Workshop Review

- Anatomy and Architecture of a Mobile Device
- Fundamentals of NFC
- Trusted Execution Environment (TEE)
- Secure Elements (UICC/SD/eUICC)
- Host Card Emulation (HCE)
Where does all this lead?

Mobile Payments
Mobile Payment Technologies

- **NFC**
  - Secure Element Based
  - Host Card Emulation (HCE)
    - Secure Element in the Cloud
    - Software

- **Bluetooth Low Energy (BLE)**
  - iBeacon
  - Paypal

- **Other**
  - PayPal
  - Loop
  - Starbucks
The NFC Mobile Ecosystem

ISSUER
- Card Issuers
- Debit
- Credit
- Rewards
- Transit
- Retail
- Government
- Access cards
- Loyalty applications

SP-TSM
- Connects issuers and MNOS/SEIs
- Application life cycle management
- Key Management
- High security

SEI/MNO-TSM
- Secure Element Management
- Provides interface for SP-TSM
- Security domain management
- SIM OTA
- Wallet management
- Delegated authorization

MOBILE WALLET
- Provides subscriber credential interaction
- Displays installed credentials

NFC HANDSET
- NFC antenna
- BIP/HTTP Capable
- Single wire protocol

NFC SIM (Secure Element)
- Multiple security domains
- Stores credentials securely
- Single wire protocol, connection to the NFC antenna
Credit/Debit Payment Ecosystem

Merchant
A merchant or retailer, sells commodities to consumers (including businesses), usually in small quantities. A shop owner is a retail merchant. To be allowed to accept credit cards a Merchant needs to sign a contract with the respective credit/Debit card network (e.g. Visa) where the Merchant will be known as the Merchant of Record.

Payment Processor
A company that processes transactions and payments on behalf of the Merchant and helps the Merchant to get a Merchant Account from the Merchant Bank and the Credit/Debit Card Network. Some Merchant Banks have their own Payment Processing arm to work with bigger / low risk Merchants directly.

Acquirer / Merchant Bank
The Bank where the Merchant has its Merchant Account. The Merchant Bank has to ensure the Merchant’s credit worthiness and has to guarantee that the Merchant is a legitimate business that delivers the goods paid for.

Credit Card Networks / Associations (aka “Brands”)
The central clearing house for transactions and ensure that transactions are authorized at purchase time (by contacting respective brand with payment details) and are routed between the respective players. They ensure that member banks (in case of Visa/Mastercard) and accepting Merchants are in compliance to their standards.

Issuing Bank
The Bank where the Consumer has its Account. The Issuing Bank guarantees that the merchant gets paid regardless if it can collect the money from the consumer.
How do we...
ISIS Enrollment Process

1. User enrolls with ISIS

2. ISIS verifies eligibility with Issuing Bank

3. Issuing Bank provides Personalization Data (payment credentials)

4. ISIS packages data securely for OTA delivery

5. Application and Data securely transmitted to SE within Mobile Device

6. ISIS Wallet is downloaded from App Store

MNO
Google Enrollment Process

1. User downloads Google Wallet

2. Google provisions virtual MasterCard to device (payment credentials)

3. User associates card with Google Wallet

4. User can associate any card in the cloud to Google Wallet
Payment Transaction Terms

• BIN/IIN - Bank Identification Number/Issuer Identification Number
  6 Digit identification number at beginning of PAN

• PAN
  Primary Account Number (16 digit Credit Card Number)

• Card Present Transaction
  Card transaction in which the cardholder is physically present with the card

• Card Not Present Transaction
  Card transaction in which the cardholder is not physically present with the card

• CVV - Card Verification Value
  3 or 4 digit code used to secure card not present transactions

• DCVV
  Dynamic CVV used in contactless transactions
ISIS Payment Transaction Flow

1. User opens wallet and taps on contactless POS

2. Emulated Magstripe data is passed to POS

3. PAN and DCVV passed to payment processor for routing

4. Based on IIN transaction is routed to correct Credit Card Network and on to Issuing Bank for Authorization

5. Allowed/Denied Authorization passed back to POS

6. Issuing bank and Merchant Bank settle account
Google Wallet Transaction Flow

1. User opens wallet and taps on contactless POS

2. Emulated Magstripe data is passed to POS

3. PAN and DCVV passed to payment processor for routing

4. Based on IIN transaction is routed to MasterCard Network and on to Google for Authorization

5. Allowed/Denied Authorization passed back to POS from Google

6. Google settles with Merchant Bank

7. Google settles with Issuer Bank
How has the Google Wallet changed?

- **Google Wallet 1.0**
  - Followed the ISIS architecture – Secure Element required w/Payment Application
    - Only supported Virtual MasterCard Application
    - Embedded Secure Element contained Payment Application and Credential
    - Limited number of Mobile Devices supported

- **Google Wallet 2.0**
  - Created Hybrid SE/Cloud solution
    - MasterCard Payment Application and Credential contained within SE
    - Connection between Virtual MasterCard on SE and ‘true’ payment method handled in the cloud
    - Same limitation of supported Mobile Devices as Google Wallet 1.0
    - Google began to authorize NFC payment transactions

- **Google Wallet 3.0**
  - Full HCE solution – No SE needed
    - Works with any NFC capable handset running Kit Kat or higher Android OS
    - Connection between Virtual MasterCard and ‘true’ payment method handled in the cloud
    - Google authorizes NFC payment transaction
Key difference SE vs HCE for payment

- Payment Applications and Credentials resides within the Secure Element

- Payment Applications reside as Mobile Device Applications
  - Emulates a SE Application
  - Credentials can be stored within device memory or in the cloud
Questions
Open Discussion