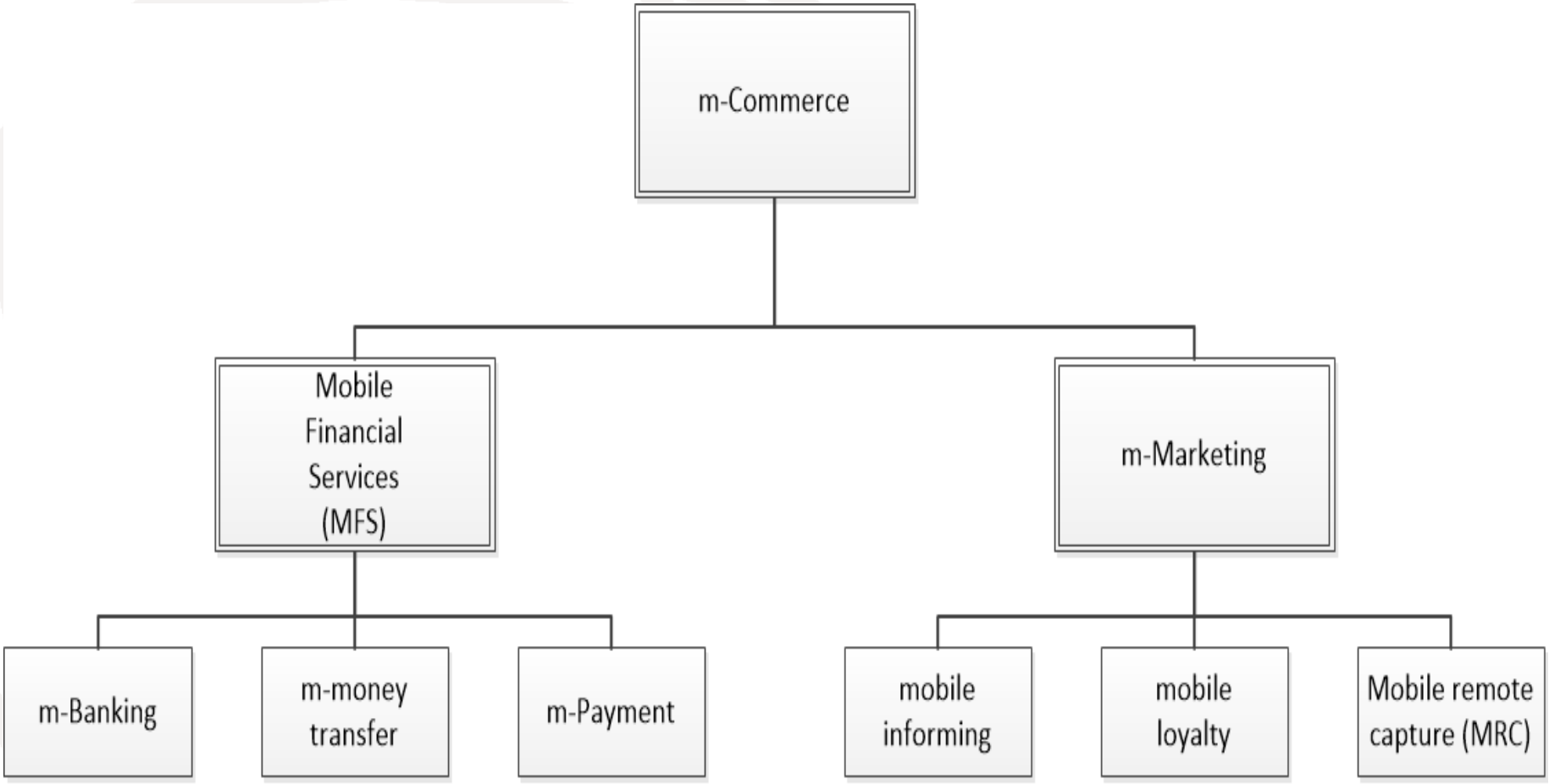
m-Powering Development Initiative Advisory Board

second meeting

Geneva, 23rd of May 2014

m –Commerce Working Group

M-Commerce structure



Definitions

Mobile Device	**A mobile device is a device with mobile communication capabilities such as a telecom network connection, Wi-Fi and Bluetooth that offer a connection to the internet or other communications networks. Examples of mobile devices include mobile phones, smart phones and tablets.**
m-Commerce	**Mobile Commerce is the delivery of electronic commerce capabilities directly into the consumer´s mobile device, anywhere, anytime via cellular and wireless networks.**
MFS	**Mobile Financial Services is an umbrella term used to describe any financial service that is provided using a mobile device.**
m-Marketing	**Mobile Marketing is the marketing process, using mobile devices for communication with customers, for the purpose of selling products or services.**
m-Banking	**Mobile banking in its simplest form lets a user retrieve the balance of an account, a small number of the recent transactions, and transfer funds in-between accounts that the user holds. In the widest of senses mobile banking is advanced enough to replace the entire suite of service offered through a bank's branch and internet banking services.**
m-Payments	**Mobile Payments are payments for which the data and instruction are initiated, transmitted or confirmed via a mobile device. This can apply to online or offline purchases of services and digital or physical goods as well as P2P payments, including transfer of funds. Mobile payments are often divided into two main categories; proximity payments and remote payments. However, the two are converging as neither is tied to a specific technology.**
mobile money transfer (MMT)	**A Mobile Money Transfer is the exchange of funds from one party to another, using a mobile device to either initiate and/or complete the transaction.**
mobile informing	**Mobile Informing is an information service, using mobile devices. The advantage of mobile informing is that information comes directly into the consumer´s device, anywhere, anytime via cellular networks. Examples of such services: bank informing, advertisement, etc.**
mobile loyalty	**Mobile Loyalty is a loyalty system, using mobile devices.**
MRC (Mobile Remote Capture)	**The availability of cameras in smartphones has given rise to the ability to capture cheques, bills and other payment related documents remotely instead of having to bring them to a branch. Using a mobile application, the user takes a picture of a document that is analysed by the MRC software to read out the payment instructions. The instructions are then submitted to the bank for processing. Alternative names for this type of feature are remote deposit capture, or mobile remote deposit.**
MPS	**Mobile Payment System**

Key drivers & key issues

Key drivers	m-Commerce
	High penetration of mobile devices
	Always “on-line”
	Fast growing capabilities of mobile devices
	Trust
	Easy to use : comfort.
	Cost savings
	Previous experience of Internet shopping.
	Business opportunities
Key issues	
	Security
	Convenience and availability
	Regulation/Legislation
	International Standards
	Affordability

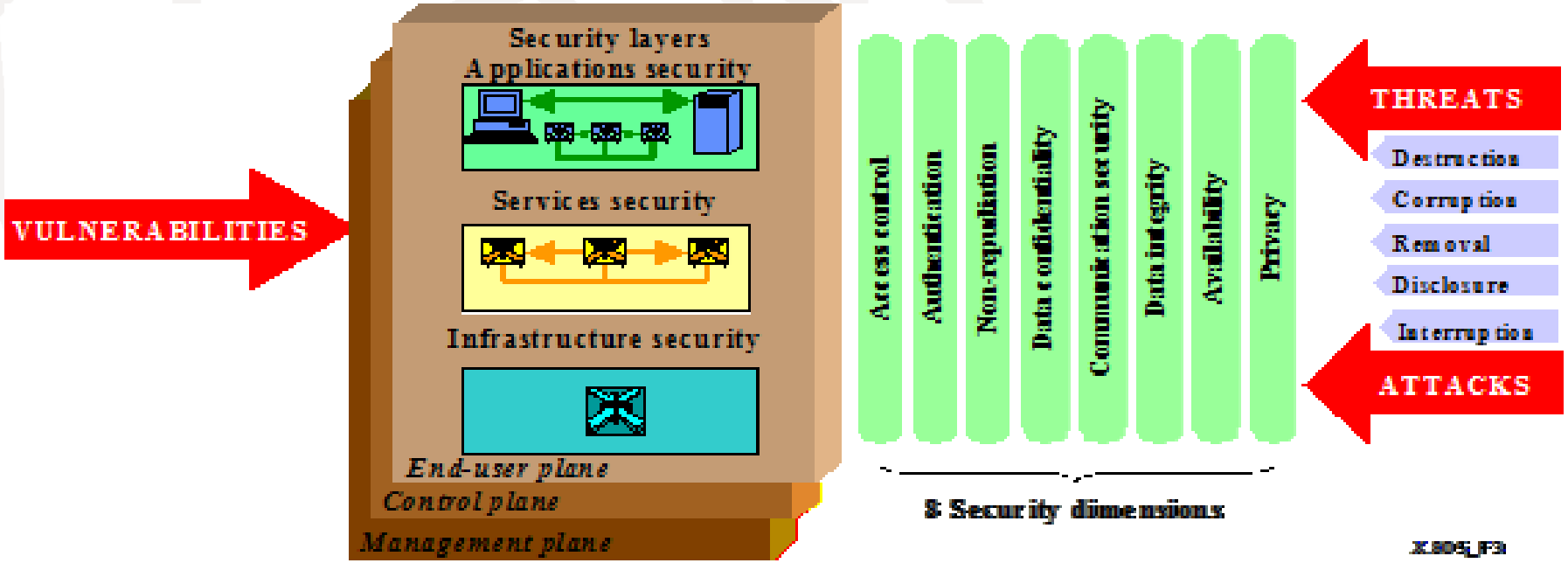
Main stakeholders

Main stakeholders	m-Commerce
Costomers	+++
Professionals in technology and services	+++
Gov. /Regulatory bodies	++
Banks	+++
Telco Operators	+++
Services & App providers	+++
IT Technology Vendors	++
Content providers	+
International Organizations	++
Funding/Sponsors	+

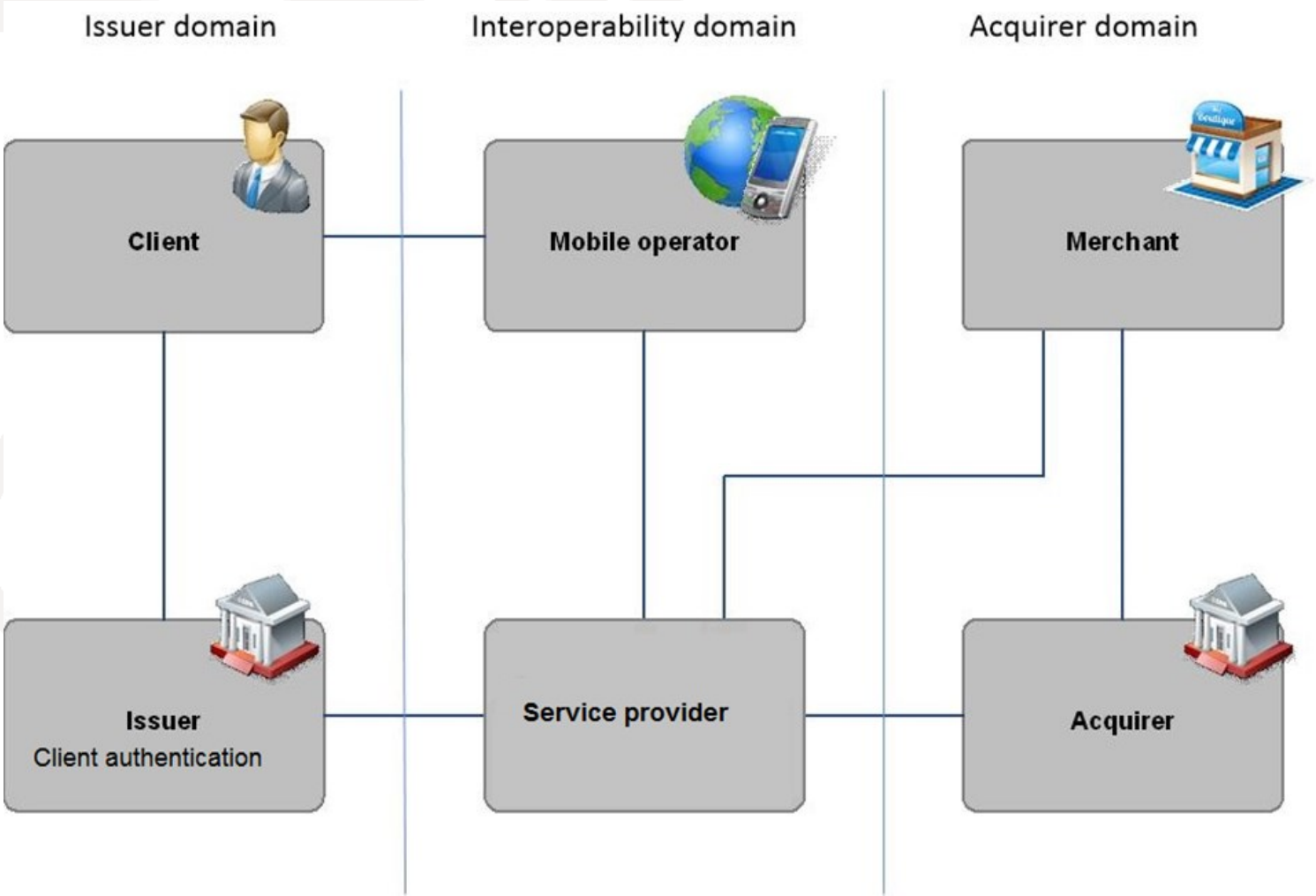
Security

- Confidentiality (encoded messages between Agency and Client)
- Integrity of data
- Impossibility of refusal and attributing of authorship of transaction
- Multifactor authentication (establishment of authority)
  - Something you have (mobile application)
  - Something you know (password or PIN code)
  - Something you are (biometric)

Security architecture for end-to-end network security



3-D architecture of m-Payment system



ITU-T Y.2740 Recommendation.
Security levels

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	The authentication in the System is ensured by the NGN data transfer environment	Single-factor authentication at the System services usage	Multi-factor authentication at the System services usage	In-person connection to services where personal data with obligatory identification is used. Multi-factor authentication at the System services usage. Obligatory usage of a 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.			
Data confidentiality	At data transfer, their confidentiality 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.		At message transfer data confidentiality is ensured by additional message encryption together with data transfer protocols that ensure the security of the data being transferred by the interoperation participants (including data integrity verification); at data storage and processing their confidentiality, integrity and privacy are ensured by additional mechanisms of encryption and masking together with well-defined distribution of access in concordance with privileges and permissions.	The implementation of the Level 3 requirements with the obligatory usage of hardware cryptographic and data security facilities on the Client's side (Hardware Cryptographic module).
Data integrity				
Privacy	Privacy is ensured by the absence of sensitive data in the messages being transferred as well as by the implementation of the required mechanisms of data storage and the System access control facilities. The System components must not have latent possibilities of unauthorized data acquisition and transfer.			
Communication security	The delivery of a message to the addressee is ensured as well as the security against unauthorized disclosure at time of transfer over the communications channels. It is ensured by the NGN communications providers.			
Availability	It ensures that there is no denial of authorized access to the System data and services. Availability is assured by the NGN communications providers as well as the service providers			

Trusted Execution Environment

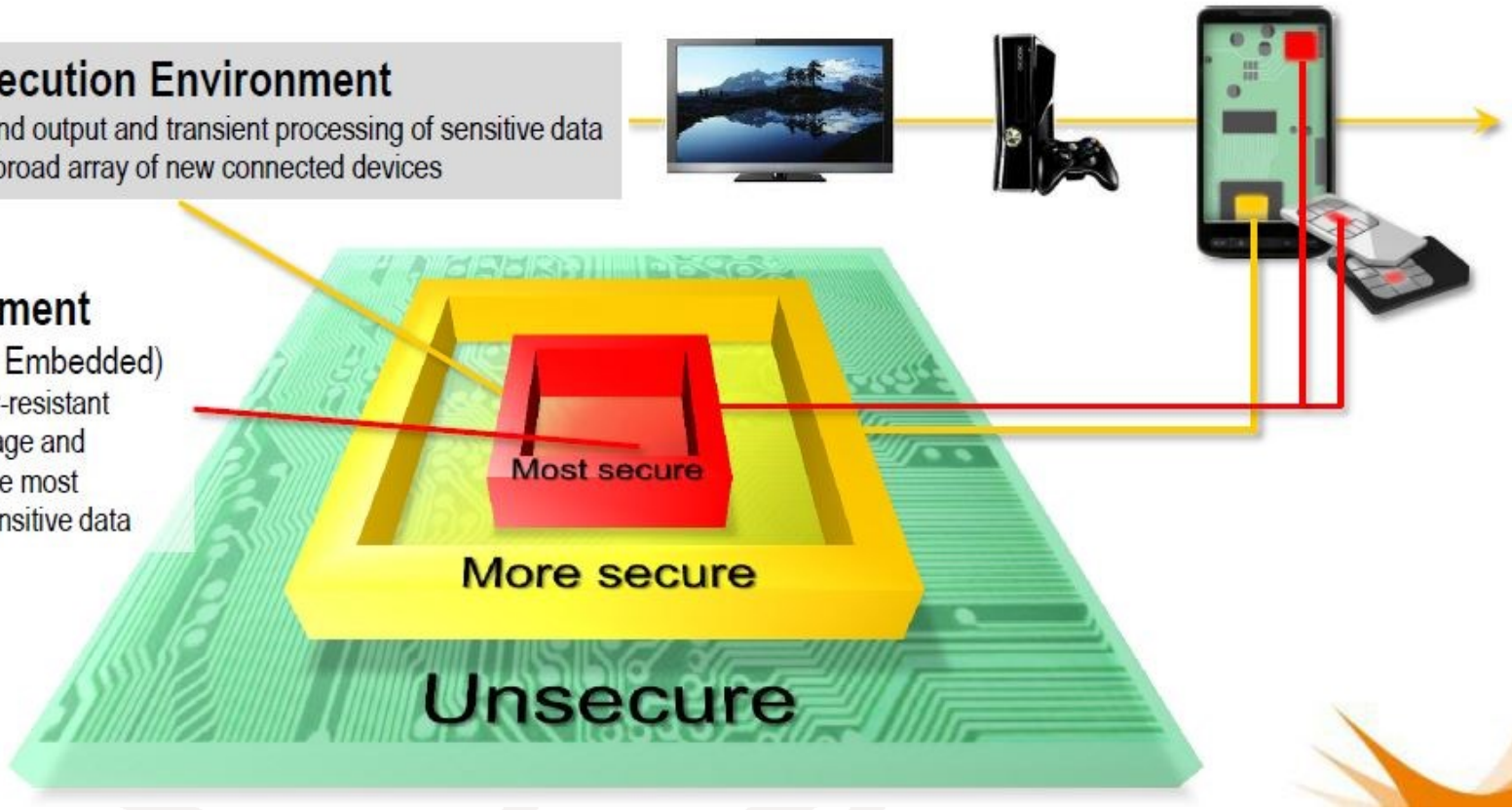
Trusted Execution Environment

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

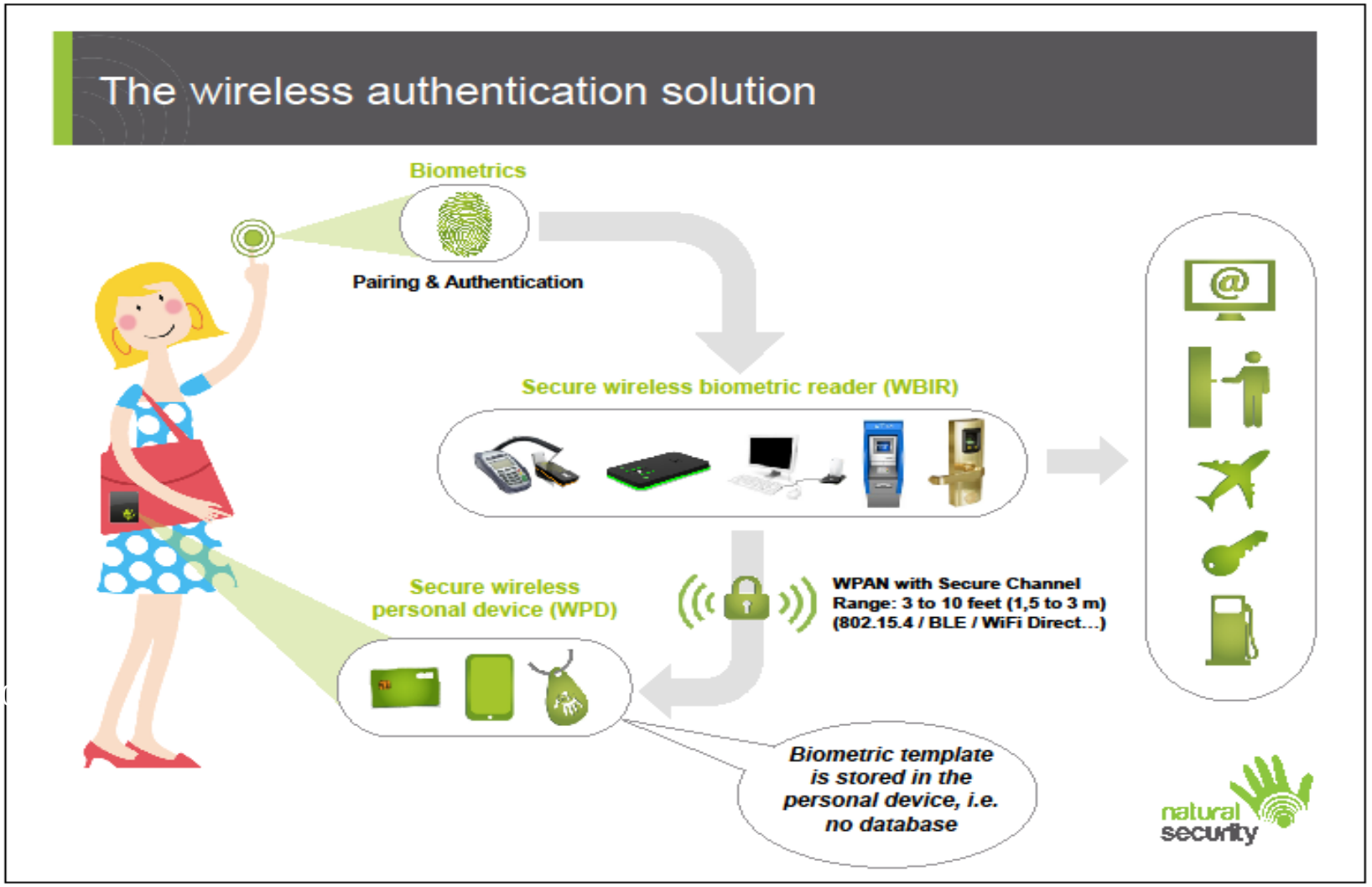
Secure Element

(Removable or Embedded)

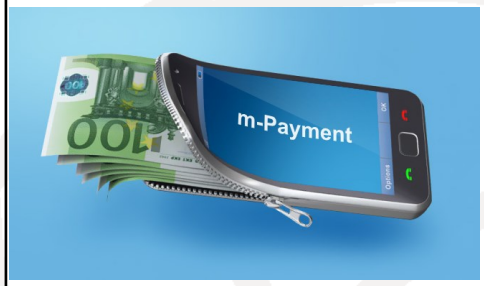
- Certified tamper-resistant
- For secure storage and processing of the most valuable and sensitive data



Biometric authentication



Variety of MPS solutions



		Means of payment				
		Bank account	Payment card	MNO account	e-money account	Other accounts
Technical implementation	WEB	**	*		*	*
	SMS/USSD	*	*	**	*	*
	Voice	*	*			*
	Application	***	***	***	***	***

Application-based Solutions

- No encryption
- Encryption and multifactor authentication
- Secure Element
- Cloud Secure Element
- Trusted Execution Environment
- Biometric Authentication

Recommendations (1)

- Mobile devices can successfully serve as payment terminals and secure communication instruments.
- Unified e-Commerce systems both with the use of laptops and mobile devices can give a choice to user to use mobile or fixed device dependent on the situation.
- Mobile device is a “digital wallet” for electronic identity cards, payment instruments and other applications such as loyalty, transport or ticketing and optional personal information items belonging to the holder (e.g., pictures, documents, etc.).
- MPS users should not be bound to any specific MNO or Bank, and should retain their current ability to choose service providers.

Recommendations (2)

- 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 Level 3 or 4 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.
- To ensure the security and to be user-friendly, the mobile device must have a special Mobile Application, providing 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.

Recommendations (3)

- 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.
- Mobile device should store minimum sensitive information.
- To reach the highest security level, sensitive data should be located at the hardware Security Element in Trusted Execution Environment.
- 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.

The digital wallet is replacing the leather one

Thank You !