Семинар МСЭ
“Мобильные платежи: проблемы и перспективы развития”

Баку, Азербайджан, 14-16 октября 2014 г.

Мобильные платежи – перспективное направление развития ИКТ

Евгений Бондаренко

Вице-председатель ИК2 МСЭ-Д

Зам. Генерального директора ЗАО «Интервэйл»

E-mail: bond@intervale.ru

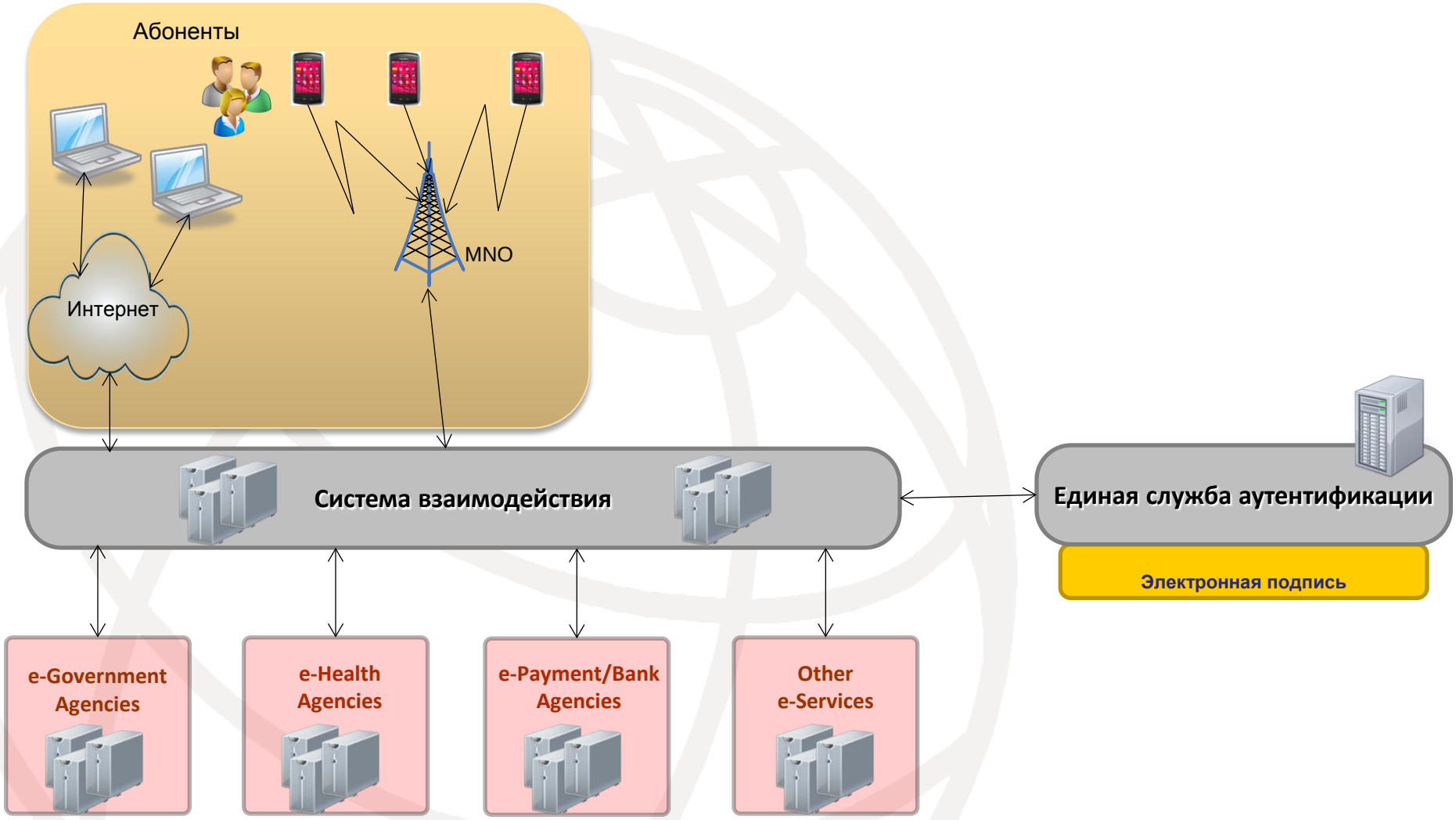
Особенности мобильных платежей

- Высокий уровень проникновения мобильной связи
- Доступность услуги в любое время в любом месте
- Удобный инструмент проведения бесконтактных платежей
- Возможность обеспечить высокий уровень безопасности
- Совместимость как с существующей платежной инфраструктурой, так и с инновационными системами платежей
- Логичное направление развития международных и локальных карточных платёжных систем
- Возможность инициирования финансовых транзакций как плательщиком, так и получателем (торгово-сервисным предприятием)
- Разнообразные средства платежа

Сдерживающие факторы

- Консерватизм в поведении потенциальных пользователей
- Недоверие к безопасности мобильной связи
- Недостаточная распространенность компьютерной грамотности населения
- Сегодняшние мобильные устройства не были задуманы для обеспечения защищенных операций
- Неудобная клавиатура и маленький дисплей большинства мобильных устройств – непривычная эргономика
- Ситуация в различных регионах сильно различается – не существует единого решения
- Оптимальные решения еще не найдены

Система с единой службой аутентификации



Архитектура мобильной платежной системы

Рекомендация МСЭ-Т Y.2741

Мобильная платежная система как часть НПС

Множество вариантов реализации

Реализация сервиса:

- **На базе стандартных услуг мобильного оператора**
- **На базе специализированных приложений**
  - на SIM-карте.
  - на SD-карте
  - на встроенном SE
  - в памяти телефона

Безопасность:

- Аутентификация
- Шифрование
- Элемент безопасности
- TEE
- Облачное хранение

Технология коммуникации:

- SMS
- USSD
- GPRS
- EDGE
- UMTS
- DTMF
- Voice
- NFC
- Blue Tooth
- QR

Выбор оптимального решения

		Средство платежа				
		Bank account	Payment card	MNO account	e-money account	Other accounts
Техническая реализация	WEB	**	*		*	*
	SMS/USSD	*	*	**	*	*
	Voice	*	*			*
	Application	***	***	***	***	***

Четыре уровня защищенности Мобильной Платежной Системы

- Level 1: Защищенность обеспечивается средствами оператора связи
- Level 2: МПС использует однофакторную аутентификацию
- Level 3: Многофакторная аутентификация, шифрование данных
- Level 4: Дополнительно к средствам, перечисленным в Level 3 используется SE/TEE

Рекомендация МСЭ-Т Y.2740

Доверенная Среда Исполнения (TEE)

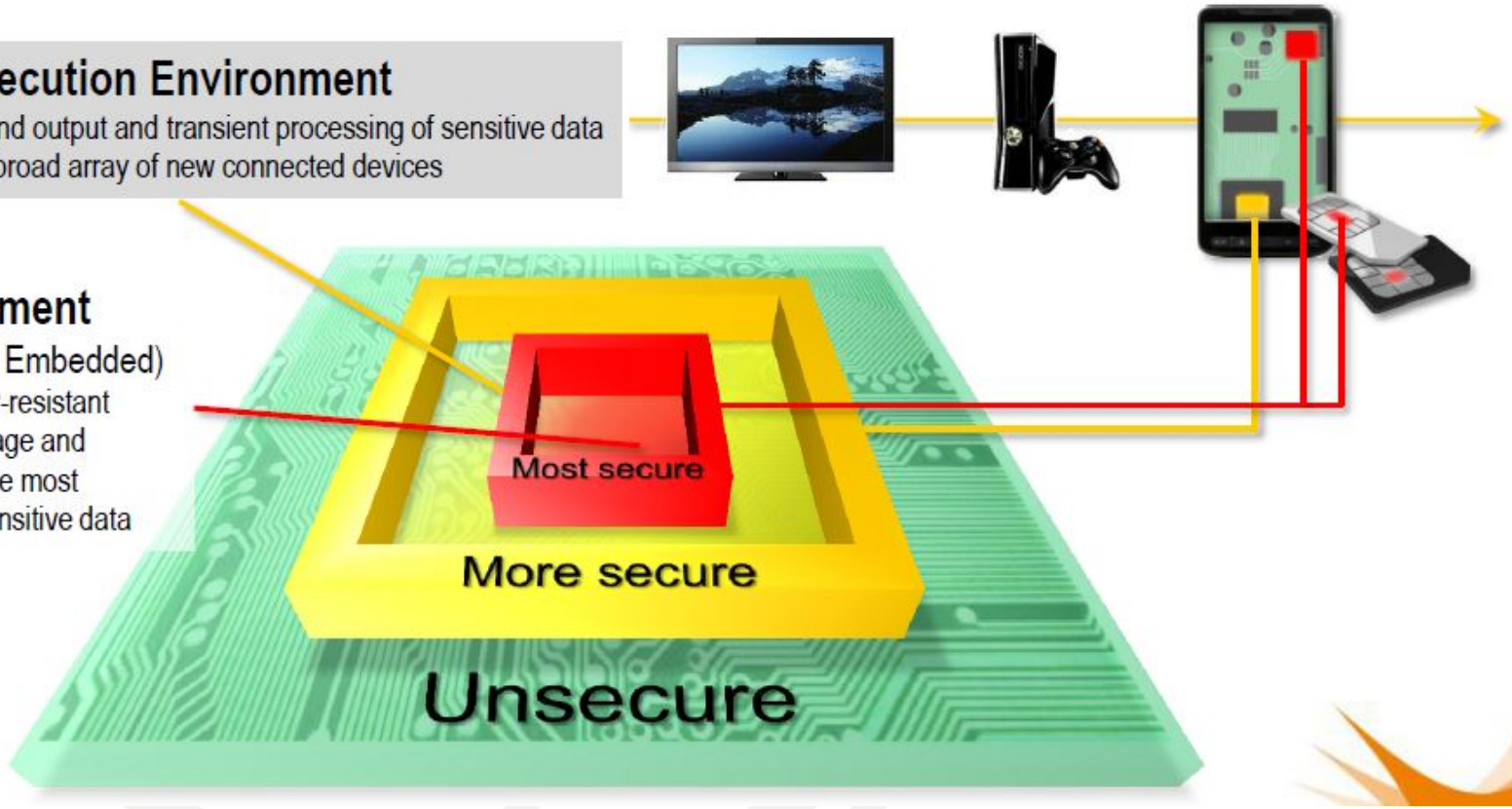
Trusted Execution Environment

- Protects input and output and transient processing of sensitive data
- Applicable to a broad array of new connected devices

Secure Element

(Removable or Embedded)

- Certified tamper-resistant
- For secure storage and processing of the most valuable and sensitive data



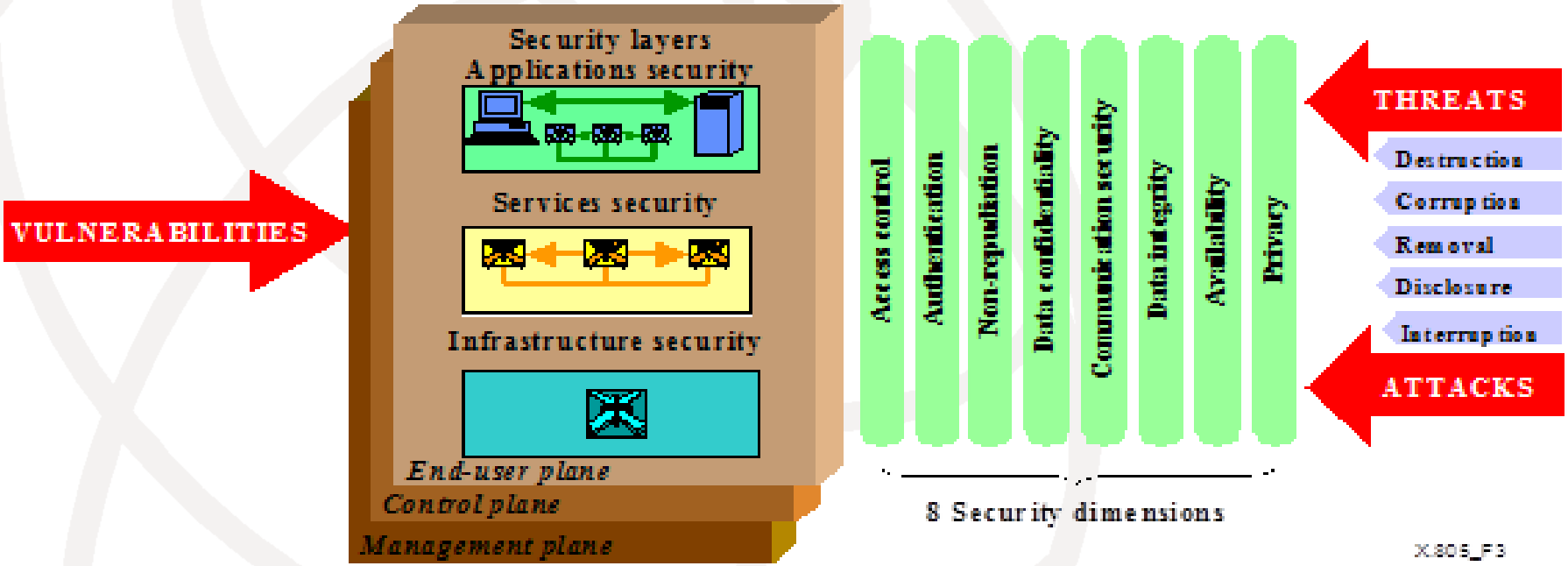
Host Card Emulation (HCE) - система с облачным хранением данных

- Без аппаратного элемента безопасности
  - Cloud-based solution
  - Tokens-based solution
- Гибридное решение (Cloud+SE)

Портмоне должно быть электронным, а не кожаным

СПАСИБО !

Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами



Рекомендация МСЭ X.805

Реализация уровней безопасности

Измерение защиты	Уровень безопасности			
	1-й уровень	2-й уровень	3-й уровень	4-й уровень
Управление доступом	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.			
Конфиденциальность 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				
Защита персональной информации	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.			

Рекомендация МСЭ Y.2740