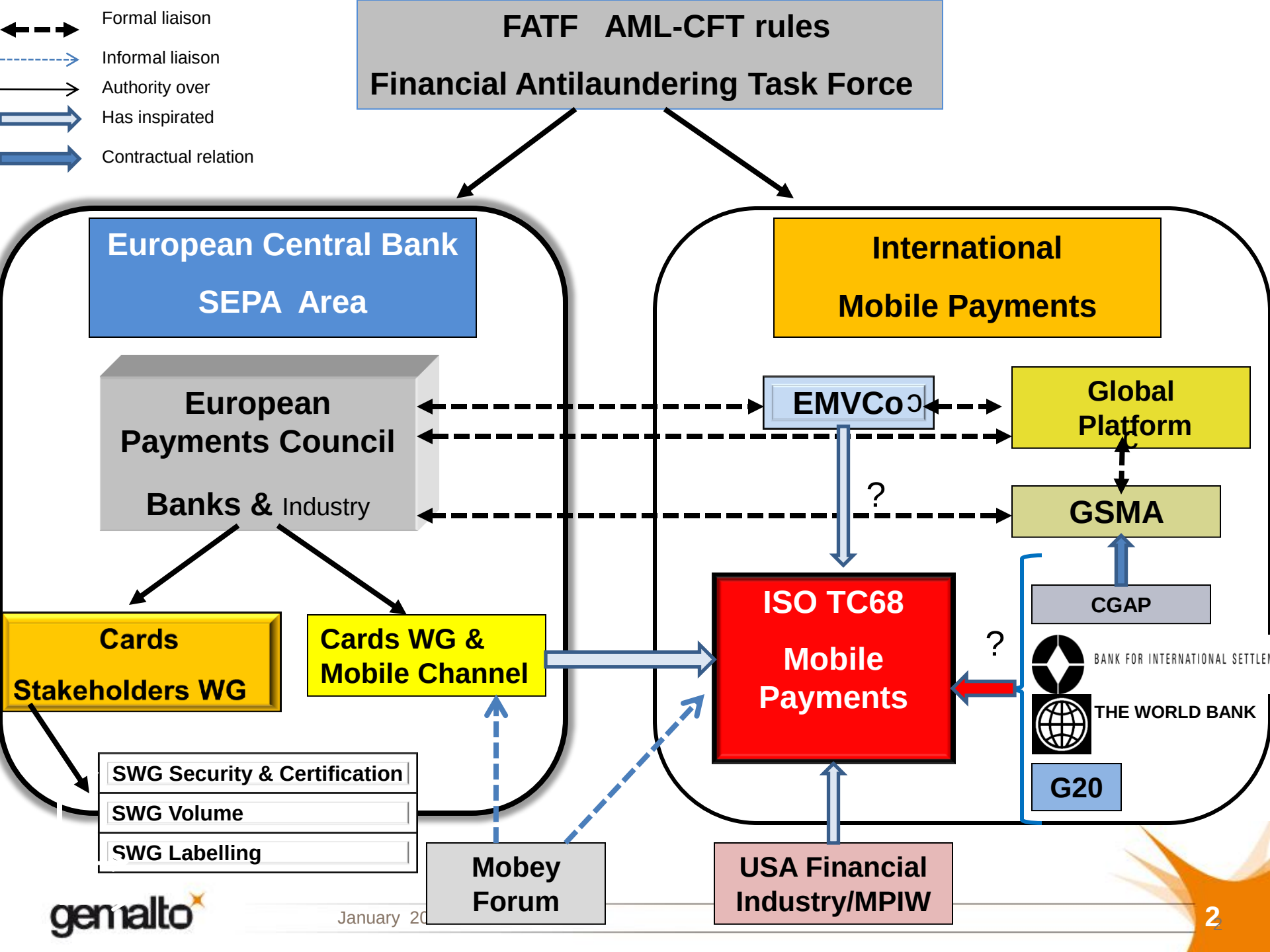
ISO 12812

A Global Standard for Mobile Payments / Banking

ISO TC68 SC7 WG10

Mobey Forum 26 January 2011


Formal liaison
Informal liaison
Authority over
Has inspirated
Contractual relation
FATF AML-CFT rules
Financial Antilaundering Task Force
European Central Bank
SEPA Area
International
Mobile Payments
European
Payments Council
Banks & Industry
EMVCo
Global
Platform
?
GSMA
CGAP
ISO TC68
Mobile
Payments
?
BANK FOR INTERNATIONAL SETTLEMENTS
THE WORLD BANK
G20
Cards
Stakeholders WG
Cards WG &
Mobile Channel
SWG Security & Certification
SWG Volume
SWG Labelling
Mobey
Forum
USA Financial
Industry/MPIW

New ISO TC68 SC7 Mobile Banking / Payments

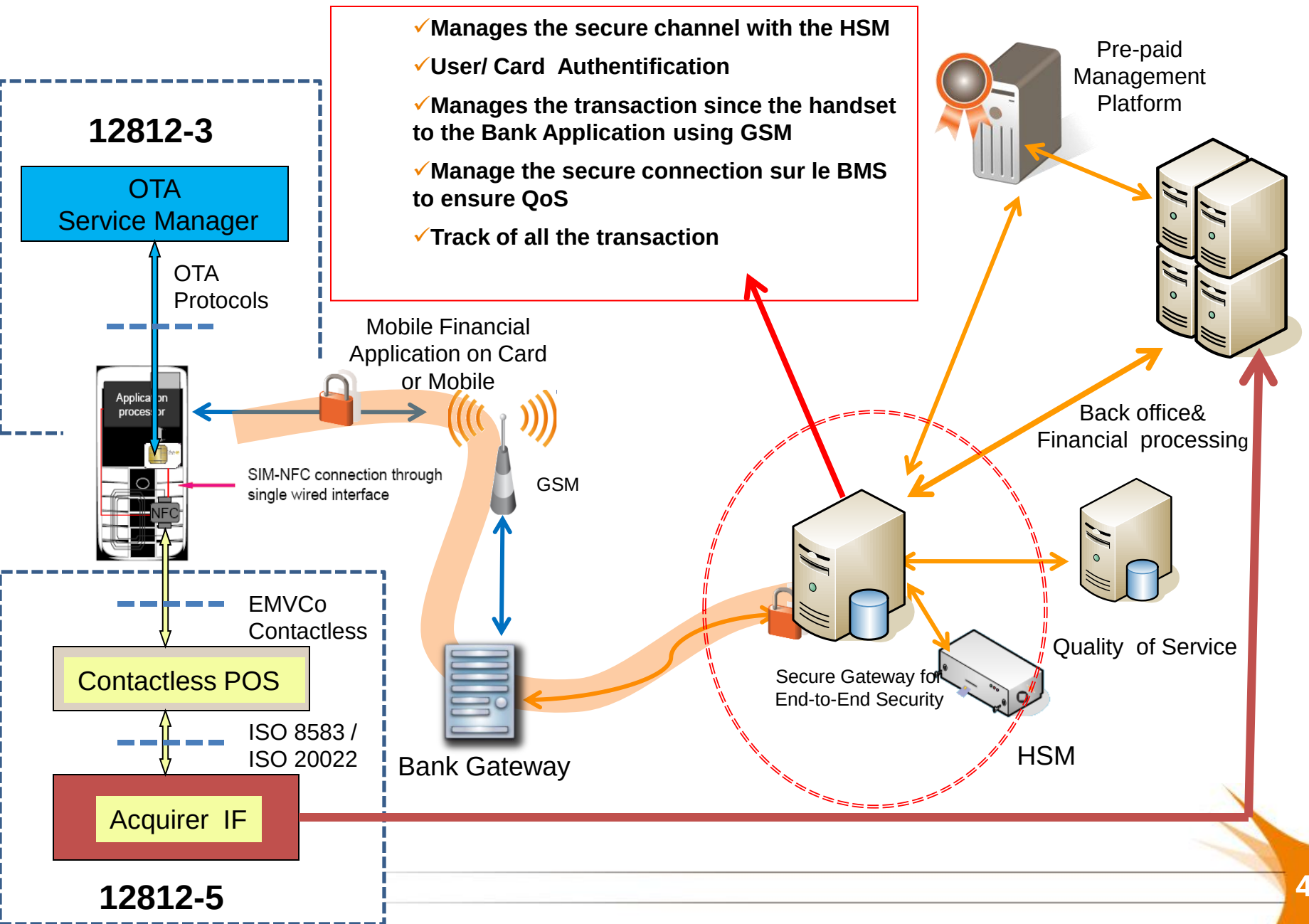
- WG10 set up upon approval of the NWIP submitted by ANSI X9
- Kick-Off meeting in Federal Reserve of Boston last December
- In principle five-part standard with editorial responsibility as follows:

1. ISO 12812-1 General Framework
2. ISO 12812-2 Security and Data Protection
3. ISO 12812-3 Financial Application Management
4. ISO 12812-4 Mobile P2P Payments
5. ISO 12812-5 Mobile P2B Payments

Still in the Pipeline

- *Mobile Banking Services , enrollment , advertising, user interface*
- *Inclusion or Mobile Money or not*

Generic Mobile Financial Services Architecture



Services mediated by TSM Trusted Service Manager

- Mobile Network Operators (MNO) who are the owners of the UICC card and also own in most of the cases an OTA platform
- Service Providers (SP) who are entities providing a service to consumers and need to have their application implemented on a UICC card
- A Secure Element also might be owned by a Financial Institution and store/load applications from other Service Providers using an OTA platform
- Trusted Service Managers (TSM) who enable the link between the Service Provider and the MNO providing (subcontracting) the technical capability to:
  - Allow the MNO to send messages to the SP
  - Allow the MNO to perform NFC services management
  - Allow the SP to send messages to the MNO
  - Allow the SP to perform NFC services management
  - Optionally, have commercial roles (aggregator, commercial intermediate,commercial agent, end user support, etc.)
- Confidential Key Loading Authority (CKLA) who is responsible for enabling the initial key set in a confidential way

Specific Weaknesses in Mobile Payments

Common security features:

- Mobile platforms become more evolved with advanced features (e.g. multimedia capabilities) and connectivity (Bluetooth, WiFi, 3G, Wimax, etc.)
  - Security vulnerabilities seen in PC world spread to mobiles (viruses, trojan, backdoors, keyloggers): enable MiM attacks and identity theft
- Authentication, confidentiality and integrity not often built in by design in standards

SMS channel

- Insecurity of the GSM protocol
  - Encryption & authentication algorithms in use have been cracked
  - Ability to forge & intercept SMS messages
- Rogue base stations enabling Man-in-the-Middle attacks

Contactless M-payments (and cards)

- No mutual authentication in the RF transport layer used (pick-pocketing, relay attacks)

ISO 12812-2 Mobile Banking Security Framework

- Assessment process establishing the specific application context, risk identification, analysis, evaluation and treatment
- Security Architecture for the Handset + Embedded SE
- Secure Certification aspects
- User Authentication to be referred PIN and Biometrics,
- Cryptography protection methods and related key management requirements form existing ISO standards
- Data Protection, including AML / CFT and Data Privacy Compatibility
- Mobile Digital Signature
- To be specified:
  - User account management and security
  - Password management and security
  - Configuration management and security
  - Software Assurance
  - Device Authentication
  - International Mobile Equipment Identity (IMEI) management and security

RF Interface: Security & Data Protection objectives

- **Establishment of a secure channel to avoid eavesdropping**
  - Authentication protocols and of Key Session Establishment to create a Secure Channel between a mobile handset an a contactless payment terminal
  - The confidential channel enables the mobile handset and the terminal to exchange data (e.g. strong authentication and/or personal data) avoiding eavesdropping
- **Other security services / properties**
  - Mobile Payer authentication
  - Secure Element Authentication
  - Keep confidential the data transmitted over the channel diuring transmission time: « forward-secrecy »
  - Preserve « privacy » of those data enabling the identification of either the Secure Element/ Mobile Handset or the Cardholder prior to the creation of the secure channel
  - **Very Highly Secure** :
    - Be « man-in-the-middle » resistant
    - Be « browser » in the middle resistant

On Mobile Digital Signatures

- ISO 10812-2 shall pay attention to Mobile Digital Signatures because of the significant use cases for Mobile Financial Services

  - Subscribing a contract for access to a new Mobile Financial Service
  - Confirming a remittance
  - Generating an e-Invoice
  - Proceeding to a Mobile Commerce Transaction
  - Identification of Mobile Payers / Confirmation of Mobile Payments
  - Downloading and transferring of e- Mobile money
  - ….

- There are standards than may serve as a starting point:

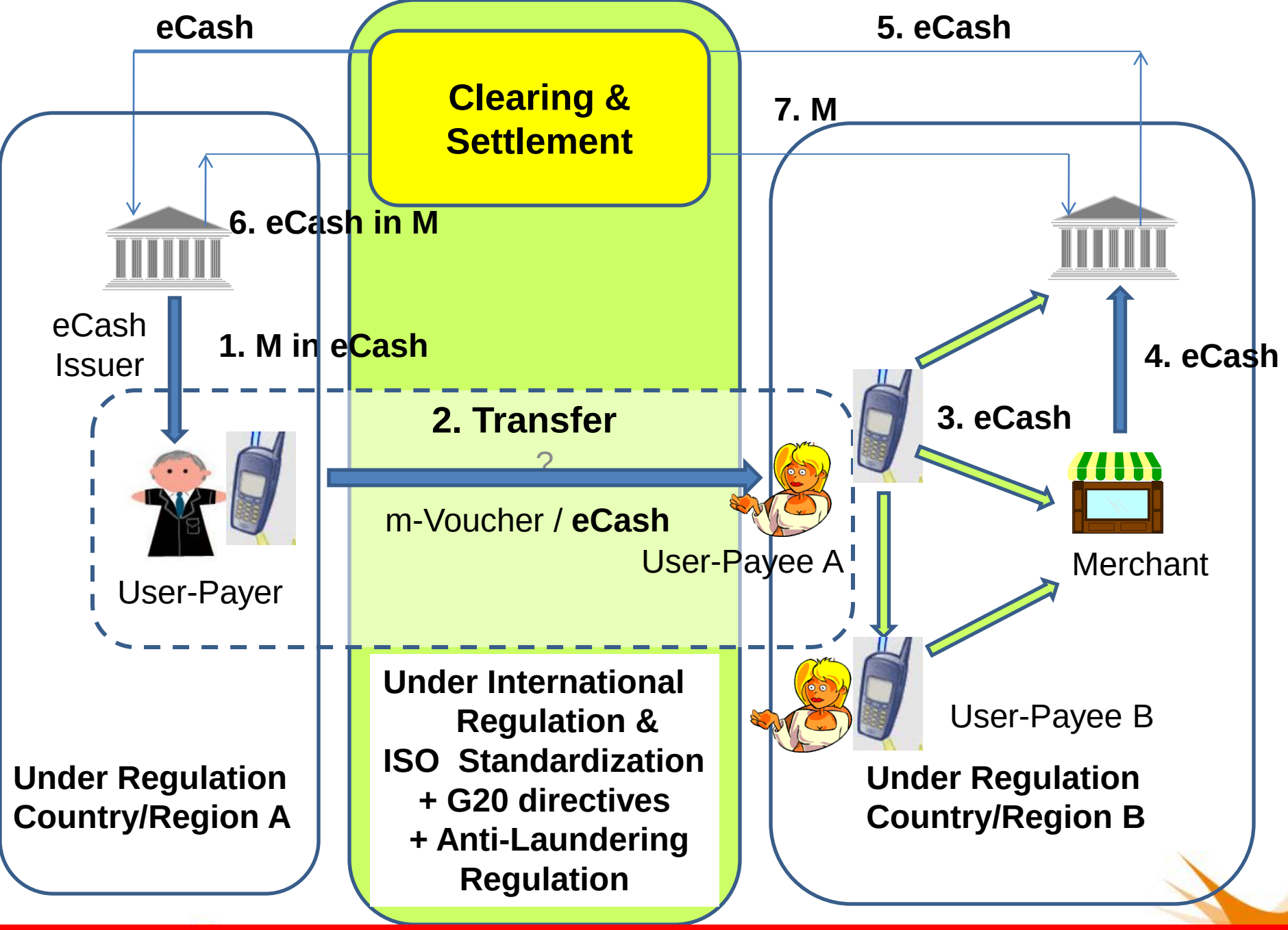
  - ETSI/ESI, “Algorithms and parameters for Electronic Signatures - Part 2: Secure channel protocols and algorithms for signature creation devices”, TS 102 176-2, Draft version 1.2.1, July 2005
  - ISO TC68 SC2 has published the technical report **ISO/TR 14742 on** recommendations on cryptographic algorithms and their use for financial services

PSP	Banks	E-Money Issuer	PI
Services permitted	**Taking deposits & granting credits + Providing payment services**	**Issuing & managing Electronic Money + Providing payment services**	**Providing payment services**
Prudential regime	**Banking Directives (2006/48 /EC and /49/EC)**	**EMD (2009/110)**	**Payment Services Directive (2007/64)**
On- pipeline	**Countercyclical Capital** Buffer **- -Project 2010/11**	**Not planned**	**Not planned**
Information to be provided to users	**PSD + Other texts (e-Privacy)**	**PSD + Other texts (incl. EMD + e-Privacy)**	**PSD + Other texts (incl. e-Privacy)**
Rights and duties of users and PSP	**Payment Services Directive (2007/64)**	**Payment Services Directive (2007/64)**	**Payment Services Directive (2007/64)**
On-pipeline	**- PSD evolution to set SEPA deadlines 2012 - Directive on Basic Payment Account 2011**		**-PSD evolution to set SEPA deadlines 2012 -Directive on Basic Payment Account 2011**
AMF/CFT rules	**3rd AML Directive + Reg 1781/2006**	**3rd AML Directive (possible exemption for e-money; + for M payments?) + Reg 1781/2006**	**3rd AML Directive (possible exemption for M-payments?) + Reg 1781/2006 (exemption for M-**

Regulatory AML provisions

- Introduces obligations for banks and money remitters
- Apply to transfer of funds **in any currency** send or received by **any payment service provider** in the EU
  - Money transfers shall be **always** accompanied by the identity of the sender including the name, address and account number
  - Regardless of the amounts involved
  - A **simplified** version of this regime is proposed for money transfers **within the EU**
- Difficulty of application
  - The regime means that banks or money remitters **reject unidentified transfers**
  - PSPs should restrict or even terminate business relationships with their counterparts when they systematically fail to provide information on the sender

    (eg, a Mobile Operator)
  - But at the same time leaving room for waivers:
  - **Regulation 1781/2006 on information on the payers accompanying transfers of funds**
    - M-payments can be excluded if they are:
      - Prepaid and transactions < 150€
      - Postpaid and:
        - The beneficiary is a merchant having contractual relationship with the PSP
        - There is a unique identifier which allows to trace back up to the originator



To be decided yet ……

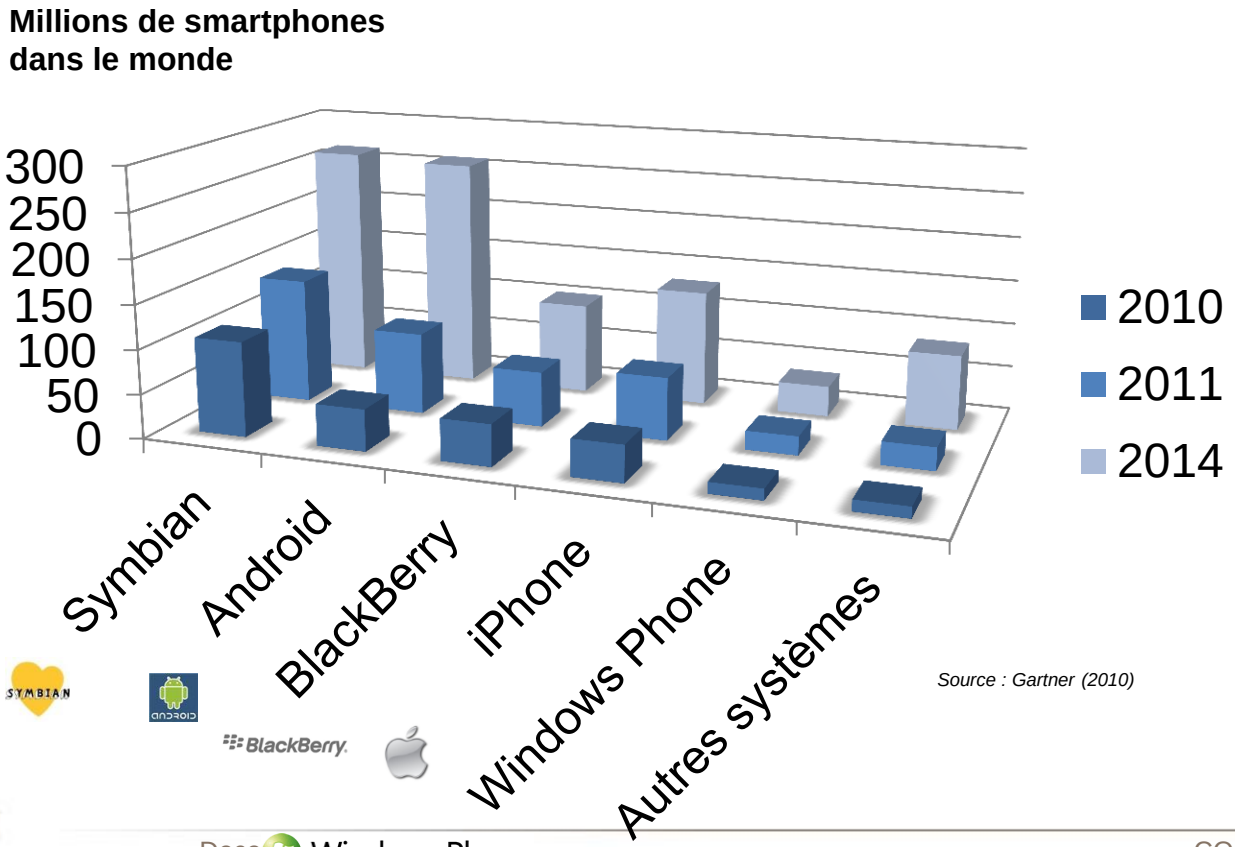
Conclusions

- The structure of the standard has been defined and approved at the WG10 Kick-Off in Boston
- Intention to progress fast despite the fact this is a five-part standard
- Scope and standardization areas to avoid overlapping with other on-going work in other industry-driven bodies
- The original NWIP scope has been somehow revamped.
  - Mobile Banking has been considered in the competitive space and not subject to standardization at present.
  - Mobile Money pending of decision
- Aggressive timeline
- Commitment by all the WG10 experts to come along
- Establishment of a liaison with the European Payments Council on-going

New ISO TC68 SC7 Mobile Banking / Payments

Provisioning of banking applications

- Any mobile banking application must be able to interact seamlessly wit various mobile phone operating systems on the market
- Includes Microsoft's Windows Mobile, Google's Android or Apple's iOS



Source : Gartner (2010)