Региональный семинар МСЭ для стран СНГ

«Развитие электронного правительства как одно из условий интеграции в глобальное информационное общество»

Москва, 25-27 ноября 2013 г.

Использование мобильных устройств в электронном правительстве

Евгений Бондаренко
вице-председатель ИК2 МСЭ-D
Зам Генерального директора ЗАО «Интервэйл»
E-mail: intervale@intervale.ru

Почему мобильные устройства?

- По данным МСЭ к концу 2013 г. в мире насчитывалось более **6** млрд. абонентов мобильных сетей и только **2,7** млрд. пользователей фиксированной сети Интернет.
- Мобильный телефон всегда с собой, практически всегда «on-line».
- В ряде случаев мобильная связь оказывается единственно-возможным средством связи.

Инициативы СНГ в секторе развития МСЭ

- **Резолюция 72, Хайдарабад**
  «Повышение эффективности использования услуг мобильной электросвязи»

- **Корректировка Исследовательского Вопроса 17-3/2**
  «Ход деятельности в области электронного правительства и определение областей использования электронного правительства в интересах развивающихся стран»

- **Региональная инициатива стран СНГ**
  «Разработка рекомендаций и создание пилотного фрагмента инфокоммуникационной подсистемы поддержки защищенных удаленных розничных платежей и управления банковскими счетами на основе беспроводных сетей связи»

МСЭ

СЕКТОР СТАНДАРТИЗАЦИИ

Разработаны и приняты новые Рекомендации ITU-T в области безопасности мобильных транзакций:

- Y2740. Требования к безопасности мобильных финансовых транзакций в NGN-сетях
- Y2741. Архитектура безопасных мобильных финансовых транзакций в NGN-сетях

СЕКТОР РАЗВИТИЯ

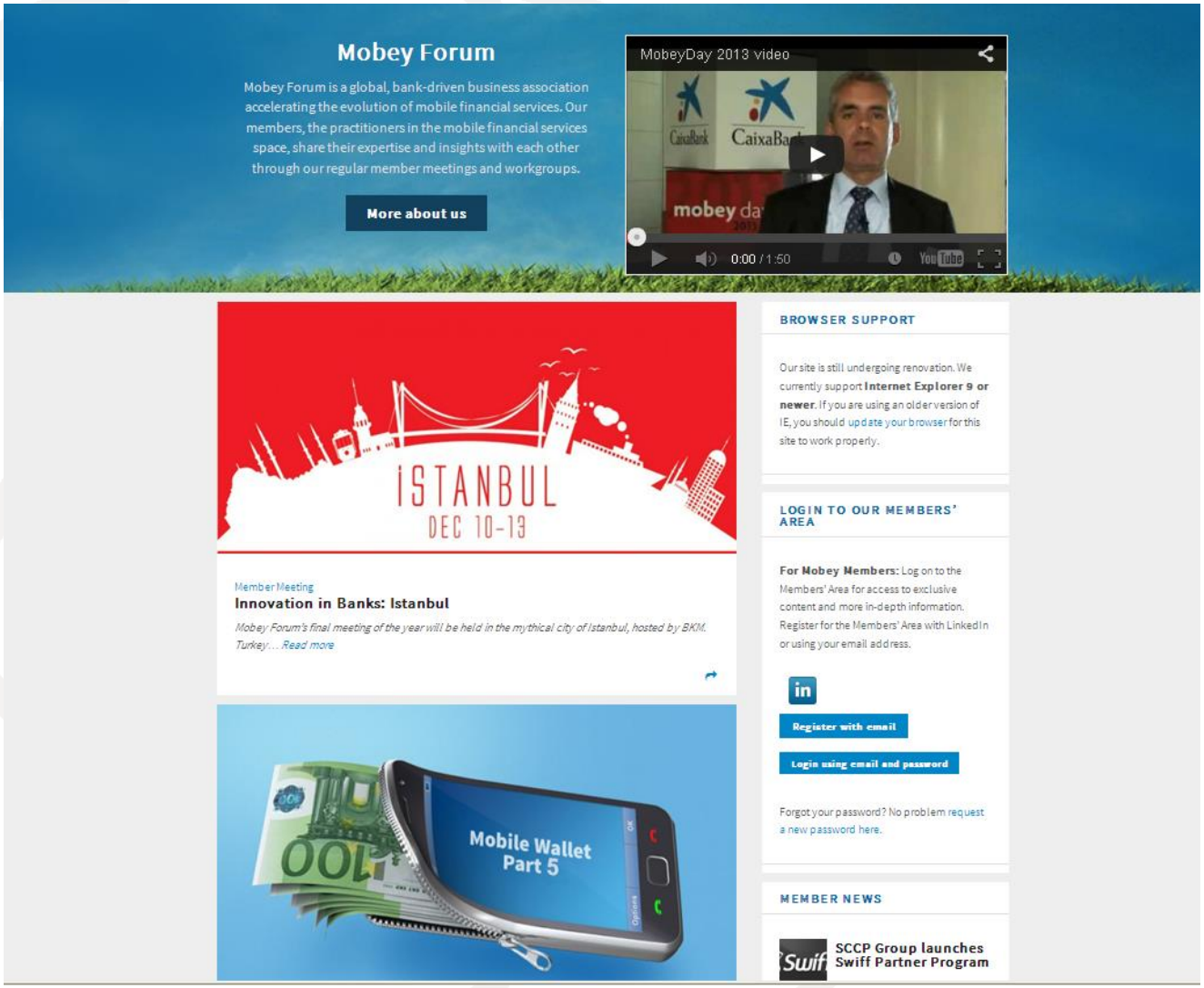
- Инициатива БРЭ «m-Powering development»
- Совместная инициатива МСЭ-ВОЗ по использованию мобильной связи в борьбе с неинфекционными заболеваниями
- Разработан Тулкит по по созданию услуг электронного правительства на базе ИКТ с использованием мобильной электросвязи (Q17-3/2).

M-Powering Development. Sectors & Stakeholders

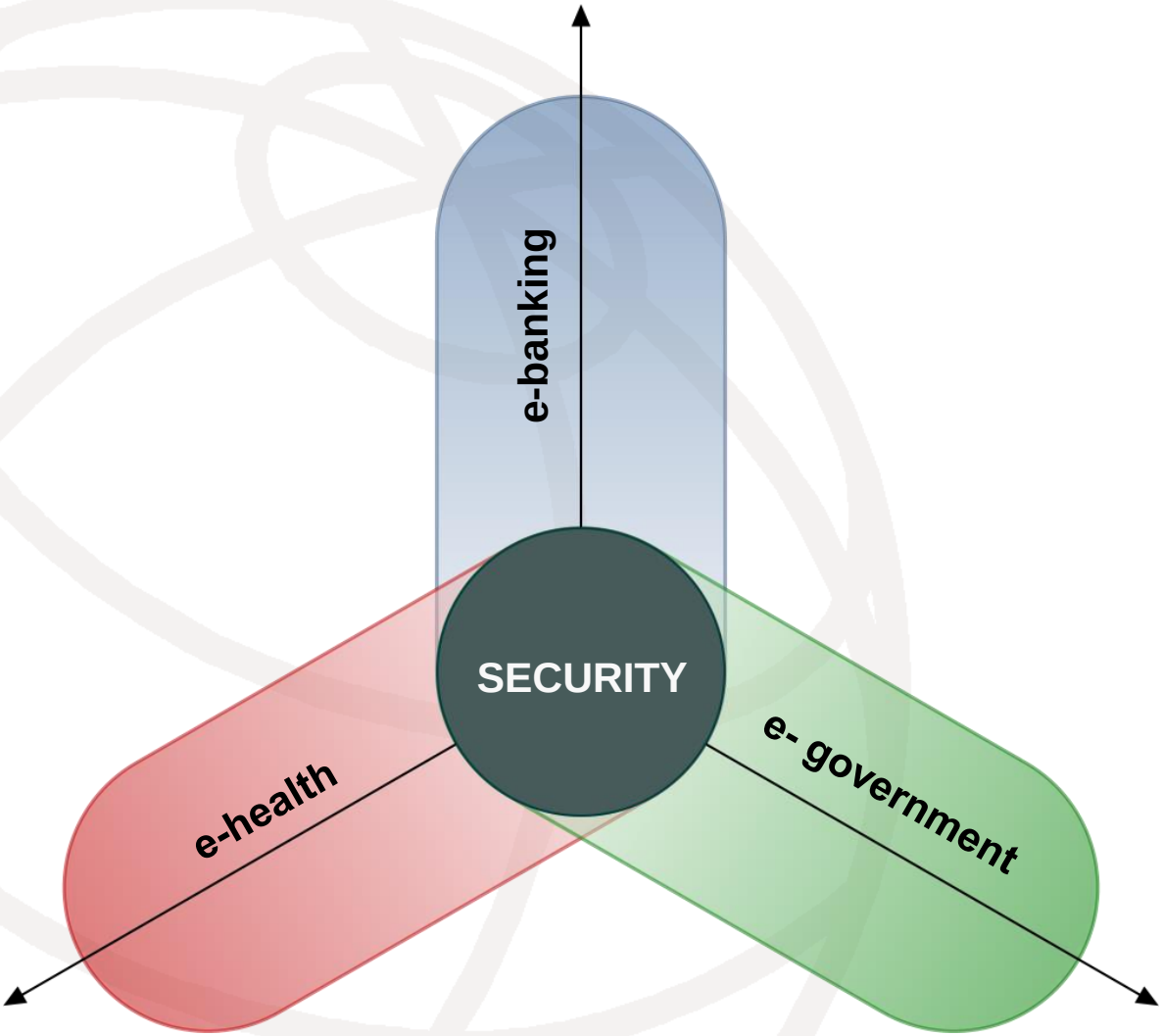
Sectors / Stakeholders	m-Health	m-Sports	m-Commerce	m-Banking	m-Governance	m-Education
Professionals	+++	++	+++	+++	+++	+++
Gov. / Regulatory Bodies	+++	+	++	++	+++	+++
Telco Operators	++	+	++	++	++	++
Service & App. Providers	+++	+	+++	+++	++	+++
IT Technology Vendors	++	+	++	+	++	+
Content Providers	+	+++	+	+	++	++
Devices	+++	+	++	+	+	++
International Organisations	+++	++	+++	+++	+	+
Funding/ Sponsors	+++	+	++	+	++	+++

+++ : Most important and influential

Mobey Forum


Mobey Forum
Mobey Forum is a global, bank-driven business association accelerating the evolution of mobile financial services. Our members, the practitioners in the mobile financial services space, share their expertise and insights with each other through our regular member meetings and workgroups.
More about us
MobeyDay 2013 video
0:00 / 1:50
ISTANBUL
DEC 10-13
Member Meeting
Innovation in Banks: Istanbul
Mobey Forum's final meeting of the year will be held in the mythical city of Istanbul, hosted by BKM, Turkey… Read more
Mobile Wallet Part 5
BROWSER SUPPORT
Our site is still undergoing renovation. We currently support Internet Explorer 9 or newer. If you are using an older version of IE, you should update your browser for this site to work properly.
LOGIN TO OUR MEMBERS' AREA
For Mobey Members: Log on to the Members' Area for access to exclusive content and more in-depth information. Register for the Members' Area with LinkedIn or using your email address.
Register with email
Login using email and password
Forgot your password? No problem request a new password here.
MEMBER NEWS
SCCP Group launches Swiff Partner Program

Безопасность – основа «е»-сервисов



Реализация уровней безопасности

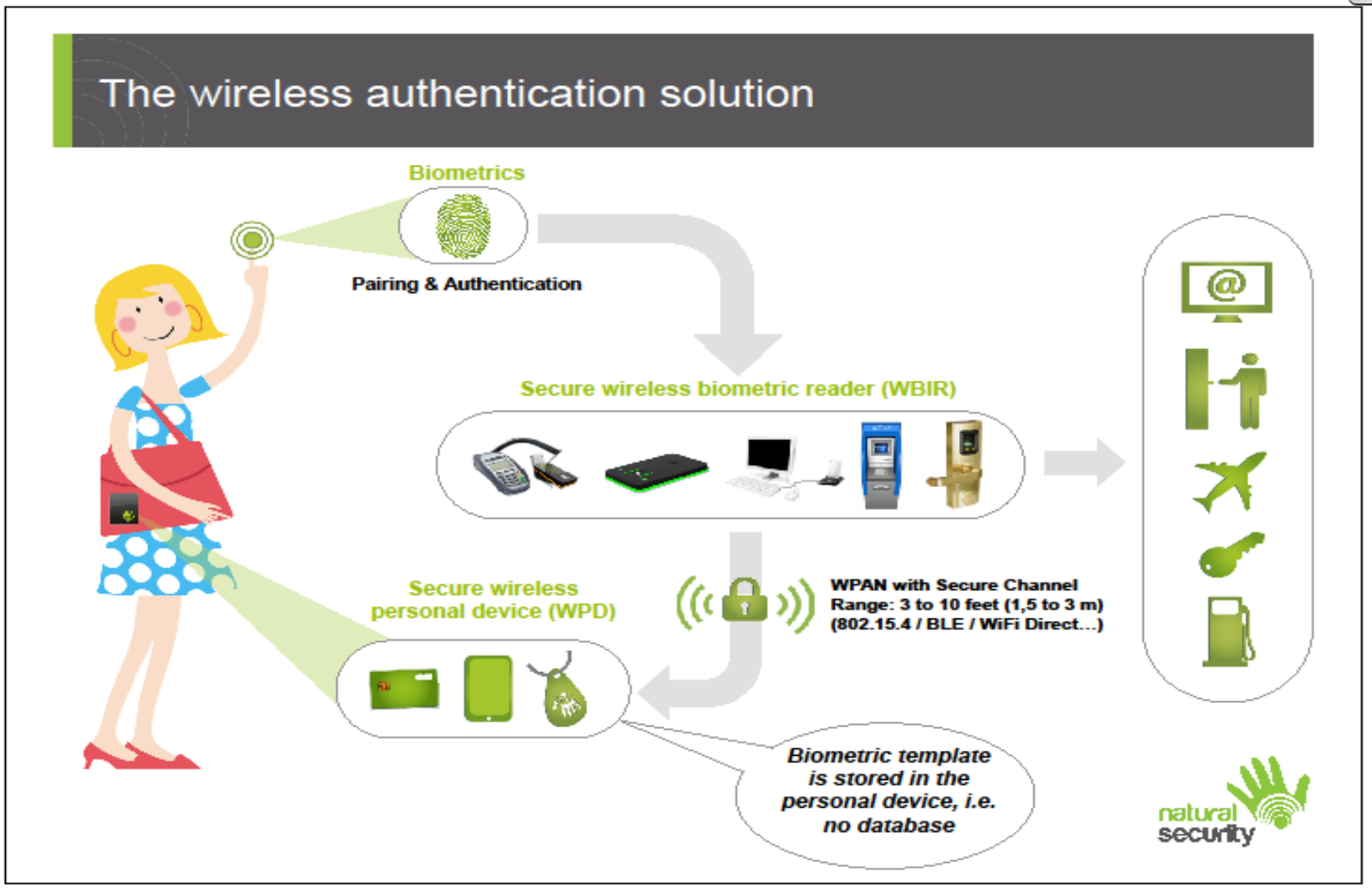
Измерение защиты	Уровень безопасности			
	1-й уровень	2-й уровень	3-й уровень	4-й уровень
Контроль доступа	Доступ к каждому из компонентов, входящих в инфраструктуру системы должен быть разрешен только в соответствии с уровнем полномочий персонала или пользователей системы.			
Аутентификация	Аутентификация в Системе обеспечивается средой передачи данных мобильного оператора	Однофакторная аутентификация при использовании услуг Системы	Многофакторная аутентификация при использовании услуг Системы	Персональное подключение к услугам с предоставлением персональных данных, с обязательной аутентификацией личности. Многофакторная аутентификация при использовании услуг Системы. Обязательное применение аппаратного криптографического модуля
Неотказуемость (сохранность информации)	Невозможность инициатору или участнику транзакции отказаться от своих действий после их совершения обеспечивается применением юридически закрепленных либо оговоренных во взаимных контрактах способов и совместно с принятыми механизмами аутентификации. Все действия системы персонала и пользователей системы должны подвергаться обязательной регистрации. Журналы регистрации событий должны быть защищены от изменений и содержать действия всех пользователей.			
Защищенность данных	При передаче обеспечивается средой передачи данных (безопасность связи), а при хранении и обработке данных - механизмом хранения данных и средствами по управлению доступом в Системе		При передаче сообщений должны обеспечиваться применением дополнительного шифрования сообщения, и применение протоколов передачи данных, обеспечивающих защиту информации, передаваемой участниками взаимоотношений (включая проверку целостности передаваемой информации); при хранении и обработке данных - дополнительными механизмами шифрованием и маскированием данных при их хранении и четким разграничением доступа в соответствии со служебными полномочиями	Выполнение требований 3го уровня с обязательным применением аппаратных средства шифрования и защиты информации на стороне Клиента
Целостность данных				
Конфиденциальность	Гарантируется отсутствием в передаваемых сообщениях sensitive data, и реализацией необходимых механизмов хранения данных и средствами по управлению доступом в Системе. Компоненты системы не должны иметь скрытых возможностей по несанкционированному сбору и передачи информации.			
Безопасность связи	Гарантируется доставка сообщения адресату и защиту информации от несанкционированного просмотра при передаче по каналам связи. Обеспечивается провайдерами сети мобильного оператора.			
Доступность	Гарантирует отсутствие препятствий для доступа к данным и услугам системы со стороны авторизованных и уполномоченных пользователей системы. Обеспечивается провайдерами сети мобильной связи и провайдерами услуги.			

Факторы аутентификации

- Пользователь **обладает некоторой сущностью**, которую сложно подделать (банковская карта, бумажные документы …);
- Пользователь **знает некоторые сведения**, которые не должен знать кто-либо еще (пароль, PIN, авторизационную фразу, ответ на проверочный запрос);
- Пользователь **умеет производить некоторое действие уникальным образом** (формировать графическую или цифровую подпись, имитовставку).

В зависимости от количества факторов аутентификации задействованных в процессе конкретной процедуры аутентификации, различают **однофакторную** и **многофакторную** аутентификации.

Natural Security Alliance



Реализация ИКТ услуг на базе мобильных устройств

Клиентские приложения

- в памяти телефона
- на SIM-карте.
- на SD-карте

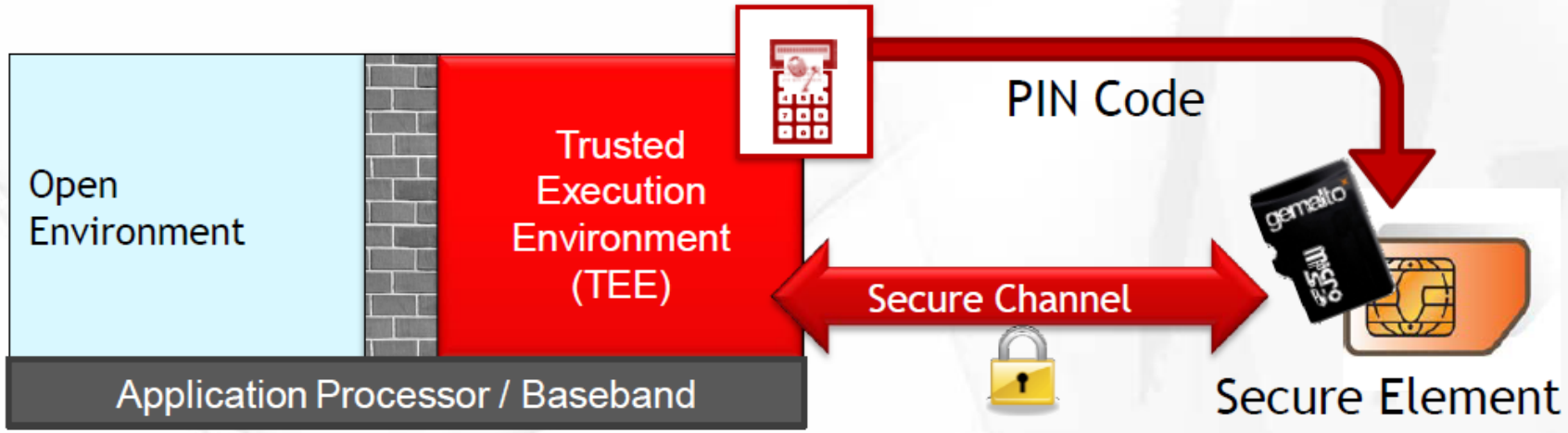
Транспорт

- SMS
- USSD
- GPRS
- EDGE
- UMTS

Средства безопасности

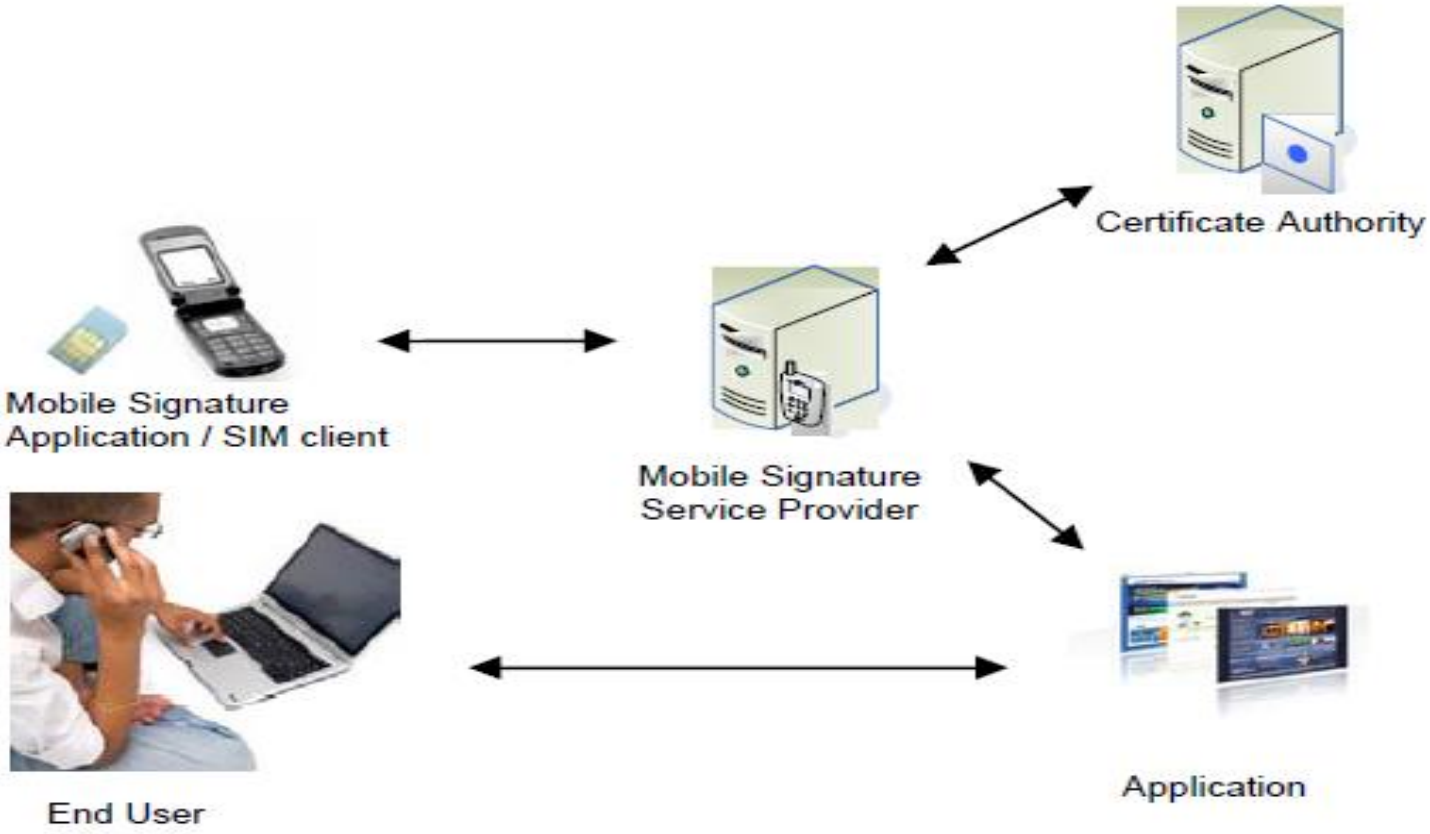
- строгая аутентификация
- шифрование канала связи
- хранение данных в Secure Element или в облаке
- TEE

Пример реализации метода верификации клиента по PIN Code в среде (TEE)



Мобильная цифровая подпись

Process flow



Бумажник должен быть цифровым, а не кожаным

СПАСИБО !