

Maintaining Security Throughout the Value Chain

Eric Johnson



Background

- **G&D America participated in 2 NFC Mobile Payment trials in 2006/2007 as the TTP**
- **CDMA / GSM networks**
- **PayPass Mag-Stripe application for 2 different banks**
- **Embedded NXP Smart MX chip**
- **JavaCard 2.2 : Sm@rtCafé / JCOP**
- **Global Platform 2.1.1**
- **Midlet as card reader proxy**

Present the security aspects of these trials

Remarks apply to both embedded and UICC solutions

Not addressing any business issues

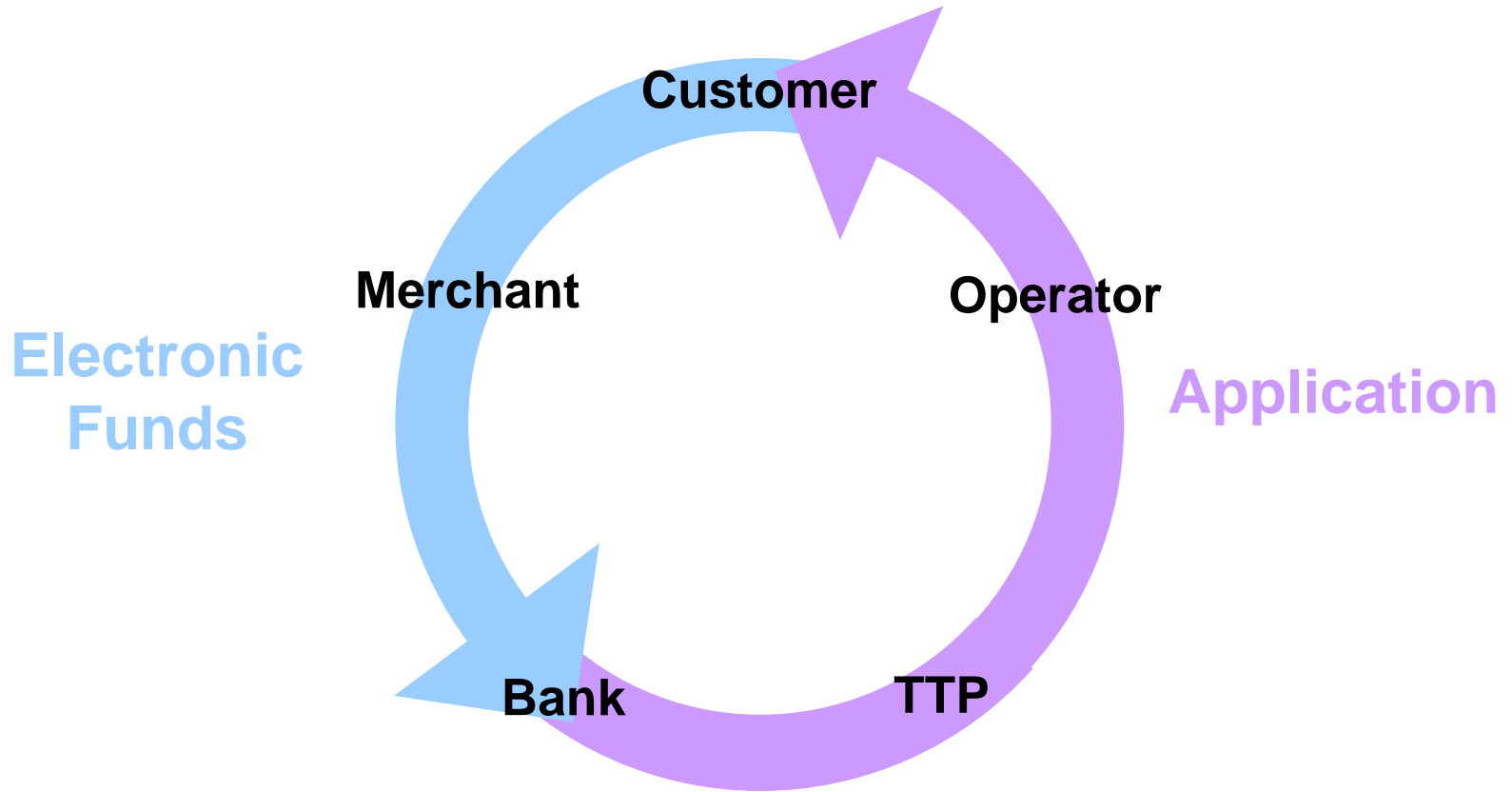


Overview

- **Logical Participants**
- **Activation/Use/Deactivation**
- **Security Mechanisms**
- **Strengths / Weaknesses**
- **Enhancements**
- **Delegated Management**
- **Concluding Remarks**



Logical Participants



Activation Overview

■ Activation

- **Mobile Device manufactured and distributed**
- **Customer Signs Up**
- **Approved by Bank and Operator**
- **Customer provides Activation Password and MSISDN to Bank**
- **Bank sends account data (PAN etc.) to TTP**
- **TTP notifies customer account is ready to setup**
- **Customer initiates download**
- **Customer enters Activation Password**
- **Repersonalization when required**



Use / Deactivation Overview

■ Use

- Customer uses application
- Merchant / Backend operate as usual

■ Normal Deactivation

- Customer/Bank/Operator initiates deactivation
- TTP successfully deactivates application

■ Abnormal Deactivation

- Bank/Operator initiate deactivation
- TTP deactivates application if possible
- Bank adds account to Blacklist

Security Mechanisms

- **Standard Global Platform approach for JavaCard management**
- **Device Manufacturer loads derived 3DES keys**
- **TTP changes keys during Activation**
- **Only TTP can load, install & delete applets**
- **TTP personalizes application with data/key from Bank**
- **Activation Password ensures application delivered to correct *user***
- **Application is at least as secure as standalone PayPass card**
- **PAN can only be used for PayPass transactions (No Card Not Present transactions)**



Strengths / Weaknesses

■ Strengths

- GP secure channel can prevent monitoring attacks
- Builds on existing security infrastructure

■ Weaknesses

- TTP sees and knows everything:
 - card management keys
 - application keys (eg CVC3 keys)
- Activation Password
- TTP doesn't know Device ID
- No Device ⇔ User association



Enhancements

- **Change key on first use or at ATM**
- **Operator provides User \Leftrightarrow Device association**
 - **Implicit with UICC implementation**

- **GP 2.2 adds Public Key option but ...**
 - **Bank/TTP interface is batch oriented: needs to move online**
 - **Need to generate and distribute Public Keys**

- **Security is a balance \Rightarrow can always be improved**
 - **Trials designed to minimize change**
 - **Banks need to modify infrastructure**

Delegated Management

- **Allows another entity to manage approved applets**
- **Applets are signed by Card Issuer**
- **Well suited for case when OTA applet management is possible:**
 - **Starbucks, McDonalds, Jack in Box**
- **GP 2.2 improves Delegated Management option**
 - **Allows delegated deletion**

Concluding Remarks

Trial

- **Technically Successful**

The Future

- **Bank infrastructure changes needed**
- **Looking forward to wider deployment of NFC capable devices**
- **Perfect fit for UICC as a security token**

