mobey forum
mobile financial services

Welcome to Mobey Forum's Member Exclusive Webinar

Best Security Practices for NFC Mobile Payments

The webinar will start at 4 pm CET.

All participants will be placed on mute for the duration of the presentation in order to reduce background noise.

17 th December 2013

Welcome to the Webinar

Presented by:

Sirpa Nordlund, Executive Director, Mobey Forum

Mario Maawad, Mobey Forum's Security Workgroup Chair and Digital Security Director at CaixaBank

Zaf Kazmi, Mobey Forum's Security Workgroup Vice-chair, and Head of mCommerce at CaixaBank

Ricardo Marin, Senior Mobile Security Consultant at GMV

Objectives

To provide Guidelines on NFC security related **Best Practices** to all stakeholders within the NFC Mobile Payments ecosystem

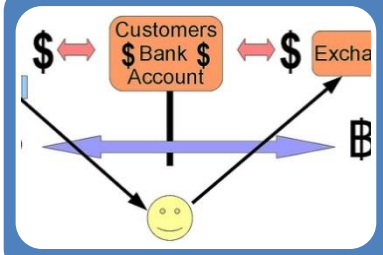
Enhancement of the overall security of NFC Mobile Payment Services based on the following scenarios:

- Securing the Mobile Device Lifecycle
- Delivering Financial Data Securely to the NFC Mobile Device
- Securing the User Financial Data
- Securing the Mobile Payment Applications
- Securing the Communication Between the NFC Mobile Device and the POS Terminal

Configuration Models

Simple Model

- MNO performs the Card Content Management with the supervision of the TSM.

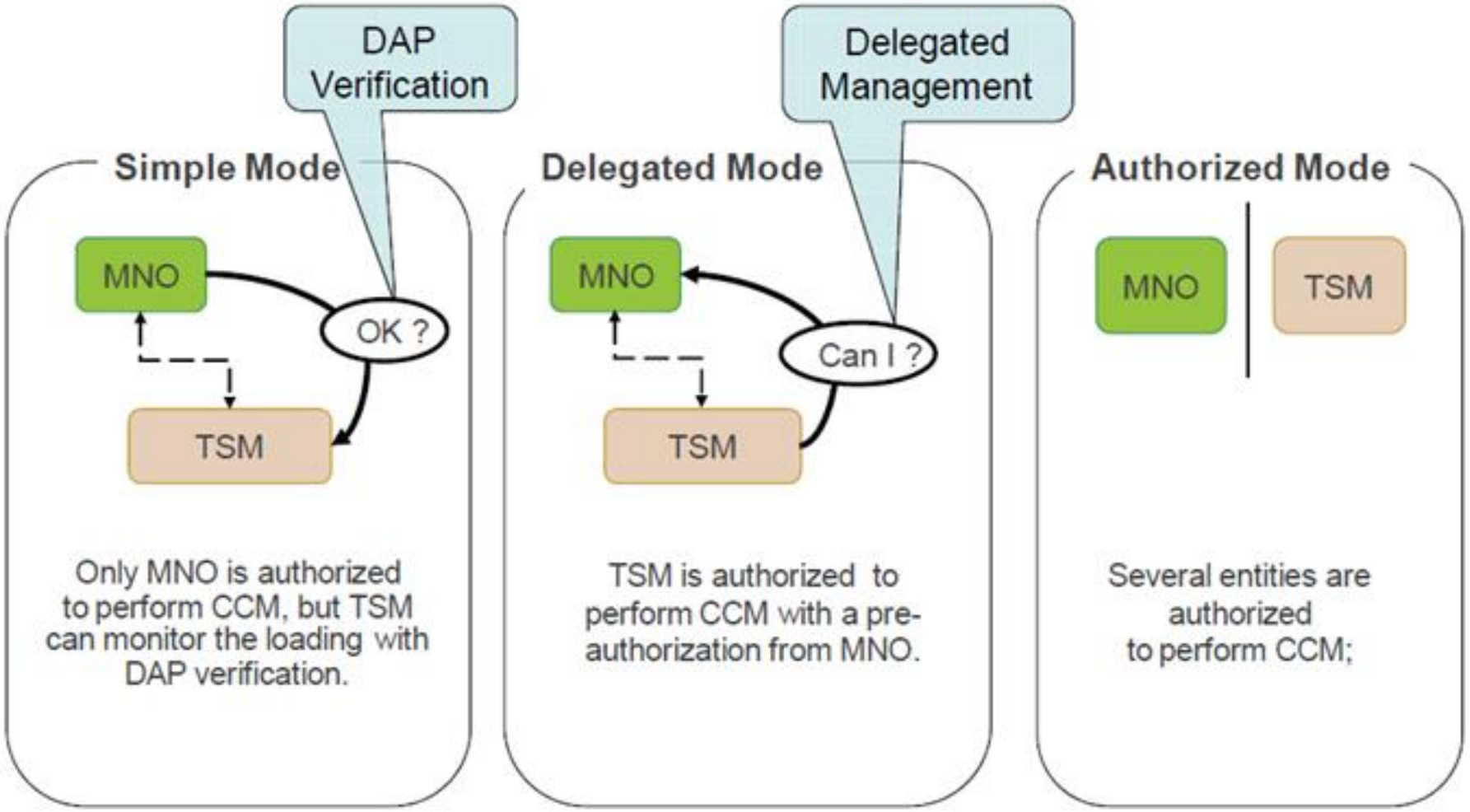


Delegated Model

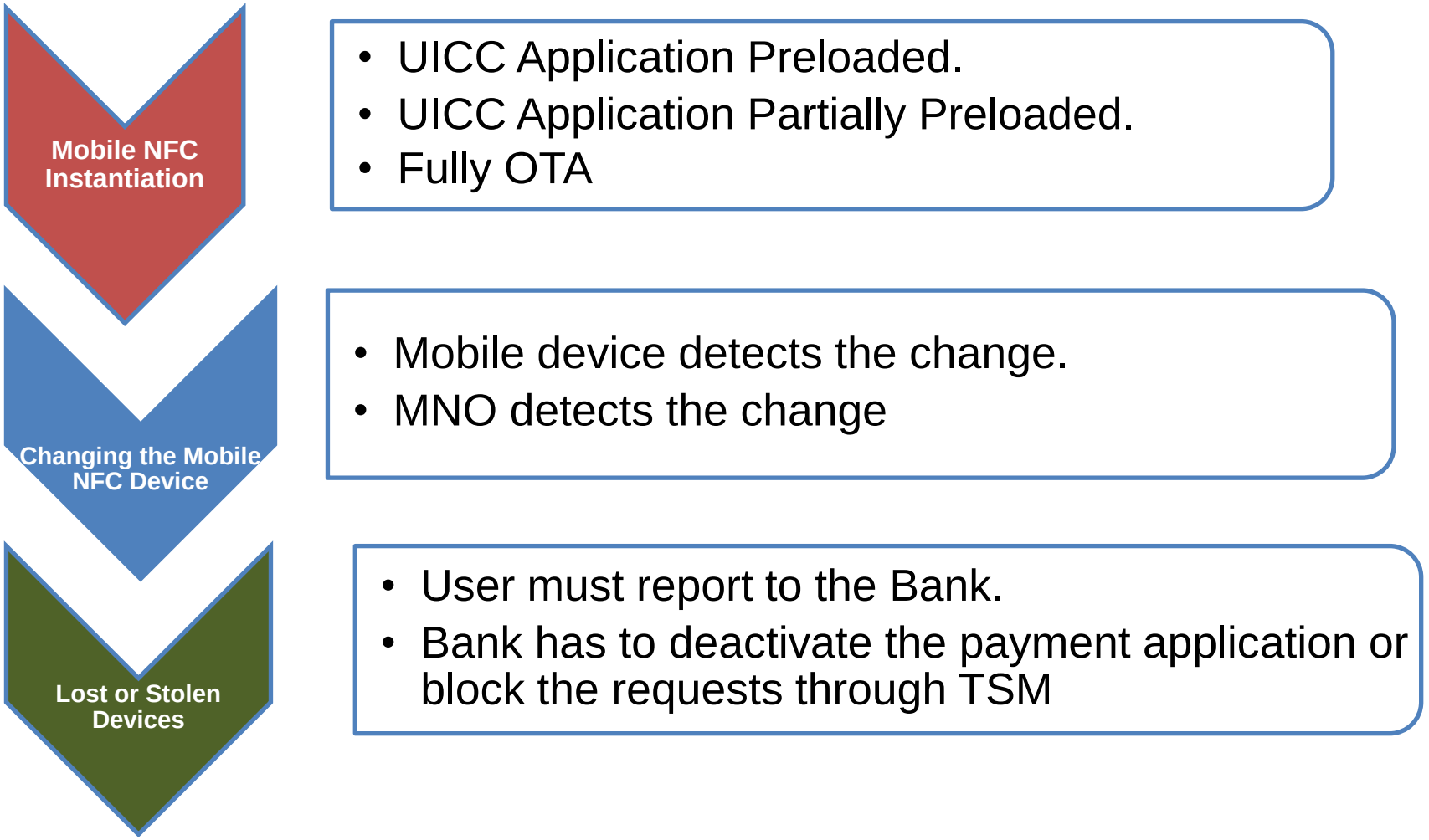
- The Card Content Management is carried out by the TSM, but all operations must be authorized by the MNO.

Authorized Model

- Card Content Management is fully delegated to the TSM but only for a part of the UICC.


DAP Verification
Simple Mode
MNO
OK ?
TSM
Only MNO is authorized to perform CCM, but TSM can monitor the loading with DAP verification.
Delegated Management
Delegated Mode
MNO
Can I ?
TSM
TSM is authorized to perform CCM with a pre-authorization from MNO.
Authorized Mode
MNO
TSM
Several entities are authorized to perform CCM;

Mobile Device Lifecycle



Delivering Financial Data

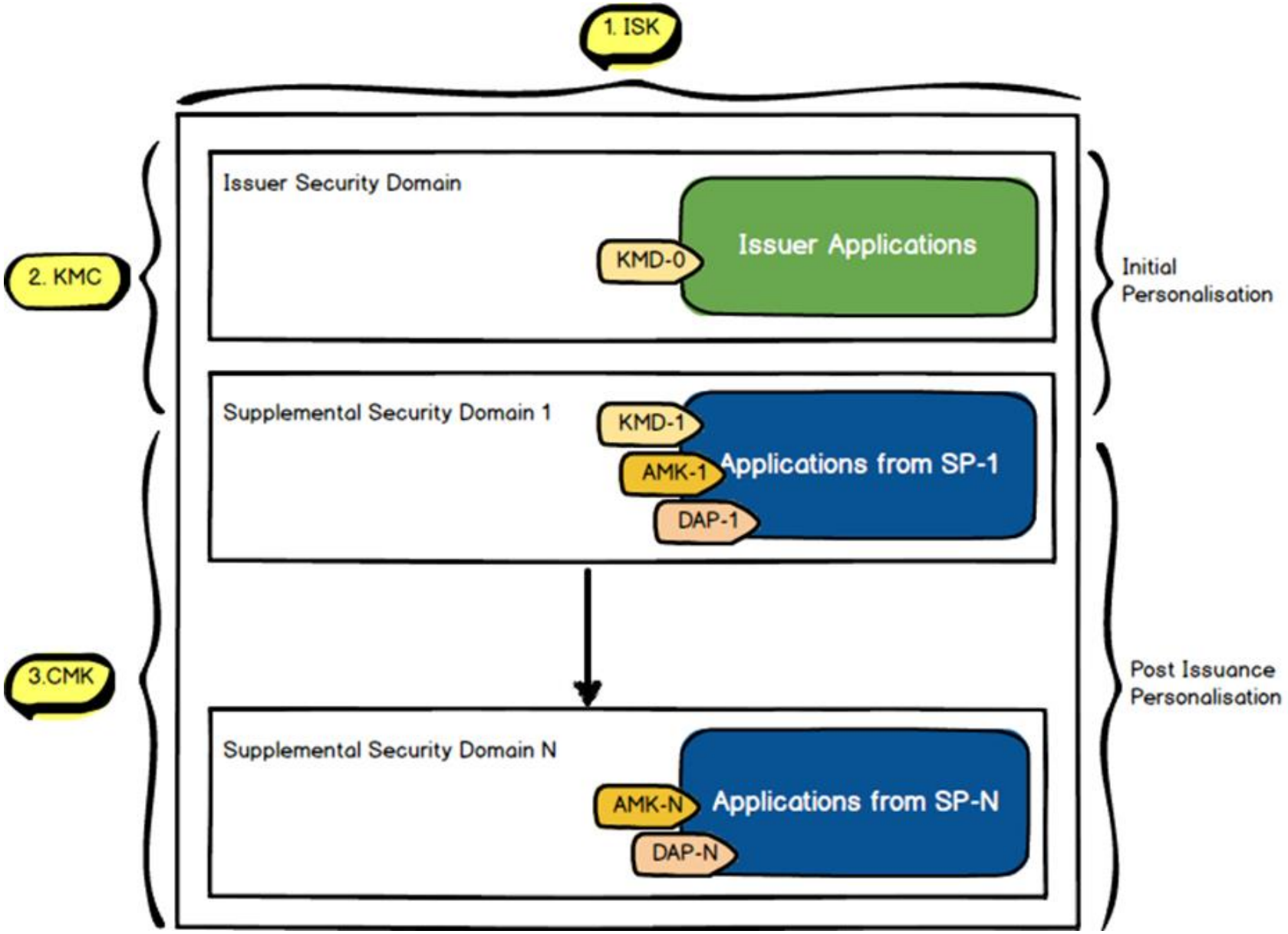
Delivering Financial Data Securely to the NFC Mobile Device.

- The financial data is issued by a bank and passed through a TSM to the SE in the mobile device.
- The objective is to protect the data with cryptography throughout this process
- The protection of this process is achieved using the following concepts:
  - ✓ **Cryptography -** An important factor to consider in order to keep the financial data secure in a mobile payment environment.
  - ✓ **Key Management -** A good Key Management Process keeps the cryptographic keys secure in a logical and physical way.
  - ✓ **User Data Persistence -** TSM could or could not access to the user's data depending on the scenario.

Securing User Financial Data

- The protection of User Financial Data is achieved by reviewing:
  - ✓ How to store financial data in the mobile device.
  - ✓ How this data is accessed securely by the applications and by the POS terminal.

- User Financial Data can be located in:
  - ✓ USIM
  - ✓ Embedded SE
  - ✓ SD Memory Card


1. ISK
2. KMC
3.CMK
Issuer Security Domain
KMD-0
Issuer Applications
Supplemental Security Domain 1
KMD-1
AMK-1
DAP-1
Applications from SP-1
Supplemental Security Domain N
AMK-N
DAP-N
Applications from SP-N
Initial Personalisation
Post Issuance Personalisation

Securing Mobile Payment App

The objective is to design, develop and deploy a mobile payment application safely and avoiding risks to user data:

- ✓ Assuring that the **code has not been tampered** or altered without authorization.
- ✓ Developing the application based on **secure coding** guidelines.
- ✓ Preventing software attacks by installing software only from **trusted sources**, protecting the device from malware, etc.
- ✓ Designing and implementing appropriate **controls**.
- ✓ **Limiting** exposure of account **data**.
- ✓ Ensuring proper **monitoring** of Mobile Payment Acceptance solutions.

Securing Communications

Securing the communication between the NFC mobile device and the POS terminal.

- The payment application may be designed to be password protected.
- The consumer must enter a password to initiate, respond or validate a payment.
- A wallet can be loaded to manage multiple payment applications.
- PIN is the most common password.

Conclusions

- NFC services tend to be **multiple SE operable in an aggregation** model. Best practices need to be followed as per the standards that support this kind of model.
- The **MNO plays the most important** role in the mobile device lifecycle (within the UICC based SE implementation scenario). MNO can however, authorize another stakeholder to manage the main tasks.
- It is recommended that the **UICC cryptography** to be implemented using public key cryptography, in order to enhance the identity and integrity of the financial data.
- The **Key Management** is based on the exchange of keys between the stakeholders depending on a relationship of trust.
- The **development of a Mobile Payment** application should follow the coding guidelines as per the best practices. A Mobile Payment application should be signed, continuously tested and updated.
- The secure management of an NFC mobile payment ecosystem depends on the **binding strength** of each of the stakeholder.

Discussion

"Recommendations for the security of mobile payments" as published very recently by the ECB
http://www.ecb.europa.eu/press/pr/date/2013/html/pr131120.en.html

Mobey Forum will aggregate the comments of the several WG's impacted by these recommendations with the aim to send a final response to the ECB at the end of January 2014.

Please send your comments by 3rd of January 2014. The template is here:
http://www.ecb.europa.eu/paym/cons/pdf/131120/pc131120_1_template_en.pdf?97d3ce051d8d548c059b8a0cdd532429

Questions?

For further information on Security white papers please visit us at www.mobeyforum.org

Want to join the group?

Do you have Webinar feedback?

Please contact:

Sirpa.nordlund@mobeyforum.org