Implementing a Cloud-Based Payment with Instant Issuance System

Robin Ehrlich
Chief Software Architect
NBS Technologies
rehrlich@nbstech.com
ICMA Expo and Smart Card Alliance 2016 Conference
About NBS Technologies

• Worldwide leader in secure, scalable credential issuance systems
• Specializes in design and manufacture of equipment and software for smart card manufacturing, card printing, embossing, card personalization and cloud-based payment systems
• First company to be certified as Visa® Ready
• Only company to conform to all Visa and MasterCard Cloud-Based standards
• Allows creation of an eWallet in combination with a companion card
• Allows an eWallet to be incorporated into the bank’s mobile application or used as a top-of-wallet branded app
• Creating a system with a HCE based eWallet is a complex undertaking requiring many components to be integrated seamlessly in order for the system to function correctly
• Many different standards must be followed including EMV, Visa Cloud-Based Payments, MasterCard Cloud-Based Payments and PCI standards
• Provides a company with a competitive edge and a platform well positioned for future industry trends
A Cloud-Based Payment System manages mobile contactless applications in NFC-Enabled Handsets using Android HCE

- Installs and personalizes Visa and MasterCard Cloud-Based Payments
- Provides tokenization services supporting security of PAN
- Supports application lifecycle management
- Manages keys securely
- Protects sensitive data and provides end to end data security
Certification Requirements

• Android eWallet (HCE) Certifications
  • Must be certified by Visa to meet the Visa Cloud-Based Payments Functional Specification
  • Must be certified by MasterCard to meet the MasterCard Cloud-Based Payments both in functionality and via a security evaluation

• Cloud Server Certifications
  • The Cloud Server must be certified by MasterCard to meet all the AES and CMS requirements
  • Currently Visa does not require any server certifications
Cloud-Based Payments Data Flow

Financial Institution

Cloud Server
- Core Server
- Data Preparation
- Key Management

Digital Distribution Platform

Processor

Point of Sale Terminal

Phone

Personalized App

Transactions
Core Server Requirements

- Lifecycle management including personalization, activation, and deactivation
- Tokenization services
- All financial institution data and other sensitive data must be encrypted so no data can be inappropriately shared
- High reliability, availability, scalability and performance
- Configurable reporting and monitoring
- Certification requirements and procedures:
  - MasterCard
  - PCI
  - Visa
Data Preparation Requirements

- Financial institutions may provide data in a variety of **input modes** via:
  - Web services
  - Files in clear text, encrypted by shared KEK, PGP encrypted
  - IBM Websphere MQ queues

- Financial institutions may provide data in many different **formats**:
  - Fixed
  - P3
  - XML
  - Need flexible input parsing rules

- Must provide easily configurable default EMV values
Key Management Requirements

- Managing keys securely is of crucial importance
- Keys must never be in the clear outside of an HSM
- Facilities must be available to securely share keys between trusted parties
- Support of a variety of HSMs so integration with other sources is easy
- Easy and secure user interface to manage keys and certificates
Server Topology

- Must be available 24/7 and support expected peak loads
- Requires conformance to functional and site requirements of
  - PCI
  - MasterCard
  - Visa
- Visa and MasterCard will require a site audit. Surviving an audit can be difficult. It is important to have the appropriate personnel available during the audit.

Total Card Solutions
Desired Handset Features

- White-labeled so that it may be easily branded by the financial institution.
- Modularized so that individual components can be integrated into other applications such as the bank’s mobile application.
- All key generation must be performed securely by the cloud server.
- Visa certification requirements and procedures must be followed.
- MasterCard certification requirements and procedures must be followed.
Instant Issuance Considerations

- Allows NFC enabled phones and companion cards to be easily created
- Different branches may need different equipment therefore the server needs to be equipment agnostic
- Common software can be used to personalize handset and companion card
Other Implementations

**Apple Pay** – only works in iPhone
- Worldwide Android has 80% market share versus 15% for iPhone\(^1\)
- In USA Android has 50% market share versus 40% for iPhone\(^2\)

**Android Pay and Samsung Pay** – generic eWallet
- Not top of wallet
- Financial institutions may need to share revenue with Google or Samsung
- Financial institutions may prefer an eWallet integrated into their mobile application or a branded eWallet

---

\(^1\) IDC Smartphone Vendor Market Share, 2015 Q2
\(^2\) comScore Reports July 2015 U.S. Smartphone
“The function of good software is to make the complex appear to be simple.”
(Grady Booch)

“That’s been one of my mantras — focus and simplicity. Simple can be harder than complex: You have to work hard to get your thinking clean to make it simple. But it’s worth it in the end because once you get there, you can move mountains.”
(Steve Jobs)

“Security is a not a product, but a process. It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.”
(Bruce Schneier)
Questions

Xpressi Cloud
Xpressi eWallet
Xpressi Instant Issuance

For more information please contact
www.nbstech.com
rehrlch@nbstech.com