе мобильных устройств.

### *4.1.7 Рекомендации*

- Поскольку мобильные телефоны достигли полного насыщения рынка и высоких уровней обслуживания, они представляют собой идеальные платежные терминалы и безопасные инструменты связи.
- Важно обеспечить простые в использовании интерфейсы мобильных телефонов с последовательным пользовательским опытом по всем поддерживаемым мобильными телефонами способам реализации, даже если наиболее продвинутые смартфоны имеют "огромные" цветные дисплеи и сенсорные интерфейсы. Опыту пользователей существенно препятствует фактор неизбежно малого размера. Так, фактор размера мобильного телефона на практике ограничивает объем информации, который может отображаться в любой данный момент времени, как и способность пользователя вводить сложный текст .
- Мобильное устройство представляет собой "цифровой бумажник" для хранения идентификационных данных владельца, данных об инструментах платежа, доступных владельцу, и факультативные персональные данные, относящиеся к владельцу (например, фотографии, документы и т. п.). Здесь может находиться информация, касающаяся идентификационных карт, цифровых подписей и сертификатов, информация об имени пользователя, адреса для выставления и отправления счетов, а также информация об инструментах платежей. Кроме того, здесь могут находиться другие приложения, такие как карта постоянного покупателя, транспортные документы и билеты.
- Клиентам не рекомендуется быть привязанными к конкретному MNO или банку, и им следует сохранять имеющуюся у них в настоящее время возможность выбирать поставщика услуг.

- Участники электронного диалога должны получить доступ с использованием по меньшей мере двухфакторной аутентификации, и передача данных должны осуществляться в безопасном режиме с использованием криптографических средств.
- Рекомендуется использовать уровень безопасности 4 или 3 согласно Рекомендации МСЭ-Т Y.2740.
- Клиенты должны быть осведомлены об уровне безопасности системы, который следует указать в соглашении между участниками. Аутентификация пользователей может осуществляться единым центром аутентификации.
- Для обеспечения безопасности мобильное устройство должно обладать специальным мобильным приложением, которое обеспечивало бы аутентификацию и кодирование.
- Наиболее реалистична концепция рынка, на котором сосуществуют многочисленные мобильные приложения, предоставляющие услуги через единое мобильное устройство.
- Регистрация и предоставление мобильного приложения должны осуществляться в безопасной обстановке. Клиентам будет проще получить доступ к мобильному приложению, если они смогут использовать существующие доверительные отношения со своими поставщиками услуг.
- Для обеспечения наивысшего уровня безопасности мобильное приложение должно располагаться на элементе безопасности аппаратного обеспечения.
- Выбор элемента безопасности оказывает существенное влияние на модель услуги и роли различных заинтересованных сторон. До настоящего времени существовало три вида элемента безопасности: UICC, встроенный элемент безопасности и съемный элемент безопасности, такой как SD-микрокарта.
- Инструмент предоставления услуг обеспечивает технологическую поддержку и интеграцию различных средств доступа, функциональную совместимость с поставщиками услуг и центром аутентификации.
- Рекомендуется использовать мобильные приложения с несколькими независимыми блоками с различными наборами ключей.
- У клиента может быть несколько мобильных идентичностей пользователя – mID, привязанных к его MSISDN. Следует ввести единые правила выдачи mID, регистрируемые в центральной директории системы, для обеспечения доставки сообщений клиентам по надлежащему маршруту.
- Все центры идентификации и аутентификации должны соблюдать одни правила и нормы распределения для мобильных идентификаторов мобильных клиентов (mID), регистрируемых в центральной директории системы для обеспечения доставки сообщений клиентам.
- Мобильные системы должны по мере возможности использовать технологии и инфраструктуру, уже широко применяемые.

## 4.2 Оценка деятельности электронного правительства и его влияния на жизнедеятельность в Корее (Республика Корея)

### *4.2.1 Введение*

На сегодняшний день разработка большого количества проектов в сфере ИТ, в том числе проектов по разработке гигантской общенациональной системы электронного правительства, начинается не только в развитых, но также и в развивающихся странах, так как все больше и больше людей понимают, что проекты в сфере ИТ будут содействовать обеспечению эффективности и

прозрачности бизнес-процессов. Однако, если не обеспечить надлежащего управления проектами в сфере ИТ, ожидаемые результаты не будут достигнуты или, что еще хуже, будет иметь место напрасная трата государственных средств. Поэтому при реализации проектов в сфере ИТ необходимо принимать должным образом спланированные меры по управлению показателями деятельности.

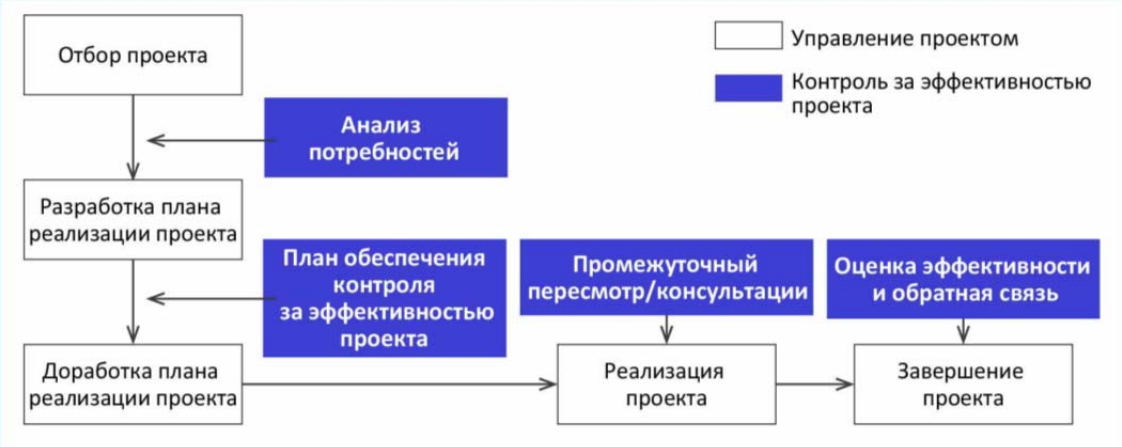
Управление показателями деятельности – это значительно более широкий подход, чем просто проведение оценки. Оценка, как правило, проводится стразу же по окончании реализации проекта, в то время как управление показателями деятельности осуществляется в рамках комплексного подхода и, таким образом, направлено на предоставление возможности надлежащим образом осуществлять управление проектом. В этом смысле для обеспечения управления показателями деятельности в проектах в области электронного правительства правительство Кореи внедрило комплексный подход, позволяющий организации, отвечающей за реализацию проектов в области электронного правительства, провести предварительные консультации и осуществить анализ промежуточных результатов.

В прилагаемом документе содержится более подробная информация о схеме управления показателями деятельности в проектах в области электронного правительства, а также о нашей деятельности по распространению передового опыта в сфере управления показателями деятельности для всех учреждений, реализующих проекты в области электронного правительства.

### *4.2.2 Механизм обеспечения управления показателями деятельности в проектах в области электронного правительства*

Обеспечение управления показателями деятельности в области электронного правительства охватывает весь процесс реализации проекта, включая отбор проекта, реализацию проекта и оценку реализации проекта. На рисунке, ниже, представлен механизм управления показателями деятельности в области электронного правительства.

**Рисунок 1: Механизм управления показателями деятельности в проектах в области электронного правительства**




Отбор новых проектов осуществляется по результатам анализа потребностей, в рамках которого в два этапа выполняется процесс пересмотра, после чего утверждаются окончательные проекты. До начала реализации нового проекта каждой организации следует подготовить собственный план управления показателями деятельности, который должен содержать описание метода осуществления мониторинга и оценки проекта, а также четкое определение цели проекта,

детальное описание показателей, на основании которых будет измеряться эффект от проекта и его результаты.

Таким образом, организация, реализующая проект, должна оценить его на основании подготовленного плана управления показателями деятельности. Во время реализации крупномасштабных проектов, которые составляют около 10% от общего количества проектов в области электронного правительства, проводятся промежуточные анализ/консультации. В ходе оказания услуги промежуточной консультации предлагается не только анализ текущего положения, но и, при необходимости, варианты решения проблем.

Завершающий этап управления показателями деятельности – это оценка эффективности и обратная связь. Все проекты оцениваются по 5 категориям: S, A, B, C, D. Проекту, получившему оценку S, будет отдано предпочтение при следующем распределении бюджета, а иногда, при необходимости, его бюджет может быть увеличен. Оценка A означает продолжение проекта без каких-либо изменений.

Проекты, получившие оценку B, должны быть изменены на следующем этапе, тогда как проекты с оценкой C требуют изменения основных принципов проекта. В проектах с оценкой D необходимо изменить саму суть проекта, в противном случае последующее финансирование может быть не предоставлено.

### *4.2.3 Будущие направления*

Управление показателями деятельности в отношении проектов по электронному правительству было введено в Корее в 2009 году, и оно все чаще становится не факультативным, а обязательным в этой стране. По сравнению с другими проектами проекты в области электронного правительства требуют более жесткого управления показателями деятельности, вследствие чего при отборе новых проектов был введен всесторонний анализ потребностей. Кроме того, были введены промежуточные анализ/консультации. Мы считаем, что в целях соответствия изменяющимся условиям реализации проектов в области электронного правительства работа по дальнейшему развитию и изменению управления показателями деятельности должна продолжаться.

## 4.3 eGovFrame: открытая платформа с открытыми инновациями

### *4.3.1 Общий обзор*

Применение различных платформ разработки программных приложений вызывает множество различных проблем, таких как сложности при эксплуатации системы, зависимость от поставщиков услуг и отсутствие функциональной совместимости между системами. В целях решения данных проблем корейское правительство создало стандартную платформу для разработки приложений для электронного правительства под названием eGovFrame. При стандартизации программного обеспечения eGovFrame многие заинтересованные стороны высказывали свои точки зрения и пожелания. Крупные компании опасались, что больше не смогут занимать господствующее положение на рынке, государственные организации беспокоились, получат ли они стабильную техническую поддержку, разработчики отказывались работать с новыми инструментами, правительство сомневалось в экономической эффективности, а малые и средние предприятия (МСП) заботило то, что проект ориентирован главным образом на крупные компании. Таким образом, многочисленным заинтересованным сторонам пришлось согласиться со стандартизацией платформы программного обеспечения. Чтобы провести стандартизацию платформы программного обеспечения и преодолеть все вышеупомянутые трудности, мы применили стратегию открытых инноваций, которая реализовывалась в четыре этапа: 1) открытые источники; 2) открытый процесс; 3) открытый результат; и 4) открытая экосистема. Платформа eGovFrame и стратегия открытых инноваций будут детально рассмотрены.

Правительство Кореи реализовало множество проектов в области электронного правительства и разработало множество приложений электронного правительства. В значительной части этих проектов применялись платформы программного обеспечения, которые представляют собой полезный инструмент повышения производительности и качества разработки приложений. В настоящее время платформы программного обеспечения стали широко применяемым инструментом разработки приложений электронного правительства, но они обладают и некоторыми недостатками. Для решения этих проблем правительство Кореи предприняло попытки стандартизировать платформу программного обеспечения eGovframe. Однако многие заинтересованные стороны высказывали свои точки зрения и пожелания, и, чтобы снять эти проблемы мы применили стратегию открытых инноваций, которая реализовывалась в четыре этапа. Благодаря этой стратегии мы осуществляем стандартизацию платформы электронного правительства и создаем открытую экосистему eGovframe.

### *4.3.2 Базовая информация по eGovFrame*

Корея ведет активные действия по созданию электронного правительства, поскольку считает это решающим инструментом для повышения конкурентоспособности своих органов власти посредством использования ведущих мировых информационно-коммуникационных технологий (ИКТ), включая широкополосный интернет. Заложив основы электронного правительства, государственное руководство Кореи сделало реализацию электронного правительства приоритетным пунктом национальной повестки дня на 2000-е годы. В результате электронное правительство заняло прочное положение во всех государственных ведомствах Кореи и дало ощутимые результаты. В связи с этим международное сообщество признало эффективность электронного правительства Кореи. Корейское электронное правительство признано одним из лучших в мире международными организациями, в том числе Организацией Объединенных Наций, и в настоящее время различные системы электронного правительства экспортируются в другие страны.

Чтобы добиться таких успехов, корейское правительство реализовало множество проектов электронного правительства и разработало большое количество приложений электронного правительства. При работе над значительной частью проектов использовалась платформа программного обеспечения. Платформа программного обеспечения представляет собой эффективный инструмент повышения производительности и качества разрабатываемых приложений, и она стала стали широко применяемым инструментом разработки приложений электронного правительства. С другой стороны, платформы программного обеспечения обладают и некоторыми недостатками.

Когда при разработке проектов электронного правительства используется платформа программного обеспечения, проекты становятся в значительной мере зависимыми от платформ ИТ-компаний. Поэтому сложно обслуживать приложение без технической поддержки поставщика платформы. В случае проектов большой продолжительности платформа, применявшаяся на предыдущих этапах работы, становится барьером технического плана для новых конкурентов, что создает порочный круг несправедливости на рынке программного обеспечения. Зависимость от платформы ИТ-компаний приводит к ряду проблем. Во-первых, экономическая логика приложения также зависит от определенной платформы. Во-вторых, поскольку определенная платформа является своего рода "черным ящиком", только поставщик платформы может осуществлять техническое обслуживание приложения, что приводит к "привязке" к поставщику платформы. В-третьих, наличие нескольких платформ порождает массу лишних действий при настройке приложений, подборе кадров, обучении сотрудников и обслуживании системы.

В целях решения данных проблем корейское правительство стандартизировало платформу программного обеспечения и разработало eGovFrame (Стандартную платформу электронного правительства). eGovFrame – это стандартизированный набор программных инструментов для разработки и эксплуатации приложений электронного правительства, предназначенный для повышения эффективности инвестиций в ИКТ и качества услуг электронного правительства.

Основное внимание в нем уделяется возможности повторного использования и функциональной совместимости приложений электронного правительства посредством создания стандартной платформы для разработки программного обеспечения электронного правительства, обеспечения независимости от ИТ-компаний благодаря введению открытых и нейтральных инструментов программного обеспечения и повышению конкурентоспособности МСП в области ИТ путем открытого совместного использования инструментов по разным каналам.

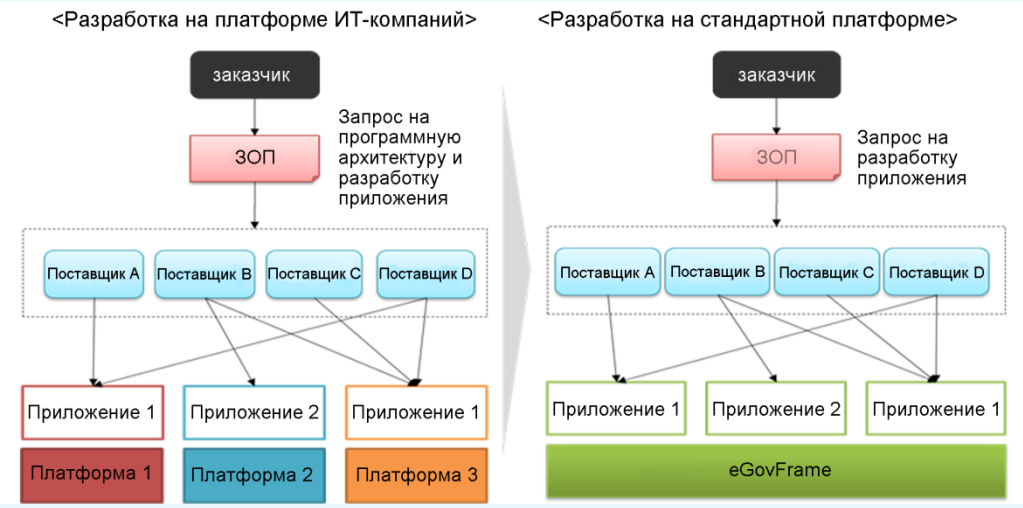
### *4.3.3 Стратегия открытых инноваций*

Для того чтобы решить проблемы, порожденные стандартизацией платформы программного обеспечения для электронного правительства, мы внедрили стратегию, основанную на парадигме открытых инноваций, которая получила название стратегии открытых инноваций. Стандартизацию программной платформы электронного правительства невозможно было провести усилиями только правительства. Также требовались знания, участие, сотрудничество и обратная связь от многих заинтересованных сторон. Чтобы выполнить все эти требования и реализовать стандартизацию и внедрение платформы электронного правительства, мы применили стратегию, состоявшую из четырех этапов: открытые источники, открытые процессы, открытые результаты и открытая экосистема. На Рисунке 2 показана общая структура стратегии открытых инноваций.

**Рисунок 2: Стратегия открытых инноваций; Открытые источники**

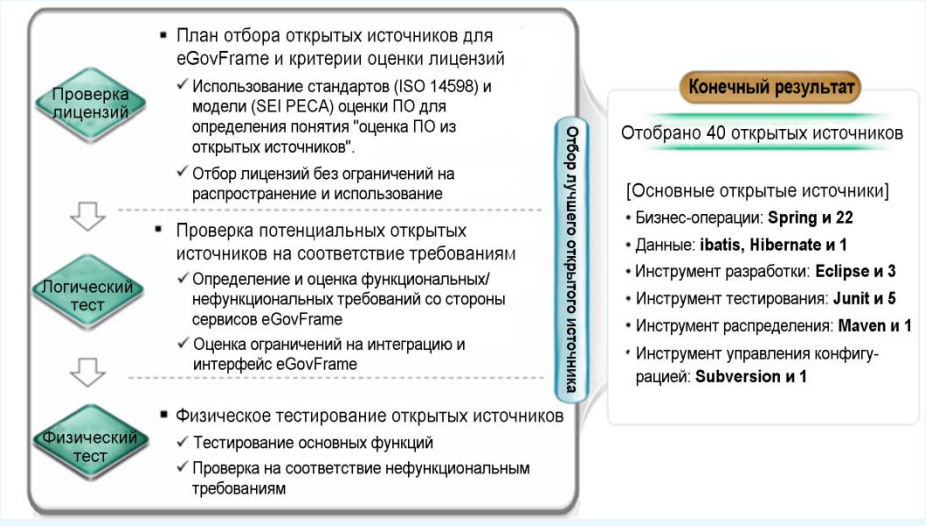

Для того чтобы стандартизировать платформу eGovFrame, был проведен анализ платформ пяти ведущих ИТ-компаний в отношении экологических и функциональных характеристик, а также обследование и опрос каждой заинтересованной стороны. В результате было выбрано четыре программных среды, состоящие из тринадцати сервисных групп и пятидесяти четырех служебных функциональных возможностей. Чтобы предотвратить повторную разработку тех же функций среди правительственных систем, был проведен анализ шестидесяти семи проектов электронного правительства за 2004–2007 годы, в частности 31 114 функциональных возможностей. Критериями для вычленения общих функциональных возможностей компонентов были: большая вероятность повторной разработки, возможность повторного использования в правительственных системах и вероятность принятия стандарта. После пяти этапов отбора было выявлено 219 общих компонентов.

**Рисунок 3: Будущее представление eGovFrame**




Чтобы сократить зависимость от крупных ИТ-компаний, были отобраны хорошо известные и проверенные открытые источники. На основе международной модели процесса оценки программного обеспечения (ISO 14598) и практического процесса оценки программного обеспечения (SEI PECA) для eGovFrame был разработан процесс оценки программного обеспечения из открытых источников. В ходе первого логического испытания сто семьдесят пять образцов программного обеспечения из открытых источников оценивались на соответствие требованиям, главным образом касающимся возможностей интеграции и интерфейсов eGovFrame. В ходе второго, физико-механического испытания, восемьдесят пять образцов программного обеспечения из открытых источников, отобранные на первом этапе, оценивались на предмет базовых функций и нефункциональных требований. В результате для разработки eGovFrame было выбрано сорок образцов программного обеспечения из открытых источников. Платформа eGovFrame, построенная на базе открытых источников, имеет несколько преимуществ. Она может быстро принимать стремительно меняющиеся технологии и использоваться в приложениях электронного правительства других стран.

**Рисунок 4: Оценка и окончательный отбор открытых источников; Открытые процессы**



Процессы разработки открыты для общественности, благодаря чему создаются такие условия, когда можно подробно изучить позиции по данному вопросу более чем 500 заинтересованных сторон. Наряду с этим нами было проведено более 20 государственно-частных встреч, которые способствовали взаимопониманию между многими заинтересованными сторонами и достижению ими консенсуса.

**Рисунок 5: Многочисленные заинтересованные стороны eGovFrame**


### Открытые результаты

Все результаты проекта доступны общественности, в том числе исходные коды и ER-диаграмма, представленные на веб-сайте eGovFrame (www.egovframe.go.kr), который создан для того, чтобы поощрять добровольное участие в процессе реализации проекта разработчиков, поставщиков и государственных служащих. Также мы организовали бесплатные курсы профессиональной подготовки, и 1236 разработчиков получили сертификаты.

### Открытая экосистема

Мы создали открытое сообщество крупных, малых и средних предприятий, а также центр государственно-частного сотрудничества. Данные организации – это отправные точки для продвижения платформы eGovFrame на мировом уровне, предоставления мощной технической поддержки и постоянного совершенствования системы. Непрерывное совершенствование eGovFrame должно осуществляться открытым сообществом, в ходе ежеквартальных встреч экспертов и открытого форума партнеров государственного и частного секторов. Тем самым мы создаем открытую экосистему для eGovFrame.

## *4.3.4 Изменения и преимущества eGovFrame*

Данный проект направлен на создание стандартизированного набора программных инструментов под названием eGovFrame, предназначенного для разработки и эксплуатации приложений электронного правительства, который позволит повысить эффективность инвестиций в ИКТ и качество услуг электронного правительства. Основное внимание в нем уделяется возможности повторного использования и функциональной совместимости приложений электронного правительства, что достигается посредством создания стандартной платформы для разработки программного обеспечения электронного правительства, обеспечения независимости от ИТ компаний благодаря введению открытых и нейтральных инструментов программного

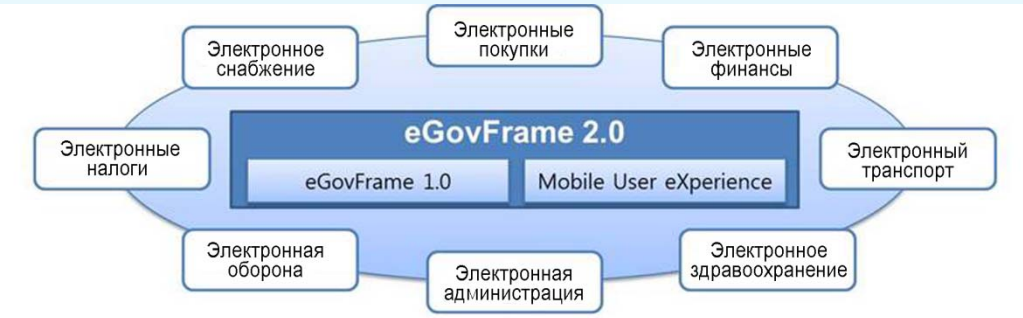
обеспечения и повышению конкурентоспособности МСП в области ИТ путем открытого совместного использования инструментов по разным каналам.

**Рисунок 6: Концепция и стратегия проекта eGovframe**


Платформа eGovFrame создана на основе хорошо известного и проверенного программного обеспечения из открытых источников, и все исходные коды доступны всем заинтересованным сторонам на онлайн-портале. eGovFrame состоит из четырех программных сред: среды выполнения приложений, среды разработки для разработчиков приложений, среды администрирования для администраторов платформы и операционной среды для операторов приложений.

На этапе разработки приложений благодаря использованию платформы eGovFrame объем расходов и работ можно сократить примерно на 30%. Это означает, что eGovFrame выступает в качестве буфера для адаптации различных приложений к конкретной инфраструктуре. Кроме того, eGovFrame служит общей платформой для разработки общих функций. Последняя версия eGovFrame 2.0 содержит компонент Mobile User eXperience, как показано на Рисунке 7.

**Рисунок 7: eGovFrame 2.0**




| Сектор | Проекты на базе eGovFrame | Сектор | Проекты на базе eGovFrame |
|---|---|---|---|
| Администрация | Портал госпредставителей | СМИ | Информационная система интеграции вещания и телекоммуникаций |
| Транспорт | Система управления Сеульского метрополитена | Патентные ведомства | Общая патентная система |
| Медицина | Система стратегического управления в больницах | Налоговые ведомства | Улучшенная система управления ИТ-услугами государственных налоговых органов |
| Военное дело | Система управления военной символикой | Порты | Система управления портом Инчхона |
| Таможенная служба | Всемирная система портовой логистики | Культура | Электронная библиотека Национального собрания Кореи |
| Земле-пользование | Система управления информацией о землепользовании | Образование | Система управления информацией для университетов |

### *4.3.5 Расширение и будущее eGovFrame Mobile*

В связи с расширяющимся использованием современных мобильных устройств, таких как смартфоны и планшеты, в государственном и частном секторах растет спрос на услуги на базе мобильных устройств. В ответ на данный новый вид спроса, а также в целях повышения качества и эффективности eGovFrame в конце 2011 года была представлена новая версия программы eGovFrame 2.0 с использованием HTML 5 и новым пользовательским интерфейсом. Данная версия совместима по меньшей мере с тремя мобильными браузерами (Chrome, Safari и FireFox). Многие мобильные услуги электронного правительства в Республике Корея были разработаны на базе eGovFrame 2.0, как показано на Рисунке 7.

Для использования таких функций мобильных телефонов, как вибрация, управление камерой, компас и т. д., eGovFrame 2.0 также представит новые компоненты, которые поддерживают создание мобильных приложений. Ожидается, что это станет для разработчиков программного обеспечения стимулом к созданию ряда мобильных веб-услуг и мобильных приложений.

### *4.3.6 Возможности для других стран*

Получив позитивный опыт, правительство Республики Корея вносит большой вклад в международную деятельность по информатизации. Очень заинтересованы в этой стандартизированной платформе страны, которые хотят решить проблему монополии отдельных компаний-поставщиков или отдать предпочтение программному обеспечению из открытых источников. eGovFrame уже применяется в некоторых других странах, как показано в Таблице 1.

**Таблица 1: Страны, применяющие платформу eGovFrame**

| Страна | Проект | Соответствующее ведомство | Длительность проекта |
|---|---|---|---|
| Болгария | Административная система Софийского университета | Софийский университет | 11/2011~10/2012 |
| Эквадор | Система одного окна | Таможенная служба Эквадора | 01/2011~03/2013 |
| Вьетнам | Инвестиции в модернизацию и расширение проекта системы водоснабжения | Министерство национальных ресурсов и окружающей среды | 09/2010~12/2013 |
| Монголия | Система государственной регистрации | Главное управление государственной регистрации | 07/2011~06/2012 |
| Тунис | Система электронных закупок | Национальное агентство по государственным закупкам | 11/2011~11/2012 |

Многие другие развивающиеся страны проявляют желание ознакомиться с опытом Кореи в области электронного правительства и, в частности, платформы eGovFrame. В связи с этим власти Кореи различными способами участвуют в совершенствовании услуг электронного правительства в других странах, в том числе активно сотрудничая с международными организациями. Чтобы стимулировать другие страны к использованию платформы eGovFrame, исходный код можно загрузить с англоязычной версии портала http://eng.egovframe.go.kr, а также предлагается онлайновая техническая поддержка. Кроме того, например, на базе программы Korea IT Learning (KoIL) и Центра сотрудничества в области информационных технологий (ITCC) проводятся обучающие курсы, которые призваны способствовать сотрудничеству в секторе ИТ между Республикой Корея и странами-партнерами.

# 5 Сферы применения на благо развивающихся стран

## 5.1 Руководящие указания для определения сфер применения

В сегодняшнем мире, определяемом технологиями, ИКТ стремительно становятся основным элементом программ модернизации правительства. Это происходит не только в развитых странах. Все в большей степени в развивающихся странах получает признание потенциал новых технологий в преобразовании образа действий правительства. То, как правительство использует ИКТ, – электронное правительство – вполне сформировалось и является составной частью ведения дел правительствами, но нам необходимо подготовить руководящие указания для определения сфер применения и определить их очередность на благо развивающимся странам. При разработке руководящих указаний следует учитывать следующие моменты:

1) особенности конкретно взятой развивающейся страны (экономические и социальные условия);

2) индивидуальные потребности страны и существующие возможности;

3) приоритетность наиболее значимых для развивающихся стран приложений;

4) рассмотрение возможностей использования мобильных и беспроводных платформ для обеспечения взаимодействия между государственными органами и гражданами в сфере получения государственной информации и предоставления государственных услуг.

Сферы применения для стран, находящихся на начальном этапе развития электронного правительства, могут быть выбраны на основании следующих принципов:

- программы, теснее всего связанные с повседневной жизнью граждан, чтобы они ощутили максимальную пользу от внедряемых электронных услуг;

- программы, в основном служащие интеграции бизнес-процессов вне зависимости от организационных границ;
- максимальное увеличение потенциала государственных учреждений по совместному использованию информации для ликвидации дублирования регистрационных записей и управления ими;
- содействие использованию ИКТ для упорядочения административных процессов посредством принятой методики перестройки рабочих процессов (BPR).

Наряду с вышеизложенными принципами определения сфер применения нам необходимо учитывать, с одной стороны, нехватку национальных ресурсов для электронного правительства, в особенности в развивающихся странах, а с другой – безотлагательную потребность модернизации страны посредством внедрения электронного правительства. Решение, позволяющее удовлетворить эту потребность, основывается на стратегии, отборе и концентрации; при этом отбирается небольшое число проектов электронного правительства на основании вышеизложенных принципов, сосредоточивая ограниченные ресурсы на отобранных проектах.

## 5.2 Инфраструктура

- Обновление правовой системы для электронного правительства и безопасности.
- Профессиональная подготовка персонала в сфере ИКТ и реструктуризация управления в сфере ИКТ.
- Электронная система аутентификации.

## 5.3 G2G

- Система электронной документации, подключаемая к рабочим системам правительства, таким как система государственных закупок, система местного самоуправления, налоговая система и т. п.
- Система местного самоуправления.
- Система управления государственными финансами (общенациональная и местные).
- Система совместного использования информации.

## 5.4 G2C и G2B

Опыт и уроки в отношении реализации удобных для пользователей услуг, интеграции и персонализации государственных услуг, использования многоканальной связи, улучшения качества услуг с учетом требований пользователя, продвижения услуг в области электронного правительства, защиты персональных данных и обеспечения безопасности транзакций электронного правительства.

- Система порталов для предоставления гражданам государственных услуг.
- Налоговая интернет-система.
- Электронная система государственных закупок.

# 6 Факторы обеспечения успеха деятельности в сфере электронного правительства

## 6.1 Руководство со стороны президента (политическая поддержка)

- Национальные проекты в области ИТ, в особенности проекты электронного правительства, обычно затрагивают несколько учреждений, между которыми могут существовать разногласия по многим пунктам. Процесс разработки политики нередко прерывается бюрократическим соперничеством между министерствами, заинтересованными в том или ином конкретном вопросе.
- Возможно, наиболее масштабной проблемой в инициативах в области электронного правительства является достижение координации деятельности соответствующих организаций в процессе развертывания сетей и внедрения системы приложений. Различные организации принимают во внимание разные уровни и типы рисков и стимулов. Маловероятно, чтобы какая-либо одна схема удовлетворила потребности всех организаций. Для смягчения этой проблемы на межведомственном уровне создается руководящий комитет высокого уровня для разрешения разногласий между государственными учреждениями. Эффективность работы комитета зависит от того, в какой мере его поддерживает руководство в лице президента, которое является источником власти при обеспечении координации.
- Проекты в области ИТ требуют огромных инвестиций, размер прибыли на которые не сразу очевиден, поскольку инициативы в области ИТ проявляют свою истинную ценность лишь через определенное время. В то же время, поскольку проекты в области ИТ неосязаемы, непросто продемонстрировать их достижения тем, кто несет ответственность за выделение национальных ресурсов на государственные проекты.
- Многие люди сознают потенциал использования ИТ и их воздействие на эффективность и конкурентоспособность, но структуры, занимающиеся распределением государственного бюджета, не в состоянии найти доказательства финансового значения ИТ, которые свидетельствовали бы об их преимуществах. В разрешении этой дилеммы ключевую роль играет руководство со стороны президента, признающего потенциал ИТ. Так, президент Кореи в 1987 году принял решение об изменении обычного бюджетного процесса для выделения крупной суммы на использование исключительно в проектах в области ИТ. Это доказывает, что на начальных этапах инициатив в области ИТ в Корее имело место решительное руководство со стороны президента.

## 6.2 Баланс предложения и спроса в отношении услуг электронного правительства

- В типичном национальном генеральном плане развития ИТ нередко устанавливаются приоритеты в политике, в основном в отношении предложения. Правительство видит необходимость руководства развитием предоставляемых гражданам прикладных услуг, в первую очередь для формирования спроса. Но следует учесть и проблему, в которой основное внимание уделяется стороне спроса, например, какого рода услуги соответствуют значительным средствам, вкладываемым в проекты электронного правительства. Это объясняется возможностью того, что мы создадим дорогостоящее решение, для которого нет соответствующей проблемы.
- Уделение основного внимания стороне предложения не исключает значения рассмотрения потенциального спроса на ту или иную конкретную услугу электронного правительства. Дилемма возникает потому, что, по-видимому, проекты в области ИТ создают спрос, который невозможно прогнозировать, пока не появилось предложение. Становится важным, чтобы в

стратегии в отношении ИТ учитывалась необходимость формирования спроса после внедрения ИТ-систем, например, путем подготовки потенциальных пользователей, чтобы они могли воспользоваться реальными преимуществами ИТ.

- Чтобы уравновесить спрос и предложение по той или иной услуге электронного правительства, следует учитывать каждый аспект потенциальной услуги. Например, анализ проводимых в автономном режиме транзакций между правительством и гражданами является одним из способов изучения аспектов спроса, когда предстоит решить, какие услуги должны охватить инициативы в области электронного правительства. Это может восполнить недостаточную прогнозируемость спроса, поскольку можно ожидать, что, чем больше объем офлайновых транзакций, тем больше будет спрос на онлайновые услуги.

## 6.3 Четкое понимание сути электронного правительства

- Применительно к электронному правительству важнее, что оно правительство, чем что оно электронное. Суть электронного правительства заключается в преобразовании органов государственного управления для обновления внутренних и внешних взаимоотношений с помощью ИТ. Вопросы электронного правительства следует включить в инициативы по реформированию национального государственного управления и благому управлению. Хотя вопросы обновления стояли в повестке дня с начала применения приложений ИТ в государственном управлении, фактическое воздействие на процессы работы правительства в реальном мире обнаруживается чрезвычайно медленно.
- Правительства должны не просто сосредоточиваться на внедрении ИТ, но принимать решения о преобразовании административных процедур, руководить этим процессом и контролировать его так, чтобы реализовать в полной мере потенциал ИТ при реструктурировании процессов.
- Ожидается, что электронное правительство приведет к глубинным и масштабным изменениям во внутренних процессах правительства и предоставляемых гражданам услугах. Изменения происходят на основе природы ИТ, в частности интернета, что дает правительству возможность вести работу комплексным образом. Интеграция, стимулируемая совместным использованием информации, обычно происходит в группах правительственных организаций с общими функциями или одним и тем же набором услуг. Большинство проектов электронного правительства проходят стадию перестройки рабочих процессов (BPR) до начала фактической реализации. BPR, как правило, проводится в несколько этапов, таких как анализ рабочих процессов, касающихся целей организации, упразднение дублирующих друг друга процессов, упорядочение методов работы и упрощение сложных процессов.
- Устранение дублирования и упорядочение процессов работы подразумевает сокращение рабочих мест, что вызывает сопротивление заинтересованных сторон. У тех, кто привык к традиционным методам работы, практически нет стимулов соглашаться на перемены. Мы должны разработать стимулы для государственных служащих, а также создать структуры для координации деятельности правительственных учреждений, участвующих в том или ином конкретном процессе. К числу стимулов относятся переподготовка и перестановка служащих по их желанию. Чтобы управление стало более гибким и эффективным, ставшие ненужными процессы упраздняются, сложные – упрощаются, а сокращаемые – объединяются.

## 6.4 Поощрение активности и участия граждан

- Готовность граждан участвовать в процессе принятия государственных решений резко возрастает ввиду расширения возможностей взаимодействия между правительством и гражданами. Этому частично способствовало развитие демократических процессов и широкое использование интернета, упрощающее доступ к различным государственным организациям. Необходимо следить за тем, как технологии дают частному лицу возможность

быть услышанным и не позволить государственной точке зрения заглушить себя в массовых дебатах. Так, правительство должно иметь возможность должным образом реагировать на мнения отдельных людей.

- Для активного участия в онлайновой деятельности граждане должны иметь возможно более полную информацию по вопросам, представляющим интерес для общества, а государственные служащие – сознавать перспективы и ограничения интернета в отношении участия граждан в выработке политики.

## 6.5 Инновации в управлении информационными ресурсами (IRM)

Поскольку в рамках проектов электронного правительства ИТ-ресурсы аккумулируются в различных секторах правительства, необходимо найти способ управлять ими, чтобы избежать напрасной траты ИТ-активов. Для IRM отдельные государственные организации должны сотрудничать, чтобы совместно использовать ИТ-ресурсы и интегрировать их для достижения максимального потенциала.

В такой методике IRM, как архитектура предприятия (EA), документально отражаются имеющиеся и желательные взаимоотношения между бизнес-процессами и ИТ-ресурсами, с тем чтобы обеспечить безопасное совместное использование информации и интеграцию процессов в рамках отдельных организаций и между различными организациями. EA также позволяет избегать дублирования в закупках ИТ-ресурсов государственными учреждениями для повышения эффективности инвестиций.

В деятельности в рамках EA основное внимание уделяется способам претворения в жизнь совместного использования информации и повышения эффективности инвестиций в ИТ посредством предоставления руководящих указаний и эталонных моделей для отдельных компонентов. Эталонные модели предназначаются для содействия общему определению, применению, надлежащему совместному использованию данных, бизнес-процессов, программных приложений и аппаратного обеспечения. Руководящие указания позволяют эффективно управлять информационными ресурсами на основании элементов, вероятность изменения которых минимальна в отношении изменения экономических приоритетов и технологических условий.

## 6.6 Защита конфиденциальности и безопасности систем

- Поскольку поддерживаемая той или иной организацией информация все в большей мере совместно используется соответствующими сторонами в процессе разработки инициатив в области электронного правительства, потенциальные пользователи услуг электронного правительства начинают беспокоиться относительно того, что их персональная информация может использоваться ненадлежащим образом и чрезмерно широко. Необходимо достичь компромисса между защитой персональной информации и совместным использованием информации для скорейшего развития электронных приложений правительственной деятельности. Крайне важно добиться равновесия между стимулированием совместного использования информации соответствующими учреждениями и разработкой инструментов для защиты конфиденциальности.
- Поскольку по мере развития электронного правительства мы начнем испытывать негативные последствия приложений ИТ, следует укрепить меры защиты конфиденциальности для достижения равновесия между двумя крайностями. Системы электронного правительства всегда открыты для атак извне правительства, а иногда даже изнутри него. Ввиду этого необходимо принять все меры предосторожности в техническом, правовом и институциональном плане в отношении взлома, подделки или мошенничества.

### 6.7 Стратегии принятия электронных услуг

- Хотя электронные услуги появились, вопрос в том, принимают ли их граждане и предприятия. Граждане не готовы принимать системы электронного правительства, если они не ощущают реальных преимуществ электронных услуг. Вполне обычное явление представляет собой более низкий уровень использования электронных услуг, чем он должен был бы быть в начале внедрения систем электронного правительства. При этом не в полной мере используется потенциал вложенных средств, из-за чего начинаются серьезные дебаты относительно того, стоит ли продолжать осуществлять инициативы в области электронного правительства.
- Следует тщательно изучить интернет-приложения правительственных операций, чтобы понять, как их улучшить, чтобы люди реально почувствовали удобство этих приложений. Каналы доступа должны быть достаточно широки для удобства доступа, а число гиперссылок – достаточно небольшим, чтобы среднестатистические граждане могли попасть на нужный сайт для получения правительственной информации и услуг.
- Следует заниматься не всеми приложениями, а сосредоточиться на нескольких существенных, чтобы было удобно взаимодействовать с правительством в реальном киберпространстве. При отборе приложений электронного правительства, которые следует улучшать, важно выбирать услуги, чаще всего запрашиваемые гражданами, чтобы преимущества системы могли оценить возможно больше людей.

## 7 Руководящие указания по стимулированию деятельности электронного правительства и определению сфер применения электронного правительства для развивающихся стран

### 7.1 Сфера охвата

Настоящие руководящие указания охватывают вопросы, касающиеся стимулирования деятельности электронного правительства и определения сфер применения электронного правительства для развивающихся стран.

### 7.2 Задача руководящих указаний

Настоящие руководящие указания рассчитаны на то, чтобы помочь развивающимся странам определить, какие факторы следует учитывать для успешного ведения деятельности электронного правительства и какие сферы следует определить для приложений электронного правительства на благо развивающихся стран.

Руководящие указания обеспечивают:

a) руководство по определению сфер применения электронного правительства на благо развивающихся стран; в отдельных странах есть условия, показывающие конкретные сферы применения электронного правительства;

b) факторы, которые следует принять во внимание для успешной реализации инициатив в области электронного правительства в развивающихся странах.

## 7.3 Руководящие указания по определению сфер применения на благо развивающихся стран

Существует множество сфер применения электронного правительства, поскольку практически все правительственные операции можно преобразовать с помощью информационно-коммуникационных технологий.

При определении сфер применения для развивающихся стран мы должны рассмотреть следующие факторы:

c) социально-экономические особенности отдельных развивающихся стран;

d) индивидуальные потребности страны и существующие возможности;

e) приоритет наиболее значимых для развивающихся стран приложений;

f) рассмотрение возможностей использования мобильных и беспроводных платформ для обеспечения взаимодействия между государственными органами и гражданами в сфере получения государственной информации и предоставления государственных услуг;

g) национальные стратегии и механизмы, позволяющие упростить административные и организационные процессы и обеспечить соответствующее взаимодействие между государственными органами, т. е. сфера G2G по терминологии электронного правительства;

h) опыт и уроки в отношении реализации удобных для пользователей услуг, интеграции и персонализации государственных услуг, использования многоканальной связи, улучшения качества услуг с учетом требований пользователя, продвижения услуг в области электронного правительства, защиты персональных данных и обеспечения безопасности транзакций электронного правительства, т. е. сферы G2C и G2B.

## 7.4 Руководящие указания для обеспечения прогресса в деятельности электронного правительства

Чтобы обеспечить надлежащий прогресс в деятельности электронного правительства, развивающиеся страны должны иметь возможность создавать условия, ведущие к эффективной реализации инициатив в области электронного правительства.

Выявлены несколько факторов успеха на основании опыта стран с передовыми системами электронного правительства. В процессе внедрения систем электронного правительства необходимо учитывать следующие факторы:

i) эффективная координация и сильное политическое руководство; достижение координации между соответствующими организациями в процессе развертывания сетей и реализации системы приложений – возможно, самая сложная задача инициатив в области электронного правительства;

j) баланс предложения и спроса на услуги электронного правительства; в типичном национальном генеральном плане развития ИТ нередко устанавливаются приоритеты в политике, в основном в отношении предложения. Правительство видит необходимость руководства развитием предоставляемых гражданам прикладных услуг, в первую очередь для формирования спроса. Но следует учесть и проблему, в которой основной внимание уделяется стороне спроса, например, какого рода услуги соответствуют значительным средствам, вкладываемым в проекты электронного правительства. Это объясняется возможностью того, что мы создадим дорогостоящее решение, для которого нет соответствующей проблемы;

k) четкое и верное понимание концепции электронного правительства; применительно к электронному правительству важнее, что оно правительство, чем что оно электронное. Суть электронного правительства заключается в преобразовании органов государственного

управления для обновления внутренних и внешних взаимоотношений с помощью ИКТ. Вопросы электронного правительства следует включить в инициативы по реформированию национального государственного управления и благому управлению;

l) поощрение активности и участия граждан; готовность граждан участвовать в процессе принятия государственных решений резко возрастает ввиду расширения возможностей взаимодействия между правительством и гражданами. Этому частично способствовало развитие демократических процессов и широкое использование интернета, упрощающее доступ к различным государственным организациям. Необходимо следить за тем, как технологии дают частному лицу возможность быть услышанным и не позволить государственной точке зрения заглушить себя в массовых дебатах;

m) эффективные мониторинг и оценка, наряду с соответствующей системой обратной связи; хорошее начало проектов электронного правительства не может служить мерой успеха. В конечном счете значение имеют завершенность, показатели работы и результат. Наряду со стремлением измерить выгоду инвестиций в ИКТ следует уделять внимание мониторингу и оценке инициатив в области электронного правительства, чтобы понимать потребности пользователей и их отношение к электронным услугам. Результат оценки систем по этим показателям следует направлять в механизм обратной связи;

n) инновационное и эффективное IRM (управление информационными ресурсами); поскольку в рамках проектов электронного правительства ИТ-ресурсы аккумулируются в различных секторах правительства, необходимо найти способ управлять ими, чтобы избежать напрасной траты ИТ-активов. Для IRM отдельные государственные организации должны сотрудничать, чтобы совместно использовать ИТ-ресурсы и интегрировать их для достижения максимального потенциала

o) защита персональной информации; поскольку поддерживаемая той или иной организацией информация все в большей мере совместно используется соответствующими сторонами в процессе разработки инициатив в области электронного правительства, потенциальные пользователи услуг электронного правительства начинают беспокоиться относительно того, что их персональная информация может использоваться ненадлежащим образом и чрезмерно широко. Необходимо достичь компромисса между защитой персональной информации и совместным использованием информации для скорейшего развития электронных приложений правительственной деятельности. Крайне важно добиться равновесия между стимулированием совместного использования информации соответствующими учреждениями и разработкой инструментов для защиты конфиденциальности;

p) стратегии, направленные на принятие гражданами услуг электронного правительства. Хотя электронные услуги появились, вопрос в том, принимают ли их граждане и предприятия. Граждане не готовы принимать системы электронного правительства, если они не ощущают реальных преимуществ электронных услуг. Вполне обычное явление представляет собой более низкий уровень использования электронных услуг, чем он должен был бы быть в начале внедрения систем электронного правительства. При этом не в полной мере используется потенциал вложенных средств, из-за чего начинаются серьезные дебаты относительно того, стоит ли продолжать осуществлять инициативы в области электронного правительства.

## Annexes

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

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

# Annex 1: Full Transcripts of Contributed Cases

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

### 1) Overview

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

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

### 2) Objectives and strategies

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

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

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

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

## 3) Implementation

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

### a. High-speed Internet infrastructure

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

### b. Village information center

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

### c. Granting PCs

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

### d. Internet Contents

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

### e. Training Program

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

### f. Public Awareness Program

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

## 4) Changes and outcomes

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

**Table 1: Number of villages involved in each phase**

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

**Table 2: Statistics for outcomes (2001→2008)**

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

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

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

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

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

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

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

### 5) Challenges and success factors

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

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

### 6) International recognition and partnership with private enterprises

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

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

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

## Case 2: Local Government Information System (LGIN)

### 1) Overview of local Government structure in Korea

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

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

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

## 2) Strategies of the LGIN

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

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

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

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

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

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

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

## 3) Implementation

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

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

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

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

## 4) Outcomes and benefits

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

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

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

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

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

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

## 5) Towards more advanced local IT systems

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

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

## 6) Difficulties and success factors

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

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

– by the budgetary incentives provided by the informatization fund;

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

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

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

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

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

## 7) Lessons learned for the developing countries

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

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

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

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

– how to deal with the psychological burdens for those who accept the new technical system and their potential fear over job insecurity;
– how to avoid a big loss from potential failure due to the complicated implementation processes and large scale of nation-wide project;
– how to obtain the support from the political and governmental leadership in order to get favourable conditions for financing and revising relevant laws and regulations, and so on.

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

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

### 1) Introduction to e-Government in Bangladesh

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

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

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

### 2) e-Governance

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

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

### 3) Technologies and policies

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

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

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

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

## 4) Applications

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

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

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

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

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

## 5) Conclusion

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

# Case 4: Overview on ICT-based Services in Bangladesh

## 1) Introduction to e-Government in Bangladesh

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

– Key Statistics;

– Market and Industry Overviews and Analyses;

– Regulatory Environment and Development;

– Major Telecom Players (fixed and mobile);

– Infrastructure;

– Broadcasting (including Digital Media);

– Mobile Voice and Data Market;

– Internet, including VoIP and IPTV;

– Broadband (fixed and mobile);

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

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

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

## 2) Analysis of e-Government development

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

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

– Government-to-Government (G2G)

– Government-to-Business (G2B)

– Government-to-Employees (G2E)

– Government-to-Citizens (G2C)

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

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

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

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

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

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

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

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

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

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

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

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

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

### Mobile Phone Subscribers in Bangladesh

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

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

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

*PSTN Phone Subscribers in Bangladesh*

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

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

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

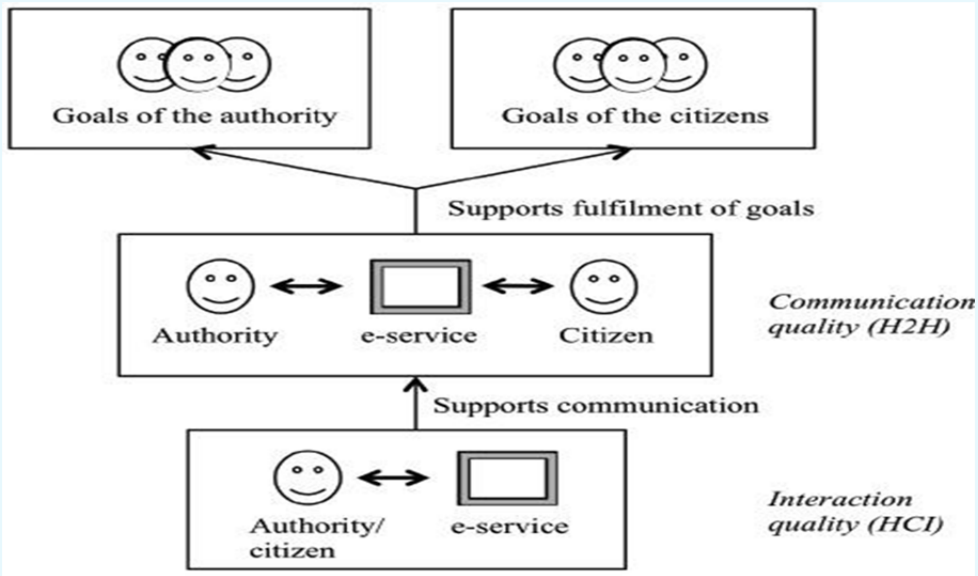
### Operators at service

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

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

## 3) Evaluation of Public e-Service

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




## 4) Applications

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

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

### 5) Conclusion

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

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

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

### 1) Overview

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

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

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

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

## 2) Objectives and strategies

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

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

## 3) Implementation and Technologies

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

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

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

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

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

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

## 4) Changes and outcomes

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

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

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

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

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

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

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

**Table 6: Global recognition for KONEPS**

| Awarding Organization | Award | Date |
|---|---|---|
| UN | UN Public Service Award<br>UN Public Service Award was established in July 2000 to raise public awareness of the improvement thereof. PPS was the first-ever awardee in the Asia-Pacific region. | June 2003 |
| OECD | Best Case for Effects on the Private Sector<br>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**

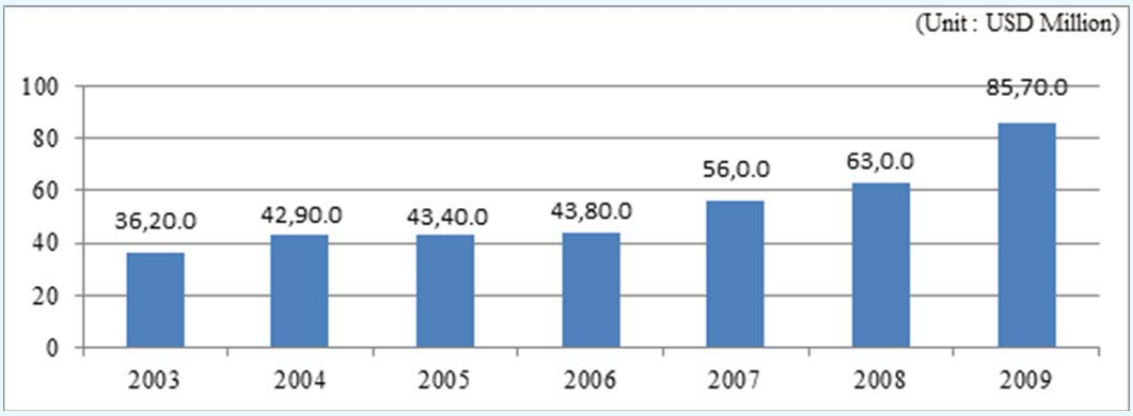
| Awarding Organization | Award | Date |
|---|---|---|
| UN | Best Practice Model in e-Procurement<br>KONEPS was selected as one of the best 23 practices in the world in the UN Global E-government Readiness Report 2004 | November 2004 |
| UN | KONEPS process reflected in UN/CEFACT standards<br>KONEPS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

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

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

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

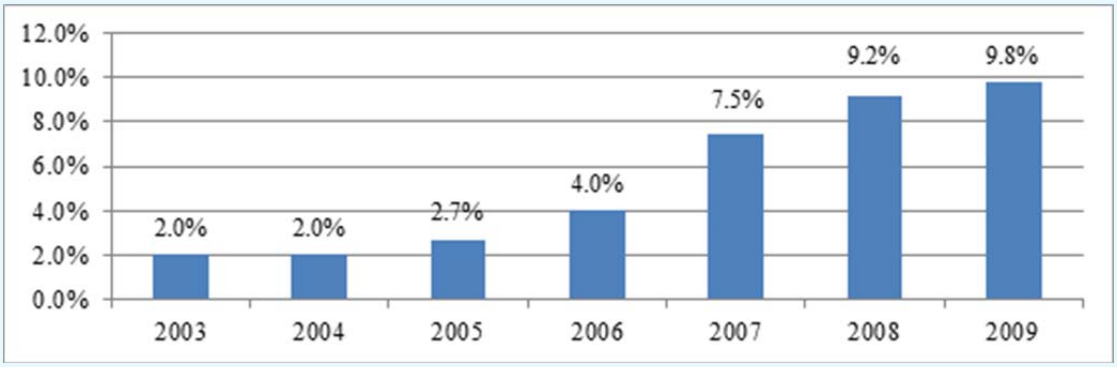
**Figure 1: Transactions via KONEPS**




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

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

**Figure 2: Use ratio of e-Contracting**




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

## 5) Challenges and success factors

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

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

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

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

## 6) Next steps

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

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

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

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

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

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

### 1) Background

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

### 2) Development of e-Government infrastructure

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

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

### 3) Legal framework

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

### 4) e-Government framework

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

a) Citizen-centric

b) Accessibility and choice

c) Trust, confidence and security

d) Better governance

e) Collaboration and integrity, and

f) Accountability

## 5) Public e-Government initiatives

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

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

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

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

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

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

## 6) Private e-Government Initiatives

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

a) Payment of utility bills using mobile phones

b) Money transfers using mobile phones

c) Payment of school fees using mobile phones

d) Checking of commodity prices using mobile phones

e) E-banking and mobile banking

### 7) Future envisaged applications

a) e-Procurement

b) e-Document sharing in government

c) Electronic passport processing

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

e) e-Education between urban and rural areas

### 8) Challenges

f) Cyber crime and cyber terrorism

g) Undefined cross-border jurisdiction for cyber litigation

h) Reliance on imported hardware and software

i) Reliance on foreign funding

j) Un-harmonised ICT Policies and Strategies

k) Inadequate Infrastructure

l) Adverse cultural beliefs and languages

m) Inadequate funding for ICT Projects

n) Inadequate human resources

o) Inadequate Public Private Partnerships (PPPs) frameworks

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

### 1) Introduction

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

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

### 2) Uganda's universal access policy framework

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

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

### a. Objective

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

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

### b. Broadband policy implementation

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

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

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

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

## 3) Expected benefits

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

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

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

## 4) Conclusions

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

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

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

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

### 1) Country overview

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

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

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

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

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

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

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

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

## 2) Background of e-government initiatives

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

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

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

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

### a. Analysis of the existing Governmental Information Systems and Databases

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

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

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

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

### c. Overview of the legal framework

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

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

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

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

## 3) Objectives and strategies

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

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

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

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

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

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

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

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

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

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

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

**Component A: Coordination of the E-Government implementation process**

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

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

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

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

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

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

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

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

**Component B: E-Government architecture and standardization**

CCICT will provide support to the development of the:

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

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

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

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

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

### Component C: Creation of the Population Register

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

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

## 4) Activities implemented

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

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

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

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

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

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

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

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

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

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

### a. Local self-governance area

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

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

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

### b. Support to election processes (2011–2012)

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

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

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

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

### c. Support to State Registration Service (SRS)

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

## 5) Changes and outcomes achieved

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

## 6) Challenges and success factors

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

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

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

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

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

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

Success factors are the following:

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

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

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

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

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

### 7) Lessons learned and next steps

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

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

### 1) Introduction

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

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

### 2) Overview

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

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

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

## 3) Objectives and strategy

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

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

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

## 4) Implementation

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

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

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

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

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

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

## 5) Outcomes

The outcomes achieved in response to such issues are below.

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

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

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

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

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

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

## 6) Difficulties

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

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

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

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

### 7) Lessons learned and follow-up

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

## Case 10: e-Government in Lebanon

### 1) Introduction and country overview

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

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

The four e-Government strategy pillars

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

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

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

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

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

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

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

## 2) Objectives and strategies

### a. Objectives and vision for e-Government in Lebanon

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

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

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

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

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

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

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

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

### b. Strategies and underlying principles of e-Government

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

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

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

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

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

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

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

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

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

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

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

– The program of reinforcing governance, accountability and transparency.

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

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

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

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

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

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

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

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

### c. E-Government scope

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

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

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

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

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

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

## 3) Activities implemented

The Activities implemented are listed below:

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

**June 2011 to October 2011**

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

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

**April 2012 to July 2012**

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

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

The civil works for this project have been completed

### c. Government Data Center physical infrastructure – Portal

**June 2012 to August 2012**

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

The Data Center is expected to provide the following benefits:

– Resources are housed in a single location

– Optimal Management of resources

– Efficient Provisioning of applications

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

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

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

**December 2011 to present**

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

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

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

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

### e. Unique ID Number

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

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

## 4) Technologies and solutions deployed

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

## 5) Lessons learned and next steps

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

### a. Project of Law – Electronic Transactions

This law is meant to address the following different elements:

– Banking Transactions
– Electronic Payments

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

**b. Draft Law – IT salaries scale law**

This draft law integrates the following elements:

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

**c. E-Transactions Law Adoption**

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

**d. Simplification of Procedures**

This project includes the following activities:

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

**Implementation of the Action Plan**

It will start beginning 2013 for four Ministries:

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

**e. Reengineering of licenses at Ministry of Tourism**

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

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

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

**g. The Assistance on Simplification of Administrative Procedure:**

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

**h. E-Government Interoperability Gateway – Government Service Bus**

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

## Case 11: MWANA (Zambia)

### 1) Introduction

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

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

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

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

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

### 2) Country overview

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

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

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

## 3) Objectives and strategies

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

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

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

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

## 4) Activities implemented

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

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

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

**d.** Scaling the project nationally between 2011and 2015.

## 5) Technologies and solutions deployed

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

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

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

## 6) Changes and outcomes achieved

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

## 7) Challenges and success factors

### a. Challenges

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

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

– 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

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

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

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

### Technologies and solution deployed

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

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

### Objectives and strategies

– Develop and implement information technology policy.

– Coordinate information technology investment strategy and capital planning.

– Develop and implement Enterprise Architecture.

– Implement Data Management program.

– Identify and oversee business process improvement opportunities.

– Develop and implement information technology performance measures.

- Oversee the Department's Reports Management Program, including the Information Collection Budget.
- Develop and implement electronic government in compliance
- Manage systems integration and design efficiency.
- Analyse information technology skills for all employees including executives, end-users, and IT professionals.
- Develop and execute IT Governance and Investment processes.
- Coordinate, develop, and implement IT Security computer policy and procedures.
- Manage information technology operations.

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

**Table of contents**

# 0 Introduction

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

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

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

# 1 E-Government Delivery Models – Use of Mobile Terminals

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

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

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

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

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

– Mobile communications are not less secure than the Internet.

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

– m-Powering Development

– m-Health for NCDs (jointly with WHO)

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

– Government-to-Government (G2G)

– Government-to-Business (G2B)

– Government-to-Employees (G2E)

– Government-to-Citizens (G2C)

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

## 2 G2C Activities

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

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

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

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

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

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

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

### Two-way communication between the Agency and the Citizen

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

### Financial Transactions

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

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

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

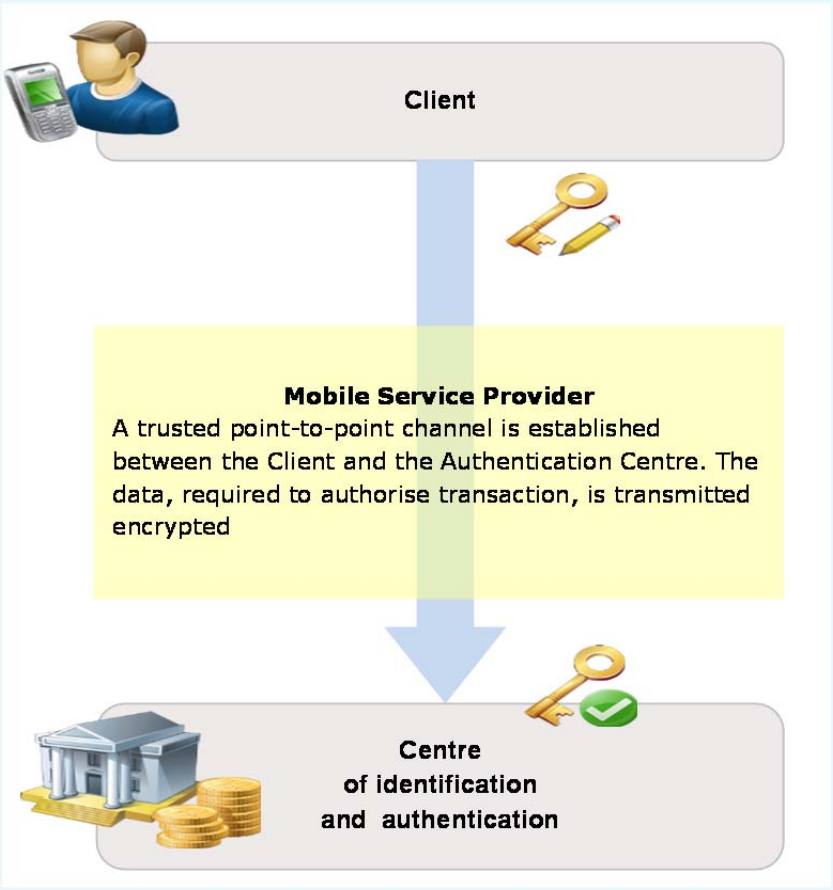
# 3 General Principles for Secure Mobile Services

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

## 3.1 Identification and authentication

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

**Figure 3: Infrastructure of secure data transmission**



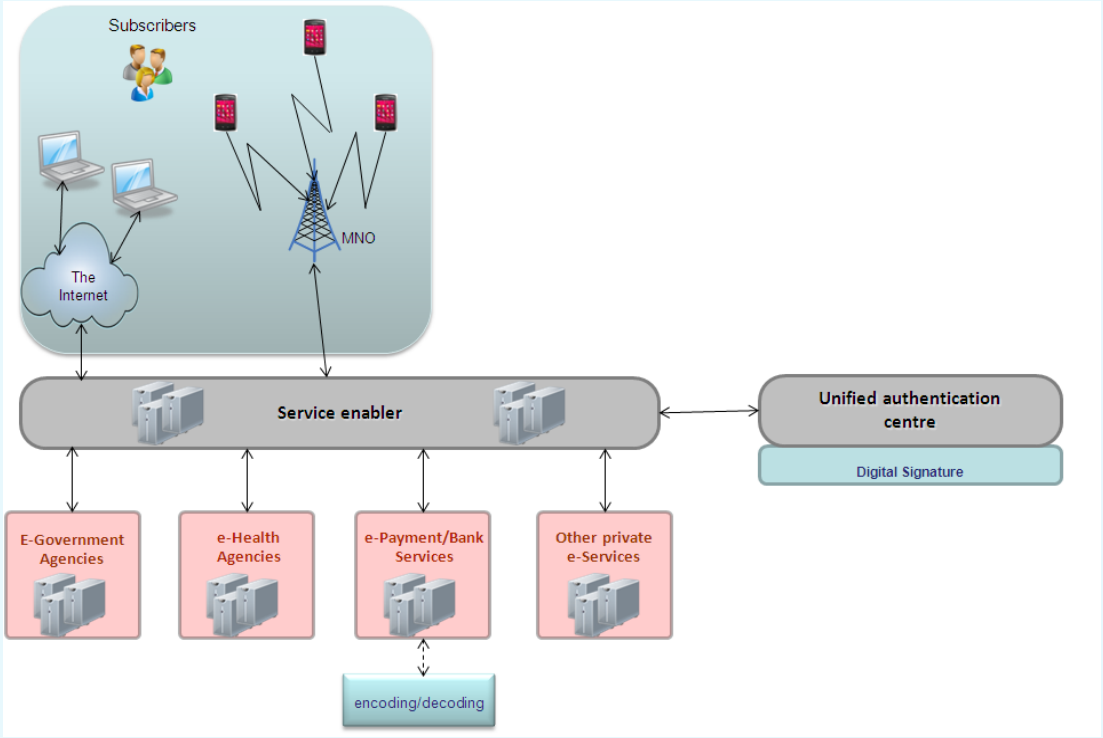

Existing mobile payment systems have already implemented their own security procedures, where security requirements are determined by agreements between service providers and their customers. Obviously, e-government requires a security system, controlled by the State and compliant with national law regulations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

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

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

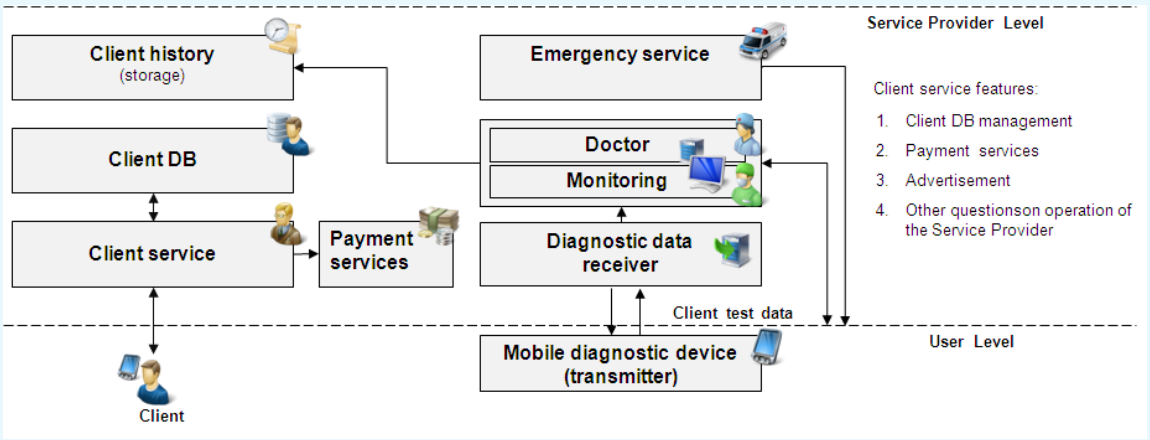
All identification and authentication centres must comply with the same allocation rules and regulations for global identifiers of mobile clients (mID), registered in a central System Directory to ensure message delivery to customers.

**Figure 4: Unified authentication model with additional cryptography**




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

**Figure 5: The structure of a separate medical service provider**




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

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

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

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

4) Insufficiency of authentication and protection of personal data

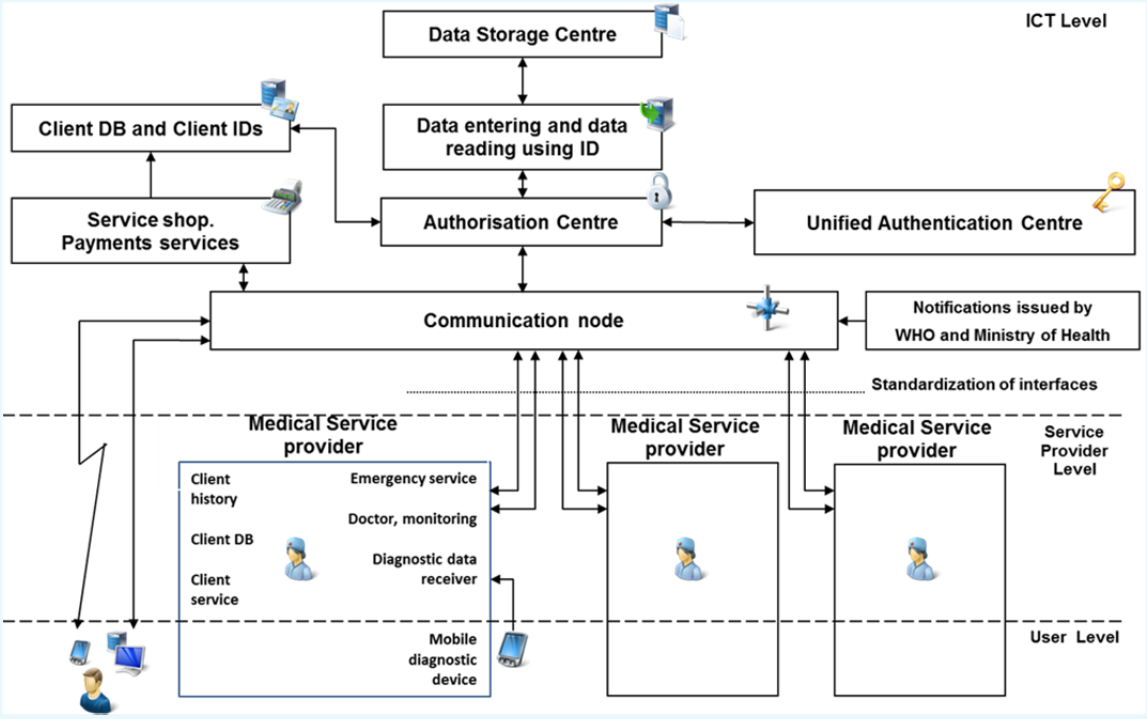
5)In case the Service Provider ends its activity, the Client history will be lost

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

At the Service Provider level, there are different medical clinics, both state and private. They may have multiple specialisations and emergency services (if needed). These clinics may provide their clients with

special mobile diagnostic devices, collecting and transmitting health parameters of clients to central devices.

**Figure 6: Proposed structure of the State healthcare system**




## 3.2 Keys administration

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

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

primary function is to acknowledge the unique relationship between private key usage and the registered identity of the Citizen by virtue of his/her ownership of the associated public key.

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

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

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

# 4 Mobile Payment System (MPS)

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

## 4.1 MPS participants and their Roles

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

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

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

– Issuers of Client applications

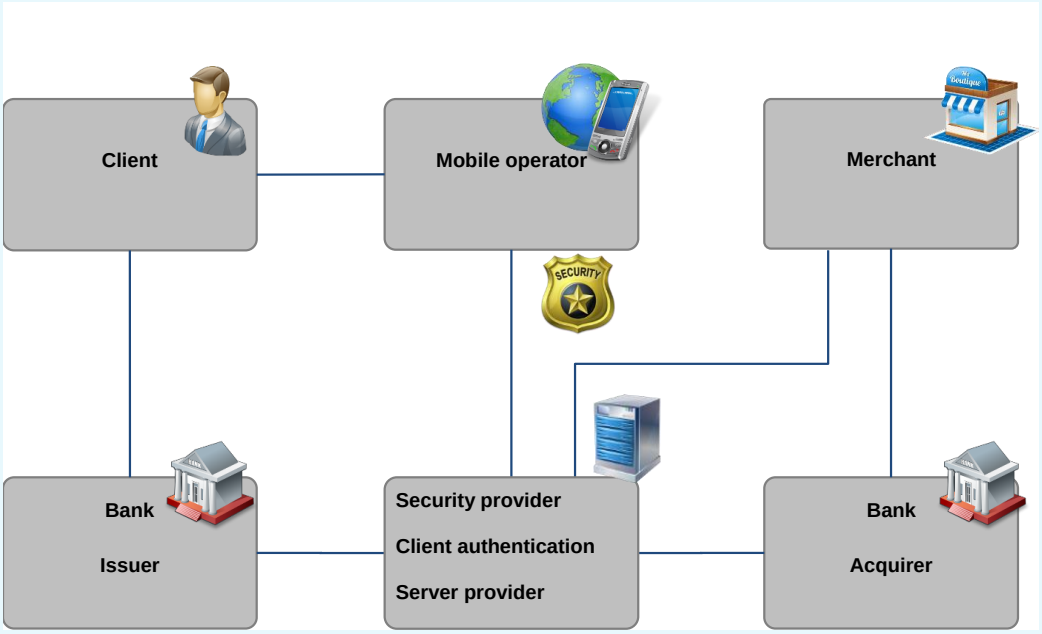
– Merchants (legal entities, clients of Acquiring Banks)

– Authentication agent (Client authentication)

## 4.2 Typical System Architecture

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

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

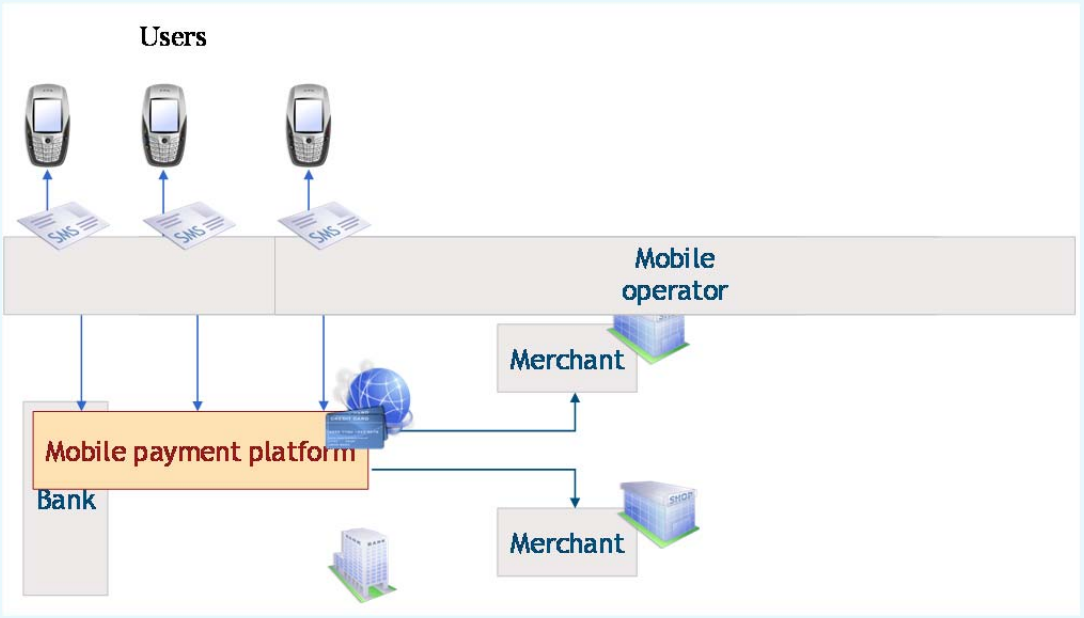



## 4.3 MPS Models

Different MPS models exist:

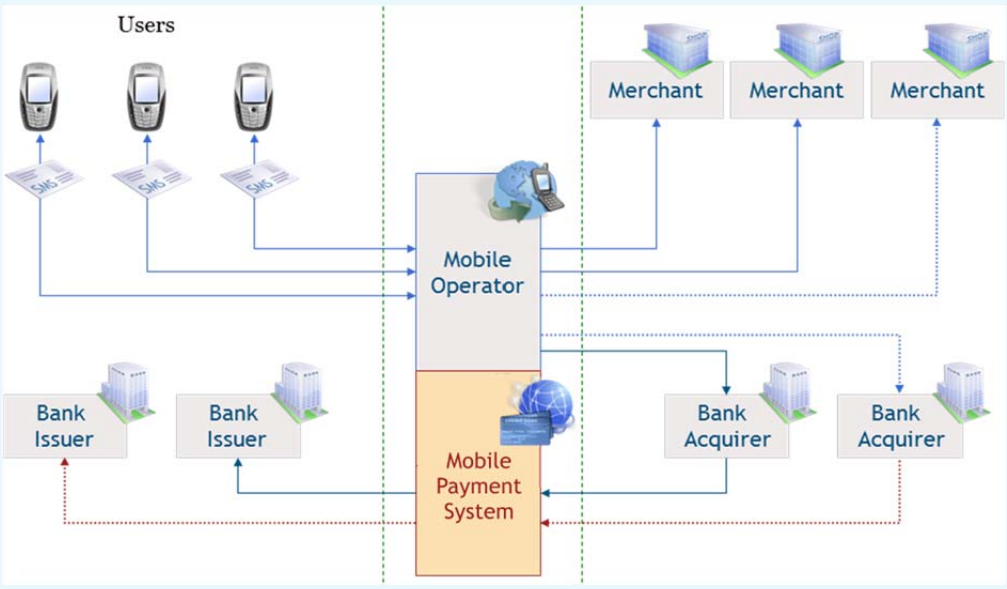
– Bank-oriented model (Figure 8), where bank offers mobile payment services with many mobile operators.

**Figure 8: Bank-oriented MPS model**




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

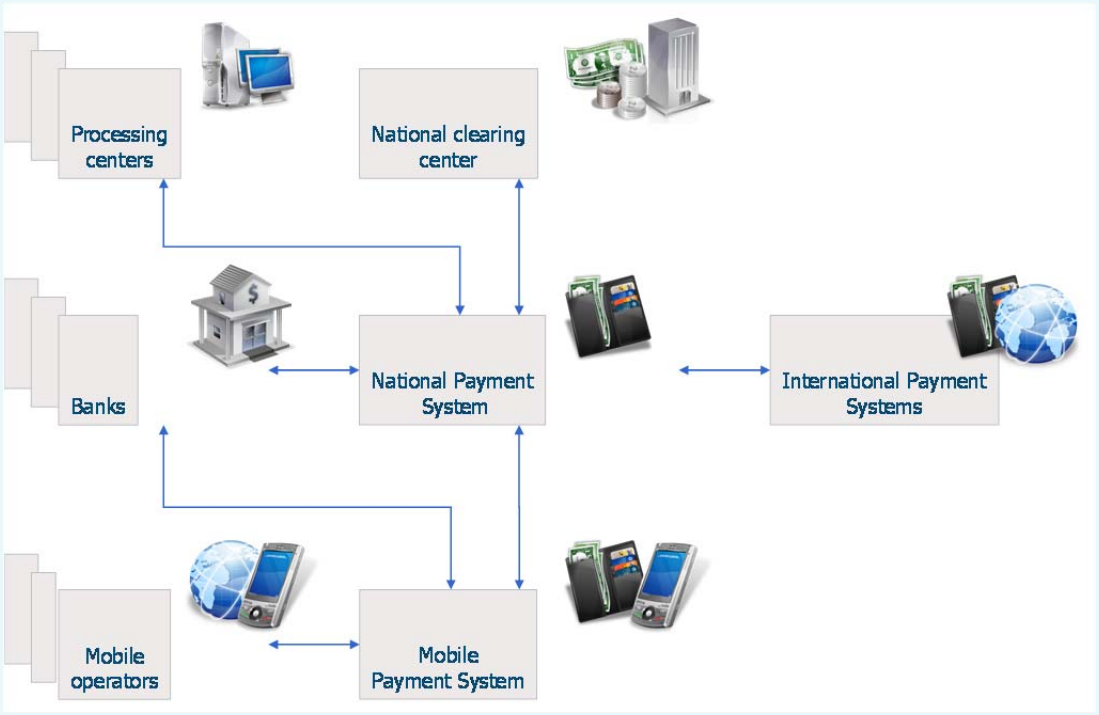
**Figure 9: Operator-oriented MPS model**




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

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

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




## 4.4 Available payment means

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

– Bank account

– Bank cards issued by local or global payment systems

– MNO subscribers personal accounts

– E-money

## 4.5 Payment arrangement

Two operation types are available in MPS:

– Operations initiated by the Client

– Operations initiated by the Merchant

### *4.5.1 Operations initiated by the Client*

Transactions initiated by the Client may contain the following steps:

1. By means of mobile device the Client generates a request containing parameters of the financial operation, payment instrument and secret PIN code
2. The request is transmitted via mobile operator channels
3. The MPS operator receives the request
4. The Client is authenticated

5. The required financial operation is performed using the Client's payment instrument details
6. The operation result is sent to the Client
7. The response is transmitted via the mobile operator channels
8. The Client receives the result of the financial operation

### *4.5.2 Operations initiated by the Merchant*

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

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

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

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

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

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

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

g) Authentication of the Client;

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

i) The operation result is sent to the Client;

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

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

## 4.6 Near Field Communications (NFC)

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

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

– Mobile Device with NFC Chipset or Secure Element of NFC Chipset containing the logic and interfaces to communicate with card readers.

– Mobile Network Operator (MNO)

– One or many Service Providers

– Trusted Service Manager or broker providing a point of contact between service providers and MO

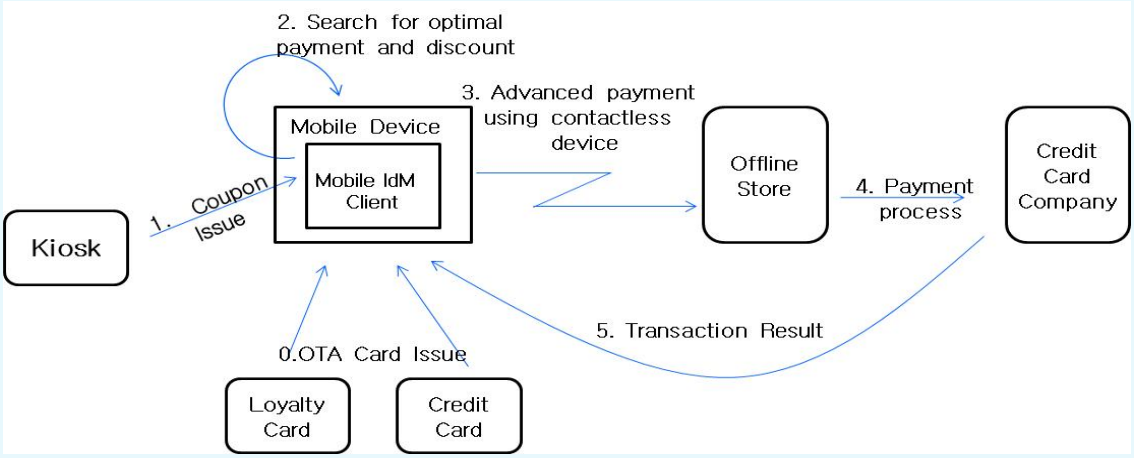
It is considered, that NFC payment systems can use credit cards as payment means for interactive shopping purchases via contactless NFC devices. After the payment transaction is processed successfully, result is stored in the system and sent to subscriber's handset. The use case is depicted in Figure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

– User Authentication Communication security

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

– System storage to accumulate and process transaction records

**Figure 11: Interactive shopping**




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

## 5 Security

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

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

a) End-point Security

b) Mobile Application Security

c) Mobile Network Security

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

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

The term "security" is used in the sense of minimising vulnerabilities of assets and resources. An asset is anything of value. Vulnerability is any weakness that could be exploited to violate a system or information

it contains. A threat is a potential violation of security. The ITU-T Recommendation X.805 "Security Architecture for Systems Providing End-to-End Communications[7]" (Figure 10) of defines set of eight so-called "Security dimensions" – set of means that protect against all major security threats, described in the ITU-T Recommendation X.800 "Security architecture for Open Systems Interconnection for CCITT applications"[3]*:*

– destruction of information and/or other resources;

– corruption or modification of information;

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

– information disclosure;

– service interruption.

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

1) Access control;

2) Authentication;

3) Non-repudiation;

4) Data confidentiality;

5) Communication security;

6) Data integrity;

7) Availability;

8) Privacy.

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

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

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.

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

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.

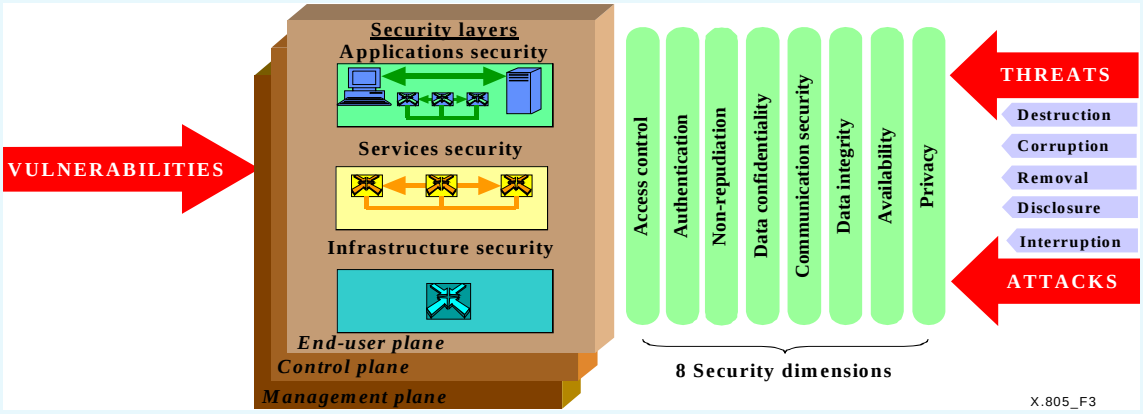
Each of these security Layers consists of three security Planes, representing a specific type of network operation, protected by Security dimensions:

– 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;

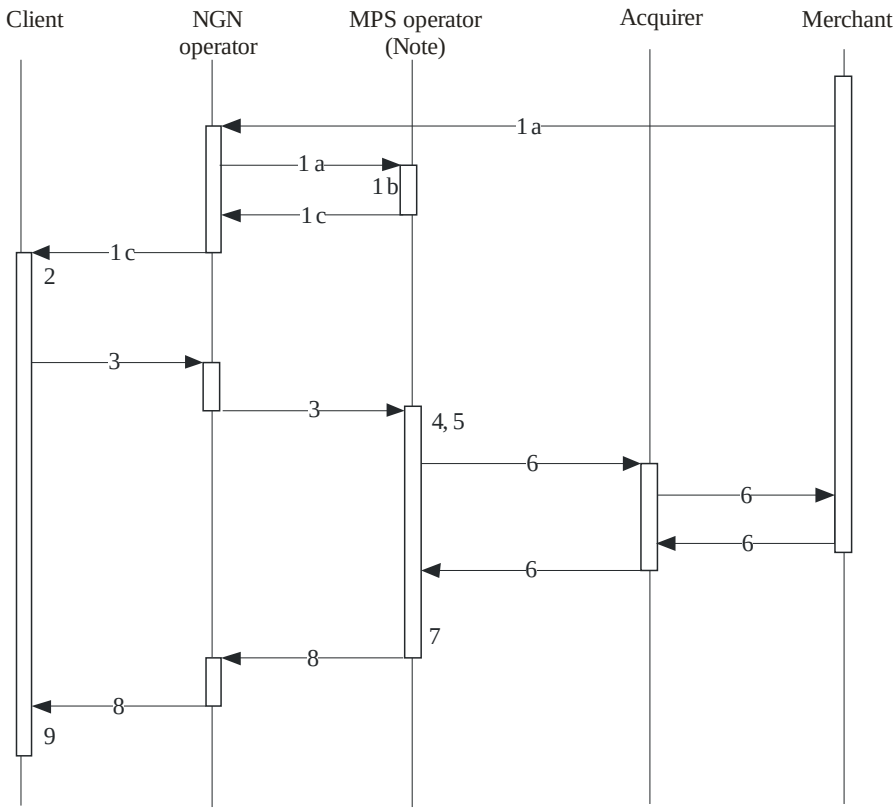
– Encryption of data transmitted through communication channels;

– 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**




**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.<br>Multi-factor authentication at the System services usage.<br>Obligatory usage of Hardware Cryptographic Module. |
| Non-repudiation | The impossibility of a transaction initiator or participant to deny his or her actions upon their completion is ensured by legally stated or reserved in mutual contracts means and accepted authentication mechanisms. All system personnel and end-user actions shall be logged. Event logs shall be change-proof and hold all actions of all users. | | | |

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

<table>
<tr><th rowspan="2">Security Dimension</th><th colspan="4">Security Level</th></tr>
<tr><th>Level 1</th><th>Level 2</th><th>Level 3</th><th>Level 4</th></tr>
<tr><td>Data confidentiality</td><td colspan="2" rowspan="2">Data confidentiality during the data transfer, is ensured by the data transfer environment (communications security), and by the mechanism of data storage together with the means of system access control – at data storage and processing.</td><td rowspan="3">Data confidentiality during the data transfer is ensured by additional message encryption together with data transfer protocols that ensure the security of the data being transferred by the interoperation participants (including data integrity verification); at data storage and processing their confidentiality, integrity and privacy are ensured by additional mechanisms of encryption and masking together with well-defined distribution of access in concordance with privileges and permissions.</td><td rowspan="3">The implementation of the Level 3 requirements with the obligatory usage of hardware cryptographic and data security facilities on the Client’s side (Hardware Cryptographic module).</td></tr>
<tr><td>Data integrity</td></tr>
<tr><td>Privacy</td><td colspan="2">Privacy is ensured by the absence of sensitive data in the messages being transferred as well as by the implementation of the required mechanisms of data storage and the System access control facilities.<br>The System components must not have latent possibilities of unauthorized data acquisition and transfer.</td></tr>
<tr><td>Communication</td><td colspan="4">The delivery of a message to the addressee is ensured as well as the security against unauthorized disclosure at time of transfer over the communications channels. It is ensured by the NGN communications providers.</td></tr>
<tr><td>Availability</td><td colspan="4">It ensures that there is no denial of authorised access to the System data and services. Availability is assured by the NGN communications providers as well as the service providers</td></tr>
</table>

# 6 Mobile Technology

To date, the term "mobile communication" is most often associated with the GSM Standard of the second and the third generations. These mobile communication systems use different subsystems for voice and data transfer (with the use of time-division switching and packet switching technology) and this is an intermediate step in evolution of mobile communications. Next Generation Networks (NGN), which has already come to replace existing networks, provides subscribers with broadband access and use only packet switching channels technology.

NGN perform voice, images, text and multimedia messages transmission services, as various applications of universal process of Batch Data Transmissions. As a result, SMS and MMS data transmission technologies, widely used at the present time, may yield to other technologies. Users may not even notice these changes. However, technological solutions developed for m-services should be prepared for the process of evolution of mobile communications.

Today's mobile terminals are widely used, but originally they were not designed for systems with strong authentication. Therefore, terminals of different manufacturers and even different models of terminals made by the same manufacturer may use different algorithms, which lead to greater complexity, and in some cases – to inability to create Applications which perform all required System functionalities. For instance, an application should be able to be activated automatically upon receiving a message from

Mobile Payment System (Operations initiated by Merchant). Unfortunately, it cannot be implemented in every mobile terminal.

To unify operation of such systems, some additional protocols should be standardised and ITU, together with equipment manufacturers, can perform this task. Another important challenge is the location of crypto-application and administration of access to this application. As it is shown in the chapter "Security", in order to achieve the highest level of security, these applications should be located in a special module (hardware security element), which protects stored information from unauthorized access. Thus, SIM/UICC card can be successfully used as a module, provided that the problem of delegation of administrative rights to access SIM card, belonging to the mobile operator, will be solved. This problem is easily solved when both of these functions are performed by the same entity, otherwise it becomes difficult. Creation of mobile terminals equipped with an additional hardware security element can be considered as a solution to resolve issues resulted from SIM card co-management. This may be reached by an embedded security module or specially installed tamper-resistant memory card.

There are different ways of data transfer available in mobile networks, such as CSD, SMS, USSD, GPRS, EDGE, LTE. Each of them has its advantages and disadvantages. For example, SMS is very reliable and easily implementable way, but limited by message length. On the contrary, GPRS is not limited by message length, but less reliable and requires correct adjustments for mobile terminal, especially in roaming, which is also very expensive.

The success of technology progress has led to wide implementation of geo-location services in smartphones based on GPS or GLONASS systems. Geo-location essentially expands functional capabilities of mobile terminals. Therefore, lately geo-location services are widely used in applications for mobile devices (where the share of smartphones grows rapidly).

# 7 M-Government in the European Union

According to "Mobile Signatures Whitepaper: Best Practices[10]", issued on 25th April 2010, the most advanced national m-Government services, based on Digital Identity systems using cryptography techniques are implemented in Turkey and Estonia. Also, Finland is a top-ranked leader in the field of e-ID, including mobile PKI, which is seen as a great alternative for strong and flexible user authentication and electronic signature service.

Mobile PKI offers a very strong security framework for all parties. The security related operations are done in the SIM card, tamper resistant environment, making it almost impossible to misuse the user identity. Software that tries to steal the user identity, passwords or other credentials cannot penetrate into SIM content. Authentication and signature information are transmitted via SMS and back-end channels to the service provider and are verified by the operator, so even if the user is attacked at the browser level, or the computer is infected, it does not matter. The data never goes through the Internet channel. To be successful, attacker should also gain access to the mobile operator network to attack/infect the encrypted SMS messages.

All of these services are using asymmetric cryptography techniques and based on European Parliament and Council Directive on Electronic Signature and ETSI Mobile Signature Requirements and Specifications:

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

[4] ETCI TR 102 203 "Mobile Commerce (M-COMM); Mobile Signature; Business & Functional Requirements" (page 19).

– ETCI TS 102 204[5]
"Mobile Commerce (M-COMM); Mobile Signature; Web Service Interface".

– ETCI TR 102 206[6]
"Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework".

– ETCI TS 102 207[7]
"Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services".

Mobile signature is *"A universal method for using a mobile device to confirm the intention of a citizen to proceed with a transaction."* It is an enabling technology that allows remote or present authorisation of electronic events using a mobile phone. Mobile Signature can carry legally valid identity information (qualified digital certificates) of over a GSM network and provide that information to any authorised application. According to documents, mentioned above, mobile signatures are digital signatures that are created using private key data that is stored on the UICC; so it can be used to provide legal and ultimately secured transactions. Essentially, Mobile Signatures extend the concept of Digital Identity and encompass the mobile phone as main device for authentication. Mobile Signatures can, in principle, be applied to any electronic event that requires authorisation by a nominated individual or by a member of a defined group of individuals. Mobile Signature is an important building block for secure services, which helps service providers to identify and authenticate users, and also may be used to sign secure transactions.

**Figure 14: Typical mobile smartcard implementation**


Modern communications and e-commerce are largely built on a solution, i.e. Internet that was built without an identity layer that would allow each party to identify their communicators. 'Identity' leads to the development of trust models that are so important to the functioning of current societies. By establishing a Public Key Infrastructure (PKI) and providing digital certificates and keys to end users on a mobile phone UICC (Wireless PKI), digital identity can be established thus enabling the delivery of new and enhanced features and services For example, virtual access to Internet resources, financial transaction authorisation or electronic document signing. It should be noted that Digital Identities are not necessarily unique as one identity may be used by more than one person as in the case of joint signatories or members of shared groups with equal authority to access a resource or service. Also one person may

[5] ETCI TS 102 204 "Mobile Commerce (M-COMM); Mobile Signature; Web Service Interface" (page 19).

[6] ETCI TR 102 206 "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework" (page 19).

[7] ETCI TS 102 207 "Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services" (page 19).

have multiple digital identities for different services. Identity Management System (IDM) not only provides a structure for storing identity but also provides assurance that the right people have the right access at the right time. Essentially the systems provide authentication, authorisation and administration. Authentication ensure that the requesting application or individual is who they say they are; authorisation determines what they are allowed to access; and administration deals with the routine maintenance, ensuring that the system works and that integrity is ensured.

Security is greatly increased due to the use of UICC in secure chain of events and also due the nature of services which will typically require two “points of presence” in the transaction chain, i.e. Internet portal access from the computer will also require the user to authorise the event from his mobile phone. If the mobile phone user, phone (UICC) and the originating event are not all present, the activity will not be possible. Further, information required to perform an event, for example, account information, can be transmitted over different channels thus disassociating it from the originating service and reducing the risk of fraud.

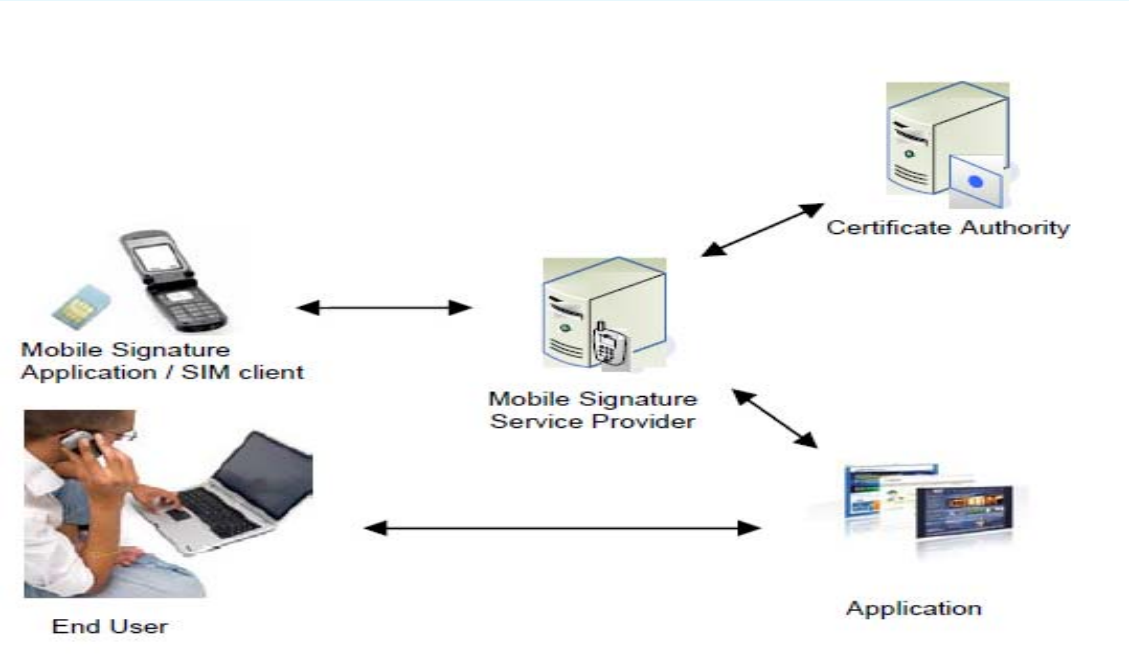
Mobile signature creation is achieved using a crypto-processor on a smartcard, such as Subscriber identity module (i.e. SIM card) found inside GSM mobile handsets or the Universal Integrated Circuit Card (UICC) that has been adopted for 3rd Generation mobile devices (Figure 12). The use of SIM or UICC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

Signature requests, received on citizen’s mobile device, trigger a "signing" application on a smartcard. This allows the display of the transaction text on the mobile device screen and provides an option for the citizen to enter his/her signing PIN. The fact of entering the correct PIN initiates creation of the mobile signature in the smartcard and transmission of the signature to the mobile signature service. By entering the correct signing-PIN, citizen is deemed to have confirmed his/her intention to proceed with transaction details displayed on his/her mobile device screen.

In the solution described above, Mobile Signature extends PKI authentication technology to the Mobile Phone environment (WPKI) and positions the SIM/UICC card along with the mobile phone as the main device in the service chain. Below a simplified process flow for the User to access a Service Provider is described (see Figure 13):

– The User shall access the service via the Internet browser.
– Internet service requests the User to input the account name or a similar account identifier.
– Internet service identifies that the User has the Mobile Signature and initiates an authorisation request to the relevant Mobile Signature service provider (MSSP).
– MSSP sends an SMS to the SIM Client on the User’s mobile phone, which requests a Mobile Signature from the User.
– The User enters the signature PIN code.
– Mobile application sends Mobile Signature to MSSP.
– MSSP sends a request to the Certification Authority, which shall verify the Mobile Signature.
– MSSP returns a positive confirmation to the Application.
– The User is authorised to enter the service menu at the Internet site.

**Figure 15: Use of the 2nd "Point of Presence"**




### Roles

The following describes the roles of MSSP, Registration Authority and Certification authority.

These are described in greater detail in ETSI TS 102 203.

### Role of MSSP

MSSP is in charge for service facilities it provides. MSSP may be required to demonstrate compliance to contractual agreements (where they exist), including active management of:

– Preparation of a documented security policy.

– Prevention of unauthorized Access to databases, etc.

– Detection of unauthorized access to databases, etc.

– Implementation of processes to monitor vulnerabilities.

– Actual monitoring for system vulnerabilities.

– To record and retain system information sufficient to perform security audits and investigations.

– To record and retain security audit reports.

MSSP may also be in charge for physical elements used in the delivery of services they provide (e.g. mobile equipment). This may include (but not be limited to) of the following elements:

– Provide assurance that "what the user sees is what the user signs …"

– The PIN should be erased from all memory after being transmitted to the card.

– A card with which no interaction occurring should be powered off after a prescribed timeout.

– No application capable of mimicking user screens should be installable in the mobile handset.

– No application capable of disclosing the PIN (e.g., Capturing it and sending it via SMS) should be installable in the mobile handset.

– The keying in of the PIN should not generate DTMF signals (a malicious party eavesdropping on the communication could then determine the PIN even if the PIN itself is not transmitted out of the mobile handset!).

– Users may have the ability to customise the screens displayed by the mobile handset goal being to avoid confusing the user with a fake mobile handset whose sole function is to capture the PIN).

– The signature and the signed message should be erased from all memory after use.

– Entering the PIN may result in display of a sequence of characters unrelated to the PIN's value or length.

– The human interface should be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

– All software running on the mobile device should be immune to buffer overrun attacks.

– Citizens may have the ability to terminate the mobile signature service from the mobile device (e.g. in emergency/distress situations).

**Role of the Registration Authority (RA)**

The RA is responsible for acquiring and validating personal information provided by potential users. The process of acquiring this information is called the Registration Process (RP).

**Role of the Certification Authority (CA)**

The CA is responsible for processing information from the RA and certifying public keys of citizens who intend to use the mobile signature service. In addition, CA will provide a certificate revocation service (i.e. to manage mobile signature lifecycle and permit audit transaction investigations).

**Benefits for the service provider**

One of the biggest advantages for the service provider is cost efficiency. According to the Tax Administration in Finland, the cost for a single transaction went down from of €10 - €50 to of €0.20 - €0.50 per transaction, when they adopted on-line services. Cost savings for the service provider, even in a small nation such as Finland, can be huge.

These on-line services are under constant threat. On-line crime has turned into highly professional business. The service provider needs to protect its own assets and give users the assurance their information is also protected. User’s trust is a key for the service provider. Today, passwords to protect customers and their data are not enough to establish trust with the customer. They may even discourage potential customers, slow down adoption and eventually kill the service. More and more services are going into the cloud, and the normal authentication is “username + password”. Security breaches in these kinds of services are not breaking news any longer. Online services that offer alternatives gain competitive advantages over others.

Strong authentication is one way of mitigating some of the risks related to on-line services and Mobile PKI offers one of the strongest and easiest ways to authenticate the end user. Another aspect in on-line business is transaction protection.

There are several potential threats when a high-level transaction is performed in on-line service. Mobile PKI offers two distinctive advantages over other methods:

– Transactions are signed using a method that complies with the EU electronic signature directive and making signatures legally binding;

– The transaction and the identity of the user are protected against even the most sophisticated attacks. Pretending to be someone else requires access to both the service and the operator network. This is not an easy task to do. New on-line services can be delivered in a favourable environment with minimal risks as they will be protected from fraud from the start.

### Benefits for mobile network operators

Mobile network operators have to get the best ROI from their investments. They have to create new opportunities and generate revenue. Mobile PKI enables both. One of the issues service providers are struggling with is the mobilisation of the user base. Users crave for services that are available 24/7, reachable from almost anywhere and at the same time they need security. Mobile PKI offers both. For the MNO it creates new opportunities in several ways:

– adds value to current services;

– can secure new products and services to attract new customers;

– can stimulate new business models;

– can strengthen customer loyalty.

For revenue opportunities the MNO can investigate these different options:

– Negotiate high volume, special priced authentication transactions for e-Government, corporate or financial services;

– Produce new services and integration options for the end user organisations;

– Offer trust centre-type of services to other organisations;

– Generate transaction revenue in services requiring transaction verification (electronic signing).

Mobile PKI creates a wealth of new opportunities. For the MNO, it means offering new and innovative services to its existing customer base, targeting completely new customer segments and use cases where MNO presence was previously only through the subscriber base.

A micro loaning service and a pension fund provide Mobile ID authentication for their users. The Lahti municipality uses Mobile ID to authenticate people accessing several different online services. The National Board of Patents and Registration of Finland allow users to access the services using Mobile ID.

Every week new service providers join mobile PKI revolution and create more value for the stakeholders in the mobile PKI ecosystem. The main beneficiary being is the end user.

### Benefits for the Government

Mobile ID enables governments to put the citizen electronic ID into every pocket that can hold a mobile phone. Complementing the national eID card the mobile PKI SIM card adds a true mobility factor into the e-Government services. Now citizens can access services from all over the world, only thing needed is a working SMS connection.

One of the biggest challenges in the market has always been the threshold in user acceptance. If the solution is too complex, citizens may shy away from it. Using the mobile phone as a signing and authentication device is natural for almost all users, and when it is done using a SIM card one can also see it as the most democratic method of all – it can be available to anyone who has a mobile phone. Mobile PKI truly brings power to people's fingertips!

Mobile ID provides also the capability to digitally sign documents. When using the EU directive as an example Mobile ID can be used to produce advanced electronic signatures.

### Benefits for the End User

Extreme mobility is the most obvious benefit for the user. As Mobile ID is managed in the SIM card on the client side, it can be used within almost any mobile phone out in the market.

Mobility is one of the key features that the MNO and service provider also see as a great benefit for the end user. Due to Mobile ID, the end user has a strong authentication method available in his/her mobile phone. An easy-to-use PIN is required to use the keys stored on the card for authentication or signing. This is extremely important as mobile phones have been part of daily lives for many people all around the globe.

With Mobile ID, value of the mobile phone increases even more. Besides games, entertainment, web access or banking applications, it offers remote electronic identity tool, that always available for the user, strong authentication, and consent through secure electronic signature, secure banking access, age verification, and much more.

Mobile ID can open up a multitude of new possibilities for the benefits of users, mobile operators and service providers.

Recently, European system that serves to provide mobile signatures was adopted by non-EU countries, such as the Republic of Moldova. Long-term experience of successful operation of the system and its global penetration show real attraction of this solution, however, most likely, in the long term the encryption algorithm RSA-1024 will not meet tamper resistance requirements and probably will be replaced with some more complicated algorithm, which will require, as it was stated above, to use more powerful processors. However, most likely, progress of mass production technology will allow not to increase costs of UICCs.

# 8 Case Study in Japan

In Japan, number of domestic subscribers of mobile phones, having been increasing year by year, was 128.21 million (up of 7.3 % of from last year) by the end of FY2011[15]. The mobile phone is an important infrastructure to support economic and social activities and the daily lives of the people.

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

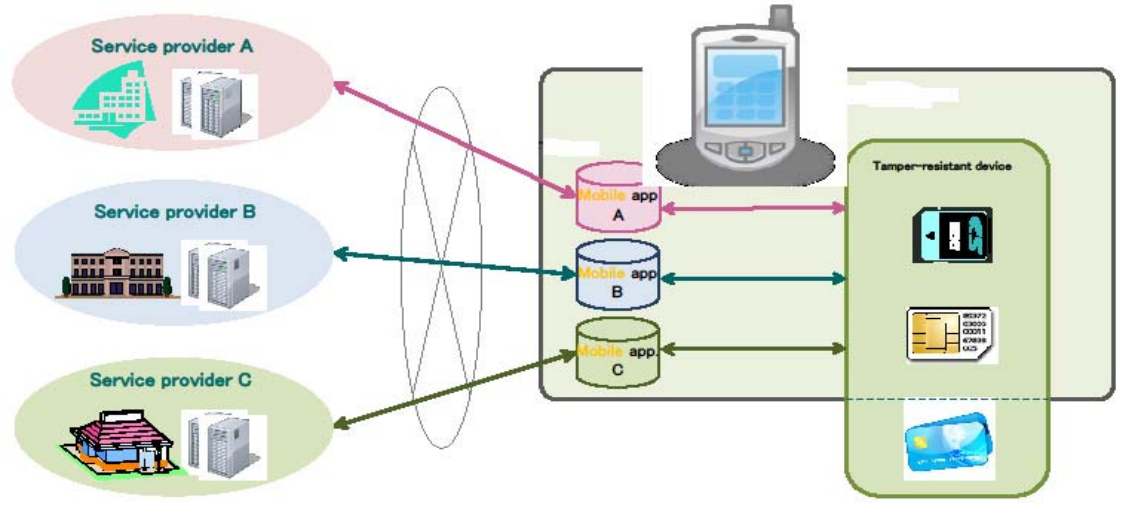
The government of Japan, in “The New Strategy in Information and Communications Technologies (IT) Roadmaps” (suggested in June 2010, revised in August 2011 and in July 2012) made by The Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (director-general: prime minister), presents the following goals regarding programs to diversify methods to access administration services, concerning the renovation of the government portal, and to encourage people to access the governmental service: in 2011, deliberation, verification, and demonstration of methods for mobile access to administrative services with authentication from mobile phones; from 2012 to 2013, based on demonstration, to introduce, develop and promote services partially in testing areas based on the demonstration above, and gradual nationwide deployment; by 2020, realisation of highly convenient electronic administration services, namely a 'one-stop service'.

Based on the roadmap, for the purpose of technical specification review and technical verification toward the realisation of the underlying mobile access system for using Web services through mobile phones in the field of public administration, ministry of Internal Affairs and Communications conducted the “Project Promoting Cooperative Business Administration Systems (Verification of Ways of Improving User-Friendliness for Mobile Phones as Means of Access)” in 2011, based on survey and research results from

the (Commissioned) “research and study of the diversification of means of access to electronic administrative services, etc. (research and study of technology for mobile phones to access electronic administrative services, etc.)” conducted in 2009 (Contracted).

As discussed above, mobile terminals with NFC functions are going to be commercialised from FY 2012. They realise both offline and online enclosure, into tamper-resistant devices (Devices equipped with an IC chip having a function to protect internal of physical or theoretical information), of service users’ personal information, in the form of authentication information such as ID/passwords, points and coupons, and enable the information to be read. However, at present, in order to store and use ID information or users information in tamper-resistant devices, it was necessary to develop and operate an application for mobile phones (hereinafter, “mobile app”) for each service provider. Also, users need to download and install separate mobile apps provided by service providers. In other words, both service providers and users face inconvenience when a tamper-resistant service is provided (Figure 16). For the purpose of creating an environment convenient for users, in which it is easy for service providers to provide and operate, we examined technical specifications to realise the mobile access system.

**Figure 16: Separate application for each service provider in a tamper-resistant device**




In order to resolve the difficulties mentioned above, system, that users and service providers alike could commonly utilise, was studied. In other words, it was studied the technical specifications of a mobile access system consisting of servers for storage and safe reading instead of each service provider and a mobile app utilised commonly for every service to store and use ID information in tamper-resistant devices (Figures 17 and 18).

**Figure 17: Common application and unified mobile access server for all service providers**

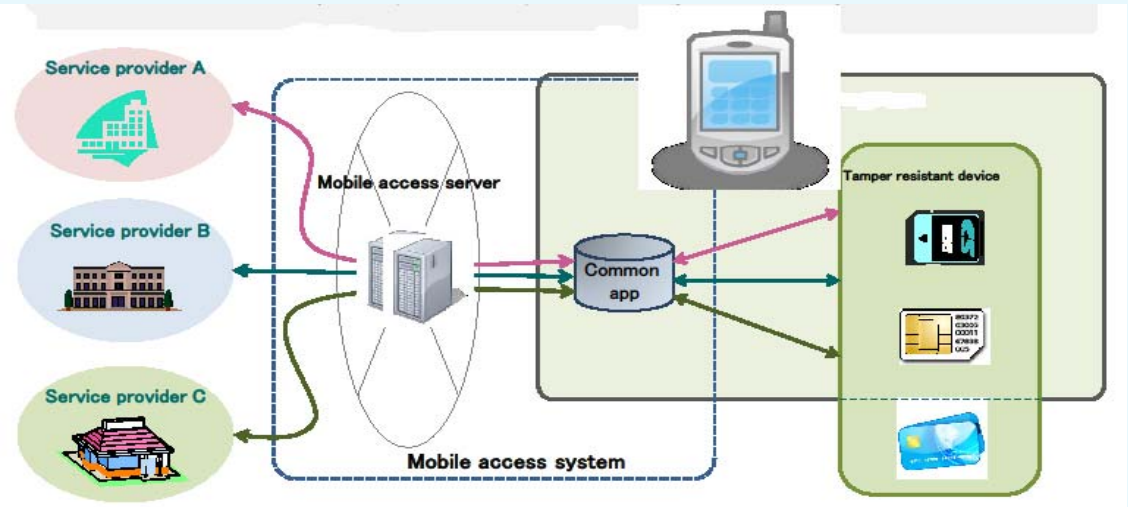
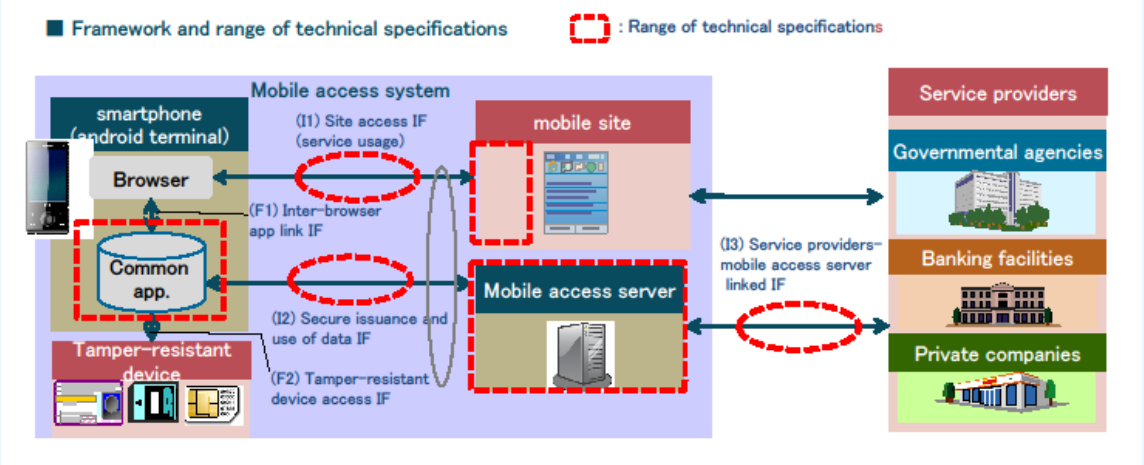



Figure 17: Common application and unified mobile access server for all service providers. Further, verification by experimentation with technical specifications etc. was studied. In other words, **A:** Examination of technical specifications for a mobile access system realising online storage and use of ID information and **B:** Based on the examination results of issue A, construction of an experimental environment, inspection of operability and user-friendliness from the viewpoint of both service providers and users, and verification of technologies.

**Figure 18: Technical specifications for structure with common application**



The outcomes on the difficulties mentioned above, A and B, are listed below.

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

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

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

In order to realise the services above, further experimental studies for overcoming technical difficulties will be conducted. The main topics for consideration in the future in light of the technology are methodologies of authentication of the issuing terminal when storing the ID information, such as an e certificate, etc. and scheme such as a mobile access system, considering the way of exchanging ID information between mobile phones and outer terminals, through local communication.

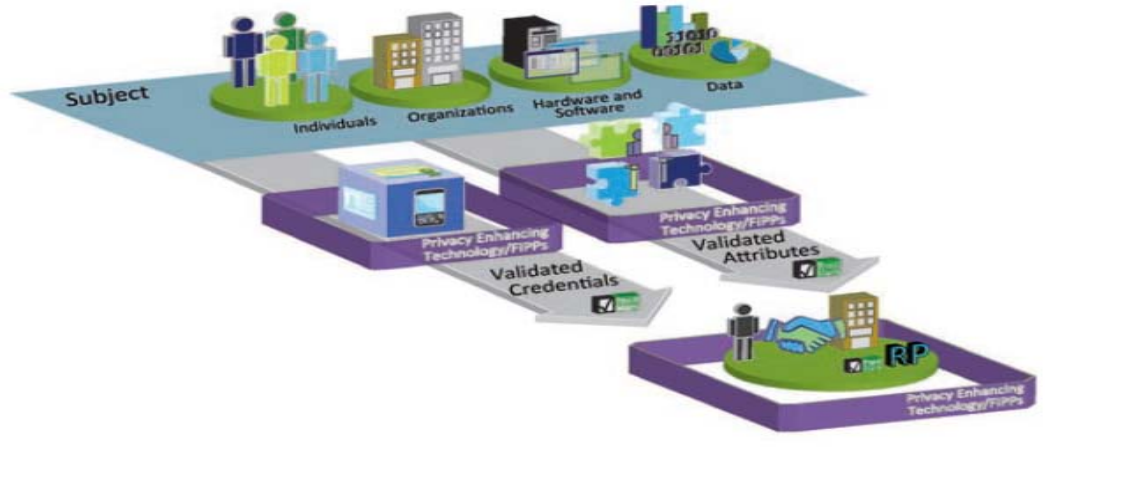
# 9 United States of America National Strategy for Trusted Identities in Cyberspace (NSTIC)

Individuals have limited ability to use strong digital identities across multiple applications, because applications and service providers do not use a common framework. Instead, they face the increasing complexity and inconvenience associated with managing the large number of usernames, passwords, and other identity credentials required to conduct services online with disparate organisations. Finally, collection of identity-related information across multiple providers, coupled with the sharing of personal information through the growth of social media, increases the opportunity for data compromise. For example, personal data that individuals use as "prompts" to recover lost passwords (mother's maiden name, name of a first pet, etc.) is often publicly available or easily obtained.

That is why the US National Strategy for Trusted Identities in Cyberspace (NSTIC) of was created by the White House in April 2011. The strategy's vision consists of the following: individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice and innovation. It offers the idea of the Identity ecosystem (Figure 19), where users can authenticate themselves at any service provider (relying party)f by their IDP using strong digital identities (for example: digital signature in a SIM card). In some cases relying party needs to confirm some characteristic inherent to the subject (for example, "this individual's age is at least 21 years"), retaining anonymity of the User. Such information can be asserted by the Attribute

provider – an organisation, responsible for the processes associated with establishing and maintaining attributes of the subject.

**Figure 19: NSTIC ecosystem**




The Identity Ecosystem will increase the following:

– Privacy protection for individuals, who will be assured that their personal data is handled fairly and transparently;

– Convenience for individuals, who may choose to manage fewer passwords or accounts than they do today;

– Efficiency for organizations, which will benefit from a reduction of paper-based and account management processes;

– Ease-of-use, by automating identity solutions whenever possible and basing them on technology that is simple to operate;

– Security, by making it more difficult for criminals to compromise online transactions;

– Confidence that digital identities are adequately protected, thereby promoting the use of online services;

– Innovation, by lowering the risk associated with sensitive services and by enabling service providers to develop or expand their online presence;

– Choice, as service providers offer individuals different—yet interoperable—identity credentials and media.

The logical step in the development of this ecosystem is the presence of the Authentication Provider Agregators that connect to many attribute providers and identity providers and provide a single interface to all of them.

# 10 Case study mobile payment in Poland

Today many equal mobile payments with NFC payment, this is not really right though NFC is one of many pairing methods to get information from the payer to the payee. Also a payment using NFC is covering one payment situation, pay at POS. A Polish bank has commercially launched a mobile payment service that includes all payment situations. The solution is unique in that it covers all payment situations, doesn't need any new hardware (ex. no need for a Secure Element), is operator independent, use the existing payment eco-system without the need of adding new players and can be used with any pairing technology (ex. NFC, RFID, QR-codes and barcodes). The roll-out includes all the bank's ATMs and very many POS-terminals. From start the mobile payment service supports:

– Point of Sale (POS) - pay in store, at restaurants, etc. (including future support for NFC)

– Online - pay at online stores

– P2P - real-time money transfer person-to-person to beneficiaries identified only by their telephone number

– Cardless cash withdrawal from ATMs

– Money vouchers – offline timed vouchers for shopping payments and ATM cash withdrawals

– Information services

Later on more payment situations can easily be added, though the same method and processes are used:

– Person-to-machine (ex. vending, parking, petrol, etc.)

– inApp payment

– mCommerce

– mPOS

More services like mobile ticketing, loyalty, coupons and gift cards can easily be added to mobile service and based on the same technology.

The Mobile payment service is available on all mobile platforms; Android, iOS, BlackBerry, Java (feature phones) and Windows Mobile/Phone.

The service uses a connected mobile device and the user is online authenticated to the issuer of the payment service. At the authentication a number of checks are performed; exchange of key's (PKI implementation), right unique application number and tied with IMEI (serial number of mobile), MSISDN (telephone number) and approved by user PIN. After successful authentication the payment transaction is performed by user pressing "pay" in his/her mobile app. No sensitive information are stored on the mobile nor transmitted during the payment transaction.

### The user process step-by-step, example (POS)

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

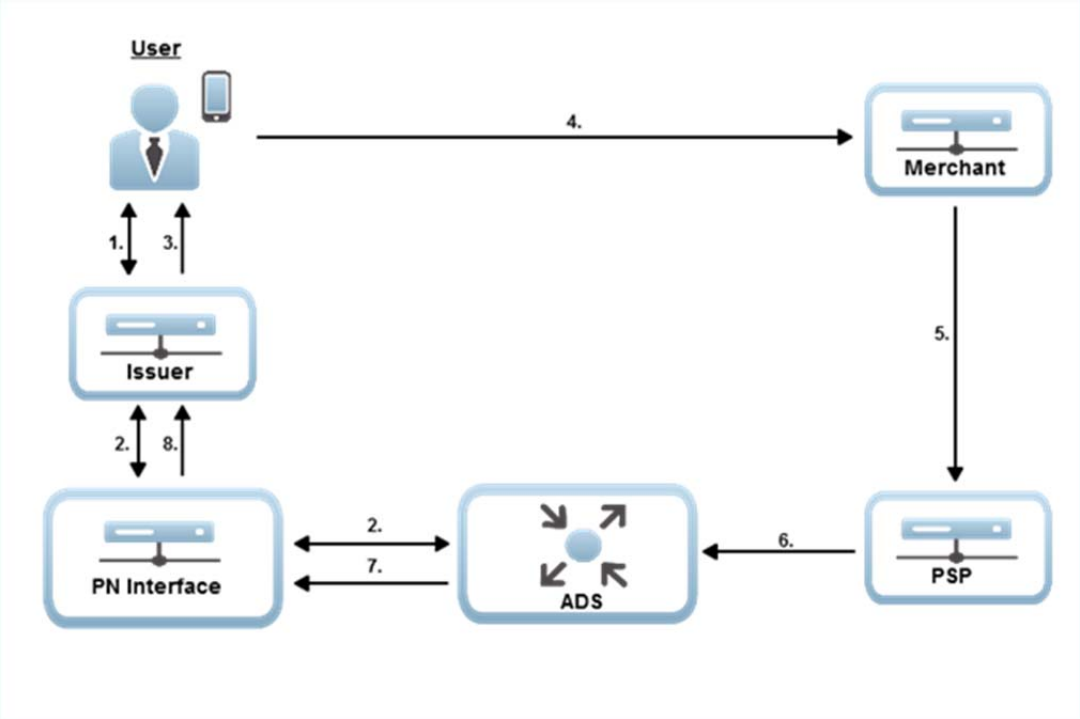
### The payment generic process step-by-step (technical)

In the Polish bank case the ADS (active discovery service) is at the bank in a closed loop system, where the bank also act as Payment Network (PN) and Payment Service Provider (PSP). Figure 20 below shows an ADS outside the bank and that give the opportunity for an open technology standard for mobile payment

in for example a country or region. The different players in the payment eco-system (issuers, payment networks, payment service providers/merchants) are connected once and can then use different mobile payment services from different issuers only by adding a commercial agreement.

An OTT is a One-Time Ticket that is generated by the ADS upon request from the issuer inside a payment network. The OTT is transferred by the user from the mobile device to the merchant's system. By having the security aspects regarding authentication between the issuer and the user instead of between the user and the merchant, the OTT is simply a nonsense code that does not hide any sensitive information. The OTT is matched in the ADS with any active OTTs and tied together with the specific user.

**Figure 20: The generic OTT process**




1. The user starts the application and initial authentication is made between the issuer system and the user's application.
2. An OTT is generated by the issuer through the ADS.
3. The issuer presents the OTT to the user through the mobile application.
4. The user transfers the OTT in the appropriate way (ex. swiping using NFC or NFC-tags, QR- or barcode or just typing it into the POS-terminal or cashier system) to the merchant.
5. The merchant sends the user-provided OTT to the PSP and its back-end system.
6. The PSP receives the OTT and forwards it to the ADS.
7. The ADS matches the OTT with any valid OTTs in the database and routes the status to the appropriate payment network.
8. The necessary details are forwarded to the appropriate issuer inside the payment network.

**Lessons learned**

– Easy (but secure) registration/enrolment process.

– It must be easy and fast to use and the trick is to get merchants where the service can be used.

– Simple for merchants to sign up and not higher fee's than for a card solution/transaction.

– Adding simple services like receipts, transaction history and balance in the mobile application will gain adoption.

# 11 Case study in the Russian Federation

Various mobile payment systems have become very popular in the Russian Federation. Some of them, while having minimum functionality limited to top-up the balance of previously registered mobile phone, do not require security and, respectively, do not provide it, the others (for example, mobile payment systems "Easy payment" and "MasterCard Mobile"), have wide functionality and meet the highest security level requirements, set forward by ITU standards to secure systems. Thus, and this is very important, security means do not invoke any additional inconveniences for users. All the diversity of means presented by modern mobile communication standards is used as transport environment. SMS and USSD have become quite wide spread, however, due to wide circulation of smartphones and development of standards for mobile telecommunication systems, increased the use of GPRS, UMTS, WiMax and LTE.

It is interesting to note, that in the market under equal conditions are present both applications with "sensitive information" stored on tamper resistance devices, and applications with the data stored in the phone's memory. Nevertheless, the latter have become more popular, yet they are potentially less secure. Obviously, the consumer benefit of the latter is that he does not need to change his SIM/UICC card. Yet, risk of reading the confidential data from phone's memory is a shortcoming. With respect thereto, it is interesting to compare these two types of applications from the point of security.

According to statistics, fraud usually takes place not when applications on stolen phones are hacked, but either because of the "human factor", or virus programs penetrated into clients' phones. And this is the least protected system elements that require further increase of security of mobile applications only in case of very high risks of being hacked, for example, for the official digital signature recognized by state entities. Unlike it, risks of payment systems can be limited by the maximum amount of financial transaction per transaction and/or a time period. Therefore, the most important role in secure usage of devices working in open networks consists of training clients to use these devices, and to use anti-virus programs. Thus, certainly, the service provider should take all measures to protect confidential information, defined by ISO 27001 and other similar standards. In particular, it is necessary to minimize amount of employees operating the system, who have access to "sensitive data", to assign different access levels to the system, and to provide mandatory authentication and login registration.

In Russia, as well as in other countries, all three MPS models, described in Section 4.3 above, have become popular and all sources of payment described in Section 4.4 are used, namely: clients bank accounts, international and local payment cards, personal accounts of subscribers of cellular communication, and e-money.

Use of mobile devices for providing legally recognized digital signature in Russia is aggravated by Russian requirements to its cryptographic protection and is not introduced yet; however, Rostelecom has been dealing with this issue for a long time and intends to implement it in nearest time.

# 12 Findings

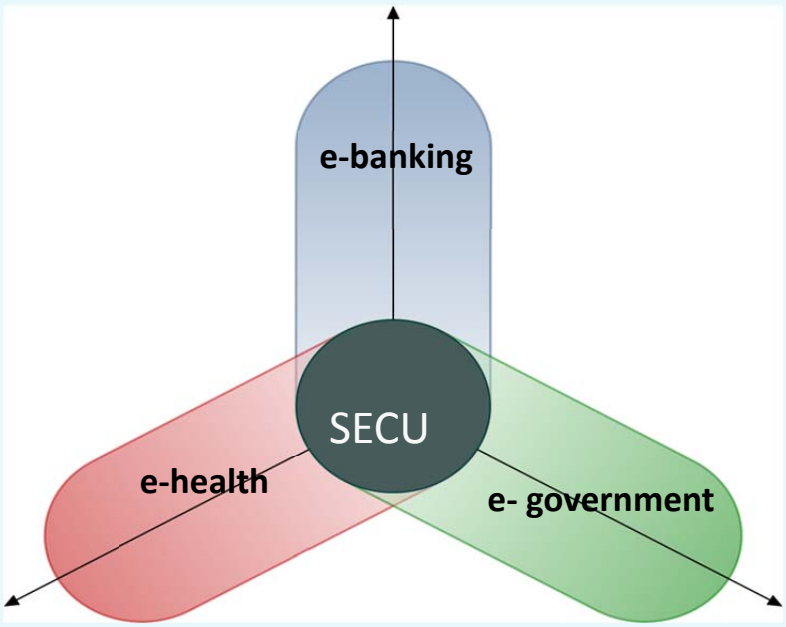
As shown in implementation cases described in chapters 6-9 above, development and usage of mobile devices for *m-Government, m-Health, m-Payment, m-Learning and so on* are at different levels in various countries, however, in today's global world the penetration of technology innovations increases drastically, that leads to step-by-step convergence of technological development levels and reduces digital gap between developed and developing countries. Today the developed countries already have fully functional electronic payment systems and mobile government, and in some developing countries even simple use of SMS to transfer the data between medical offices brings real results, reducing delays in receiving early infant diagnosis (EID) DBS HIV test results as it was described in the Project MWANA implemented in the Republic of Zambiya[17]. This proves that very soon this technological gap will be decreased. The most advanced today's systems which are based on mobile devices offer the whole range of services which is continuously extended. So, beside mobile payments and mobile banking services, wide application was received by services based on geo-location. Besides, it is stated at White Parer Mobile Payments[18], issued by European Payments Council in 2012, the mobile terminal should represent a "digital wallet" which will provide authentication and digital signature to replace multiple passwords, IDs and loyalty cards of merchants (Figure 21).

**Figure 21: The wallet shall be digital, not leather**


As a normal wallet, the "digital" wallet, in effect, contains identification data of the owner, data on means of payment available to the owner, and in certain cases - personal data of the owner (images, documents, etc.). It may include ID information, digital signatures and certificates, login information, addresses for drawing of scores and transmission, and also information on means of payment. Besides, it can also include other applications, for example bonus points, tickets or travel documents. After having passed authentication in Unified Centre, one may enter personal merchant accounts or social networks, such as Facebook, LinkedIn, etc., which is very convenient and relieves from the need to remember or to store securely numerous passwords of multiple accounts. In the short term, one can expect active distribution of mobile devices as terminals for e-government and healthcare. Recent initiatives in the use of mobile devices, launched at Telecom-2012 by the ITU and WHO, are to prove this statement.

So rapid development of systems based on mobile devices is due to security measures applied to services. Security is a common task for e-government, financial services and e-health (Figure 20) and is provided with observance of ITU-T recommendations for security.

**Figure 22: Security – touchstone for all e-services**




Due to these recommendations, cryptography has been implemented to use for authentication and encoding of transferred data instead of one-time passwords used in previous systems, that considerably increased security of mobile devices and at the same time increased convenience of their use and, as a result, led to growth of popularity of services based on mobile devices.

## 13 Recommendations

– Since mobile phones have achieved full market penetration and high service levels, they are the ideal payment terminals and secure communication instruments.

– It is important to provide easy-to-use mobile phone interfaces with consistent user experience across all supported mobile phone implementations, even if the most advanced smart phones boast “great” colour displays and touch-based interfaces. The user experience remains strongly challenged by necessarily small form factor. For example, the mobile phone form factor effectively limits the amount of information that can be displayed at any given time and the ability of the user to enter complex text.

– Mobile device is a “digital wallet”, to store identification information on the wallet holder, on payment instruments – accessible to the wallet holder and optional personal information items belonging to the holder (e.g., pictures, documents, etc.). This may include information related to ID cards, digital signatures and certificates, logon information, billing and delivery addresses as well as payment instrument related information. Furthermore, it may also include other applications such as loyalty, transport or ticketing.

– It is advised that the Customers should not be bound to a specific MNO or Bank, and should retain their current ability to choose service providers.

– Parties of electronic dialog should be authorised with the use of at least two-factor authentication, and data transfer should be executed in secure mode using cryptography means.

– It is advised to use Security Lelel 4 or 3 according to Y.2740 ITU-T Recommendation.

– Customers should be aware of the Security Level of the System, which should be stipulated in the participants' agreement. User authentication may be performed by the Unified centre of authentication.

– To ensure the security, the mobile device must have a special Mobile Application, which provides authentication and encryption.

– The most realistic vision is one of a market where multiple Mobile Applications co-exist, combining services on a single mobile device.19

– The registration and provisioning of a Mobile Application needs to be executed in secure environment. Access to a Mobile Application would be easier for customers, if they could use existing trusted relationship between them and their service providers.

– To reach the highest security level, Mobile Application should be located on the hardware Security Element.

– The choice of Security Element has a major impact on the service model and roles of various stakeholders. There are three types of SEs used until now: UICC, embedded SE and removable SE, such as micro SD card.

– Service Enabler provides the technology support and integration of various access means, interoperability with service providers and authentication centre.

– It is recommended to use Mobile Applications with several independent blocks with different sets of keys.

– The Client may have multiple customer mobile identities – mIDs, bounded to the Client's MSISDN. Unified rules to issue mIDs, registered within the System Central Directory, should be introduced to ensure proper routing of messages to Clients.

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

– Mobile systems should, as much as possible, use technologies and infrastructure which have been already widely deployed.

# 14 Terms and abbreviations

| | |
|---|---|
| ADS | Active Discovery Services |
| CA | Certification Authority |
| CPU | Central Processor Unit |
| CSD | Circuit Switched Data |
| DNS | Domain Name System |
| DTMF | Dual-Tone Multi-Frequency |
| EDGE | Enhanced Data for GSM Evolution |
| EU | European Union |
| G2B | Government-to-Business |
| G2C | Government-to-Citizens |
| G2E | Government-to-Employees |
| G2G | Government-to-Government |

| | |
|---|---|
| GLONASS | Global Navigation Satellite System |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| ICT | Information and Communication Technology |
| IDM | Identity Management |
| IP | Internet Protocol |
| ITU | International Telecommunication Union |
| LTE | Long Term Evolution |
| mID | mobile Identificator |
| MNO | Mobile Network Operator |
| MPS | Mobile Payment System |
| MSISDN | Mobile Subscriber Integrated Services Digital Number |
| MSSP | Mobile Signature Service Provider |
| NCD | Non-communicable disease |
| NFC | Near Field Communications |
| NGN | Next Generation Networks |
| NIST | National Institute of Standards and Technology (USA) |
| NSTIC | National Strategy for Trusted Identities in Cyberspace (USA) |
| OTA | Over-The-Air |
| OTP | One Time Password |
| OTT | One Time Ticket |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PN | Payment Network |
| PSP | Payment Service Provider |
| QoS | Quality of Service |
| RA | Registration Authority |
| ROI | Return On Investment |
| RSA | an algorithm for public-key encryption |
| SIM | Subscriber Identification Module |
| SMS | Short Message Service |
| TEE | Trusted Execution Environment |
| UICC | Universal Integrated Circuit Card |
| UNO | United Nations Organisations |
| USA | United States of America |
| USSD | Unstructured Supplementary Service Data |

| | |
|---|---|
| VPN | Virtual Private Network |
| WHO | World Health Organisation |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WPKI | Wireless Public Key Infrastructure |

## 15 List of References


1. ITU-T Recommendation Y.2740 (page 3)
2. Joint ITU-WHO initiative on NCD(page 6)
3. eEurope "Blueprint" Smartcard Initiative (page 7)
4. NIST Special Publication 800-57 (page 7)
5. ITU-T Recommendation Y.2741 (page 8)
6. Security in telecommunications and information technologies (page 12)
7. ITU-T Recommendation X.805 "Security Architecture for Systems Providing End-to-End Communications (page 12)
8. ITU-T Recommendation X.800 "Security architecture for Open Systems Interconnection for CCITT applications (page 12)
9. ITU Recommendation X.1122 (page 14)
10. Mobile Signatures Whitepaper: Best Practices (page 18)
11. ETCI TR 102 203 "Mobile Commerce (M-COMM); Mobile Signature; Business & Functional Requirements" (page 19)
12. ETCI TS 102 204 "Mobile Commerce (M-COMM); Mobile Signature; Web Service Interface" (page 19)
13. ETCI TR 102 206 "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework" (page 19)
14. ETCI TS 102 207 "Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services" (page 19)
15. Ministry of Internal Affairs and Communications (2012) “Information and communications in Japan, White Paper 2012,” p333 (page 23)
16. Ministry of Internal Affairs and Communications (2012) “Final Report from ‘Study Group on Information Security Issues of Smartphone and Cloud Computing,’” June 29,2012 http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/120629_03.html (page 23)
17. Project MWANA, Zambia D10-SG02-C-0215 http://www.itu.int/md/meetingdoc.asp?lang=en&parent=D10-SG02-C&question=Q17-3/2
18. “White paper. Mobile payments”, 2012. http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=564
19. A Series of White Papers on Mobile Wallets
20. http://vanha.mobeyforum.org/Knowledge-Center/Mobey-White-Papers
21 PKO Project brief http://www.mynewsdesk.com/se/pressroom/accumulate/document/view/mobile-payment-systems-brief-iko-mobile-payment-service-28292

22. PKO Bank Polski mobile payment use case
http://www.youtube.com/playlist?list=PL5xZmvvYELkUOr2a2BuIorS7NPXa17tuY

23. http://www.accumulate.se

_____

**Международный союз электросвязи (МСЭ)**
**Бюро развития электросвязи (БРЭ)**
**Канцелярия Директора**
Place des Nations
CH-1211 Geneva 20 - Switzerland
Эл. почта: **bdtdirector@itu.int**
Тел.: +41 22 730 5035/5435
Факс: +41 22 730 5484

**Заместитель Директора и руководитель Департамента администрирования и координации основной деятельности (DDR)**
Эл. почта: **bdtdeputydir@itu.int**
Тел.: +41 22 730 5784
Факс: +41 22 730 5484

**Департамент инфраструктуры, благоприятной среды и электронных приложений (IEE)**
Эл. почта: **bdtiee@itu.int**
Тел.: +41 22 730 5421
Факс: +41 22 730 5484

**Департамент инноваций и партнерских отношений (IP)**
Эл. почта: **bdtip@itu.int**
Тел.: +41 22 730 5900
Факс: +41 22 730 5484

**Департамент поддержки проектов и управления знаниями (PKM)**
Эл. почта: **bdtpkm@itu.int**
Тел.: +41 22 730 5447
Факс: +41 22 730 5484

# Африка

## Эфиопия
**Региональное отделение МСЭ**
P.O. Box 60 005
Gambia Rd., Leghar ETC Bldg 3rd Floor
Addis Ababa – Ethiopia
Эл. почта: **itu-addis@itu.int**
Тел.: (+251 11) 551 49 77
Тел.: (+251 11) 551 48 55
Тел.: (+251 11) 551 83 28
Факс: (+251 11) 551 72 99

## Камерун
**Зональное отделение МСЭ**
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun
Эл. почта: **itu-yaounde@itu.int**
Тел.: (+ 237) 22 22 92 92
Тел.: (+ 237) 22 22 92 91
Факс: (+ 237) 22 22 92 97

## Сенегал
**Зональное отделение МСЭ**
Immeuble Fayçal, 4e étage
19, Rue Parchappe x Amadou Assane Ndoye
Boîte postale 50202 Dakar RP
Dakar - Sénégal
Эл. почта: **itu-dakar@itu.int**
Тел.: (+221) 33 849 77 20
Факс: (+221) 33 822 80 13

## Зимбабве
**Зональное отделение МСЭ**
TelOne Centre for Learning
Corner Samora Machel
and Hampton Road
P.O. Box BE 792
Belvédère Hararé - Zimbabwe
Эл. почта: **itu-harare@itu.int**
Тел.: (+263 4) 77 59 41
Тел.: (+263 4) 77 59 39
Факс: (+263 4) 77 12 57

# Северная и Южная Америка

## Бразилия
**Региональное отделение МСЭ**
SAUS Quadra 06 Bloco "E"
11º andar – Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
CEP 70070-940 Brasilia, DF – Brésil
Эл. почта: **itubrasilia@itu.int**
Тел.: (+55 61) 2312 2730-1
Тел.: (+55 61) 2312 2733-5
Факс: (+55 61) 2312 2738

## Барбадос
**Зональное отделение МСЭ**
United Nations House
Marine Gardens
Hastings - Christ Church
P.O. Box 1047
Bridgetown - Barbados
Эл. почта: **itubridgetown@itu.int**
Тел.: (+1 246) 431 0343/4
Факс: (+1 246) 437 7403

## Чили
**Зональное отделение МСЭ**
Merced 753, Piso 4
Casilla 50484 - Plaza de Armas
Santiago de Chile - Chile
Эл. почта: **itusantiago@itu.int**
Тел.: (+56 2) 632 6134/6147
Факс: (+56 2) 632 6154

## Гондурас
**Зональное отделение МСЭ**
Colonia Palmira, Avenida Brasil
Edificio COMTELCA/UIT 4.º Piso
P.O. Box 976
Tegucigalpa - Honduras
Эл. почта: **ituteguciglapa@itu.int**
Тел.: (+504) 22 201 074
Факс: (+504) 22 201 075

# Арабские государства

## Египет
**Региональное отделение МСЭ**
Smart Village, Building B 147, 3rd floor
Km 28 Cairo - Alexandria Desert Road
Giza Governorate
Cairo - Egypt
Эл. почта: **itucairo@itu.int**
Тел.: (+202) 3537 1777
Факс: (+202) 3537 1888

# Азиатско-Тихоокеанский регион

## Таиланд
**Региональное отделение МСЭ**
Thailand Post Training Center,
5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 - Thailand
Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand
Эл. почта: **itubangkok@itu.int**
Тел.: (+66 2) 575 0055
Факс: (+66 2) 575 3507

## Индонезия
**Зональное отделение МСЭ**
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 - Indonesia
Mailing address:
c/o UNDP - P.O. Box 2338
Jakarta 10001 - Indonesia
Эл. почта: **itujakarta@itu.int**
Тел.: (+62 21) 381 35 72
Тел.: (+62 21) 380 23 22
Тел.: (+62 21) 380 23 24
Факс: (+62 21) 389 05 521

# СНГ

## Российская Федерация
**Зональное отделение МСЭ**
4, building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Mailing address:
P.O. Box 25 - Moscow 105120
Russian Federation
Эл. почта: **itumoskow@itu.int**
Тел.: (+7 495) 926 60 70
Факс: (+7 495) 926 60 73

# Европа

## Швейцария
**Международный союз электросвязи (МСЭ)**
**Бюро развития электросвязи (БРЭ)**
**Европейское подразделение (EBP)**
Place des Nations
CH-1211 Geneva 20 - Switzerland
Эл. почта: **eurregion@itu.int**
Тел.: +41 22 730 5111

Международный союз электросвязи
Бюро развития электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

Отпечатано в Швейцарии
Женева, 2014 г.

01/2014 г.