Mobile/NFC Security Fundamentals

NFC Application Use Cases: Security Perspectives

- Smart Card Alliance and NFC Forum Webinar
- May 9, 2013
Introductions

- Randy Vanderhoof
- Executive Director, Smart Card Alliance
Mobile & NFC Council

- Raise awareness and accelerate the adoption of all applications using NFC
  - Access control, identity, loyalty, marketing, payments, peer-to-peer, promotion/coupons/offers, transit, …

- Accelerate the practical application of NFC, providing a bridge between technology development/specifications and the applications that can deliver business benefits to industry stakeholders.
Today’s Webinar Topics & Speakers

- **Introductions:** Randy Vanderhoof, Executive Director, Smart Card Alliance

- **Isis Mobile Wallet and Payment:** Tony Sabetti, Merchant Integration Leader, Isis Mobile Commerce

- **Using NFC Devices for Logical Access:** Christian Ali, Vice President, Product Management, SecureKey Technologies

- **NFC Forum Tag Use Cases:** Jonathan Main, NFC Forum Technical Committee, MasterCard

- **Physical Access Control Use Cases:** Steve Rogers, President, IQ Devices

- **Q&A:** Randy Vanderhoof, Smart Card Alliance
NFC Application Use Cases: Security Perspectives – ISIS Mobile Wallet & Payment

- Tony Sabetti
- Merchant Integration Leader
- Isis Mobile Commerce
What Is an NFC Mobile Wallet?

- Application for Smart Phone
- Holds credentials on Secure Element
- Presentment via Near Field Communications

- Your current balance and most recent purchases
- Your credit and debit cards
- A prepaid Cash Card
- Loyalty cards
- Offers, deals and promotions

Contactless indicator is property of EMVCo, LLC
Anatomy of an NFC Smart Phone

- NFC phones contain special hardware
  - Secure Element: Stores sensitive data (e.g. payment card information)
  - NFC Controller: Manages traffic and RF signals
  - NFC Antenna: Collects & transmits the RF

- Secure Elements protect data via:
  - Encryption keys / Crypto engines
  - Secured Communications
  - Secured memory

- Secure Element Form Factors:
  - UICC / SIM Cards
  - Embedded
  - MicroSD Cards
Secure Element

- Java Card Operating Platform
- Secure memory
- Contact and contactless interfaces
  - ISO7816 and Single Wire Protocol (SWP)
- Implements Global Platform
  - Smart card specification that defines card components, command sets, transaction sequences
  - Systems specification that standardizes back end systems for personalization, security, key management and application loading
  - Supports multiple security domains - One bank can have its own separate domain for secure credentials and Java applets
End to End Security

1. Bank sends payment credentials via secure connection to the Trusted Service Manager (TSM). Credentials can be encrypted.

2. TSM uses secure carrier channel used by mobile operator to communicate and transfer credentials directly into the Secure Element (SE) on the UICC (SIM). The credential is never stored in handset memory.

3. SE runs Global Platform and a JavaCard OS. Only the bank has the keys to access its customers’ payment credentials in the SE.

4. The Isis wallet running in the handset’s host processor does not even know what the payment credentials are. It does provide basic data for display purposes.

5. The credentials are sent through the contactless interface when power is induced by a payment terminal at 4 cm or less distance.

6. All 4 payment networks use Dynamic CVV – CVV is changed for each transaction.
Security - Consumer Experience

- **Wallet PIN** can be set
- **Extremely short distance** between handset and payment terminal making it difficult to “eavesdrop”
- **Dynamic CVV** protects against any replay attacks
- All sensitive data is stored only on the Secure Element and not accessible to the app or phone OS
- **One call to freeze** your Isis Mobile Wallet if phone lost or stolen
NFC Application Use Cases: Using NFC Devices for Logical Access

- Christian Ali
- Vice President, Product Management
- SecureKey Technologies Inc.
Logical Access Options

NFC enabled devices support strong logical access use cases for:

- Government
- Healthcare
- Banking
- Payments…

Enabled through a trusted device:

- as a reader of external credentials (various form factors e.g. phone, tablet, laptop, peripheral device)
- as a proxy credential (mobile)
Improved Online Experience

- All Intel Core™ & vPRO™ PC (notebook, desktop, convertible, and tablets) will have IPT features enabled for multi-factor (device) authentication.
- OEMs adding NFC capabilities to select SKUs.

Hardware based multi-factor authentication for sign-up/into

Password
Baseline Security
Password + Intel® IPT
Improved Website Security
Intel® IPT + NFC Sensor
Improved Security + Better Experience
Tap and Pay Tap to Authenticate

Intel® Identity Protection Technology (Intel® IPT) + NFC
Proxy Credential in Phone

- Tap card to load credential to verified NFC phone
- Use phone as credential
  - Requires retrieving credential from Secure Element
- Tap NFC enabled phone on NFC enabled device
- Drives a mobile-centric, customer-centric user experience
Access Online Gov’t Services

Login Options

To use the online credential that you have with one of the institutions listed below, select the SecureKey Concierge Login button.

- BMO Financial
- Scotiabank
- TD Canada Trust

To use your Government of Canada Access Key credential, select the Access Key Login button.

If you do not have an Access Key and would like to obtain one, select Register

Return to Service Canada’s home page without logging in or registering for MSCA.

Exit
By selecting a Sign-In Partner, you are agreeing to the Terms and Conditions and Privacy Notice of SecureKey Concierge.

Switch My Sign-In Partner
Device as your UserID

- Hold the card flat against your computer's built-in card reader.
- Please tap your card to authorize this device.

- Hold your phone flat against your computer’s built-in card reader.
- Please tap your phone to authorize the device.
Enter your Passcode

Sign in to government services

Present your MyBank card using a SecureKey-enabled card reader.

Enter your MyBank password.

[Password Field]

Continue

Forgot Password

Privacy | Legal | About | Contact Us
Welcome, JOHN SMITH

Important information

- Your 2011 return was assessed and a refund of $9,901.49 was mailed to you on May 17, 2012.
  Summary of 2011 assessment

- NETFILE access code

- View your T4 and other tax slip information.
Secure Healthcare Applications

Identity Validation:

1. Patient Taps Card or Phone
2. Checks Credential is Valid

On-line Services:

1. Click to view health records
2. Prompt Patient to Tap Card or Phone
3. Done! Patient Access To Personal Health Records
Secure Healthcare Applications

• Allows for citizen access to health information when coupled with strong authentication

• Allows for healthcare provider access to records with citizen consent
Secure Banking Applications

### Current/Savings Accounts

- **View & Download Statements**
- **View Account Balance**
- **View Cheque Status**
- **Transfer Funds**

### Request

- **Request**
- **Account Statement**
- **Demand Draft**
- **Cheque Book**
- **Stop Payment of Cheque**
- **TDS Inquiry**
- **Hold Inquiry**

### My Account

<table>
<thead>
<tr>
<th>Account</th>
<th>A/C Number</th>
<th>Available Balance</th>
<th>Mini Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking</td>
<td>123-456001</td>
<td>$5800.00</td>
<td>View</td>
</tr>
<tr>
<td>Savings</td>
<td>345-678004</td>
<td>$9000.00</td>
<td>View</td>
</tr>
<tr>
<td>Tax A/C</td>
<td>134-567011</td>
<td>$3000.00</td>
<td>View</td>
</tr>
<tr>
<td>Investment</td>
<td>544-890190</td>
<td>$1200.00</td>
<td>View</td>
</tr>
</tbody>
</table>

**Total**: $23,000.00

**Note:**
The Available Balance displayed includes the credit balance and overdraft limit (if any) in your account. It excludes unclear Funds and Amounts marked for Holds.

Savings account customers can now receive their statements monthly, by email, free. To register - [Click Here]!

Register for your bills online [Click here] to know more.
Confirm Txn Online
Multi-Factor with NFC
Transfer Complete

Welcome: Evie Sun
Last Log In: Dec 03 2012 3:41 P.M. EST
Change Password | Contact Details

My Account | My Transfers | My Bill Payment | My Credit Cards | My Loans | My Funds

Current/Savings Accounts
View & Download Statements
View Account Balance
View Cheque Status
Transfer Funds

Transaction Completed
The funds have been successfully transferred.
The Reference Number: MB-893943

Shop with MyBank Points

Learn How to Invest Wisely
Securely Extend Online Services
NFC Forum Tag Use Cases and Security

- Jonathan Main
- NFC Forum Technical Committee, MasterCard
NFC Security

- NFC is a secure technology
  - Security standards are in place
  - Solutions providers and manufacturers can easily add application-appropriate security features
  - Many highly-effective mitigation measures available for tags
NFC Enables 3 Different Actions

**Card in a Phone**
Moves payment, event or ticketing information into a mobile phone
Store and redeem with a touch.
Get information back at the same time (coupons, receipts, warranties, loyalty points, etc)

**Reading Tags**
Enables mobile phones to read inexpensive tags that hold pertinent information
Examples include product comparisons, coupons, health care instructions, transit timetables

**Making Connections**
Enables devices to communicate with one another just by touching
Examples include connecting laptops and printers, sharing photos between a camera and TV, simple set up of Bluetooth and WiFi
Advertising

Tap the movie poster to see a film trailer and/or buy a theatre ticket

Source: Blue Bite
Ensuring Advertising Security

- **Potential vulnerability**
  - Tag information changed to direct user to a different (possibly malicious) web address

- **Mitigations**
  - Lock the tag – prevent overwriting
  - Physical controls to prevent replacement of the tag – e.g. display poster behind glass
In Aug. 2012, a top 5 consumer packaged food and beverage company piloted a shelf-talker with an embedded NFC tag

- Shoppers tapped their phones to access recipes, download an app or share on Facebook
- 36% of shoppers who tapped took an action
- Engagement with NFC was 12 times higher than QR codes
- Engagement time increased from 5 sec. to 48 sec.

Source: Mobile Commerce Daily
A major Australian supermarket chain

Tap your phone to the smart poster and receive:

- Free recipes from a celebrity chef
- Cookbook videos

Source: NFC World
Ensuring Retail Security

Potential vulnerabilities

- Modification of information
- Redirection to malicious web site

Mitigations

- Lock tags – prevent overwriting
- Design displays to prevent physical replacement of tags
- Sign tags – provide integrity of information using NFC Forum Signature RTD
- Mobile app may verify information source
Health Care

- Tags on prescription jars
- Provides usage/dosage information for consumers
Ensuring Health Care Security

- **Potential vulnerability**
  - Modification of prescription information

- **Mitigations**
  - Lock tags – prevent overwriting
  - Digitally sign tags using Signature RTD
  - Use an app to read tag information and verify signature and information source
  - Include (and check) patient identification information – prevent swapping of valid tags
NFC and Active Packaging

Commercial Uses

- Package tracking
- Content identification
- Temperature exposure log
- Authentication

Source: Kovio
Ensuring Active Packaging Security

Potential vulnerabilities
- Modification of data
- Moving tag to another bottle

Mitigations
- Active tags allow security at application level
- Include digital signatures on tag using Signature RTD
- Use tamper-evident labels with tags
# NFC Tag Security Landscape

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Attack</th>
<th>Mitigation</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data modification e.g. smart poster</td>
<td>Replace tag with another i.e. phishing attack</td>
<td>NFC Forum Signature RTD - Data integrity</td>
<td>Adds no cost to the tag</td>
</tr>
<tr>
<td>Eavesdropping e.g. medical history</td>
<td>Listen from a distance</td>
<td>Encrypt the tag contents or password protected URL</td>
<td>Adds no cost to the tag - Tag could have an encryption engine (cost)</td>
</tr>
<tr>
<td>Data corruption/replace ment e.g. any tag</td>
<td>Destroy the tag i.e. denial of service</td>
<td>Physical protection</td>
<td>Tag replacement can be detected using web analytics</td>
</tr>
<tr>
<td>Man in the middle e.g. ticketing</td>
<td>Intercept and modify data without parties knowing</td>
<td>Secure challenge-response and/or encryption engine</td>
<td>Tag must have a crypto engine e.g. ticketing</td>
</tr>
</tbody>
</table>
NFC Application Use Case:
Physical Access Control (PACS)

- Steve Rogers, CSCIP
- President
- IQ Devices
Traditional PACS Controlled Door
Includes Reader, Controller, Locking and Exit Devices

- Smart Card Reader
- Smart Card
- Door Control Panel
- Power
- Request to Exit (REX)
- Electric Strike
- Door Contact
- LAN / WAN Ethernet TCP/IP Network

Traditional PACS Components
Traditional PACS Credential

ISO14443 Smart Card – Student ID

- Small, Rugged, Reliable
- Familiar, Easy-to-Carry Form Factor
- Identity & Identifiers Stored Securely
- High Resistance to Use by Non-Owner
- High Resistance to Alteration, Forgery, Duplication (Authenticators)
- Inexpensive, Well Standardized
- No Battery or Internal Power Requirement
- Easily Lost or Stolen
Secure NFC Credential

NFC Technology in Smart Phones, Offers New Possibilities:

- Interoperability With ISO14443 Standards-Based Credentials
- Secure Elements, UICC, SAM, TEE Support Access Rules
- Keyboard, PIN & Biometric Verification, Screen, Power, Enable Strong Binding
- Users Control Release of Information, Specific Access Privileges & Authorization, Rules for Each Function
- Reader & Credential Communication Security, Strong Authentication
- OTA Provisioning, Just-in-Time Credentials (e.g. Visitors)
- Access Cloud Identity Infrastructure
NFC Smart Phone Security

- Device Integrity Self Check, App and Hardware Image
- Isolation of Stored Data
- Protected Storage and De-Provisioning
- OTA SAM Management
- If Smart Phone Lost or Stolen:
  - Issue Temp Key to Alternate
  - Wipe Phone
  - Remove PACS Privilege
NFC PACS Pilot Details
November 2011 - Present

Phase 1
- 30 Students & 12 Staff
- 6 dorms, office, etc.

Phase 2
- Over 100 students and staff
- 2 major residence halls 80 AD Locks
  - 4 people per room, 201 residents
- Ecosystem expanded substantially
  - Vending, Point of Sale, Laundry, PACS

Phase 1
- Access Control & Laundry
- 12 main doors, 3 elevators w/ floor control

Phase 2
- Explore alternate student demographics & feedback
- Executive MBA graduate students at Branch Campus
NFC PACS Pilots

Use your phone as your key!

Physical Access

- Laundry
- Vending Machines
- Bookstores
- College meal programs
Campus Pilot Results

- 70%-80% = Student Physical Keys & Student Access Cards Lost or Stolen
- 91% of Students Said Ease-of-Use or Convenience Was The Best Part of NFC.
- Over 70% Preferred Using Smart Phone to Enter Buildings Over Using Their Student ID (Smart Card).
- 100% of Students Surveyed Would Be Interested in Owning NFC Technology Built Into Their Own Smart Phone…BYOD
Relative Importance of Benefits

Student Survey Data

- More Convenient/ Easy to Use: 43
- Faster: 15
- Less Likely to Lose/Break: 14
- Innovative Technology: 11
- More Secure: 6
- Easy to Replace: 6
- Reduces Environmental Waste: 5
A “Frictionless” Solution Requires the Balance of Convenience & Security

Convenience:
- Always On - Tap and Go
- Activation Key - Shortcut
- No Battery = No Problem - Inductive

Security:
- PIN or BIO to activate SE
- Smart Phone Challenge the Reader
- Mutual Authentication Support
Most common student quote:

- “I sometimes forget my keys, my ID, my watch, my wallet…

  **but I NEVER forget my phone**”
NFC
Revolutionize PACS Topology?

Physical Access

Mobile network

Gateway

PACS Metadata and Provisioning

Lock Control
Alarm Input control

IP I/O device
NFC Industry Trends & Growth Drivers

- NFC-based mobile transactions are expected to reach nearly $50 billion worldwide by 2014.
  - Juniper Research

- Expected 46% of all mobile smart phones will be NFC enabled by 2016.
  – Market Research
Questions & Answers
Mobile & NFC Webinar Series Recordings

- Anatomy of a Mobile Device: Security Architecture and Secure Provisioning
- Mobile/NFC Security Fundamentals: Secure Elements 101
- Mobile/NFC Security Fundamentals: NFC Forum Tags and Security Considerations

Available at:

Smart Card Alliance
191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556-6828
www.smartcardalliance.org

• Randy Vanderhoof, rvanderhoof@smartcardalliance.org
• Tony Sabetti, tony.sabetti@paywithisis.com
• Christian Ali, christian.ali@securekey.com
• Jonathan Main, jonathan_main@mastercard.com
• Steve Rogers, steve.rogers@iqdevices.com