Over-the-Internet
User-Centric Content Management for Secure Elements in Mobile Devices

Mohamed Sabt\textsuperscript{1,3}  Mohammed Achemlal\textsuperscript{1,2}
Abdelmadjid Bouabdallah\textsuperscript{3}

\textsuperscript{1}Orange Labs, France
\textsuperscript{2}Greyc EnsiCaen, France
\textsuperscript{3}Sorbonne universités, UTC, France

MobiSecServ, February 2015
Introduction

- Smart objects
- Smart Secure Elements
Outline

1 Introduction
   - Smart objects
   - Smart Secure Elements

2 Over-the-Internet
   - Goals
   - Architecture
Outline

1. Introduction
   - Smart objects
   - Smart Secure Elements

2. Over-the-Internet
   - Goals
   - Architecture

3. Implementation and Evaluation
   - Implementation
   - Evaluation
   - Perspectives
Outline

1 Introduction
   - Smart objects
     - Smart Secure Elements

2 Over-the-Internet
   - Goals
   - Architecture

3 Implementation and Evaluation
   - Implementation
   - Evaluation
   - Perspectives
Smartphones
What makes them smart?

Nokia N900

iPhone 1
The *iPhone* Effect

**Description**

Users can easily personalize their devices with third-party applications, and service providers can easily make their applications available to end users.

**Smartness**

*smartness* is not measured by features, it is about application management.
Secure Element

**Definition**

A secure element (SE) is a tamper-resistant smart card chip capable of running applications (called applets or cardlets) with a high level of security.

There are 3 form-factors of SE:
- Embedded smart card;
- SD card;
- SIM/UICC.
Secure Element

Definition

A secure element (SE) is a tamper-resistant smart card chip capable of running applications (called applets or cardlets) with a high level of security.

There are 3 form-factors of SE:

- Embedded smart card;
- SD card;
- SIM/UICC.
The NFC Ecosystem

Ticketing

Loyalty membership

Transport

Contactless payment

NFC

UI App

M.Sabt et al. (Orange Labs)
The management of NFC applications

The unsolved problem

NFC services consist of two applications:

1. Applet: installed on the SE;
2. UI app: installed on the smartphone.

Management Problems

- The content management of SE is controlled by the SE owner;
- Current platforms in charge of content management are not adapted to install NFC applets;
- The life-cycles of applet and UI app are independent.
Outline

1. Introduction
   - Smart objects
   - Smart Secure Elements

2. Over-the-Internet
   - Goals
   - Architecture

3. Implementation and Evaluation
   - Implementation
   - Evaluation
   - Perspectives
Design objectives

Problem Statement
Our goal is to design a content management system for NFC enabled services that overcome the shortcomings of the current systems.
Design objectives

Problem Statement
Our goal is to design a content management system for NFC enabled services that overcome the shortcomings of the current systems.

Design requirements
1. **Deployable**: deployability depends on the induced cost and compatibility with industry standards;
2. **Remote and efficient**: appropriate wireless technology;
3. **Secure**: only authenticated contents are allowed;
4. **Tied life-cycle**: applet and UI app are managed together.
Outline

1. Introduction
   - Smart objects
   - Smart Secure Elements

2. Over-the-Internet
   - Goals
   - Architecture

3. Implementation and Evaluation
   - Implementation
   - Evaluation
   - Perspectives
Workflow of installation

1. Users ask for a particular NFC service;
Installation Process

Workflow of installation

1. Users ask for a particular NFC service;
2. Once installed, the UI app contacts the service provider to install the applet;
Workflow of installation

1. Users ask for a particular NFC service;
2. Once installed, the UI app contacts the service provider to install the applet;
3. The service provider creates a private space in the SE;
Installation Process

Workflow of installation

1. Users ask for a particular NFC service;
2. Once installed, the UI app contacts the service provider to install the applet;
3. The service provider creates a private space in the SE;
4. The service provider sets up a secure communication channel with the SE;
Installation Process

Workflow of installation

1. Users ask for a particular NFC service;
2. Once installed, the UI app contacts the service provider to install the applet;
3. The service provider creates a private space in the SE;
4. The service provider sets up a secure communication channel with the SE;
5. The applet is sent and installed on the SE.
Overview of the OTI architecture
Some technical details

Private Space in SE

- We leverage the concept of Security Domain defined by GlobalPlatform.
- A Security Domain (SD) is created using the radio interface.
- Once created, the service providers get the secret keys that allow them to set up a secure connection with the corresponding SD.

Wireless technology

- We leverage Internet connection to communicate with SE.
- SEs are not directly connected to the Internet.
- A bridge application is required to send the APDUs encapsulated into IP packets to the SE.
Secure Channel Protocol

- Commands Generator
- SCP
- Transport Layer

- Management commands/responses

- Secure connection

- SE Manager
- SE Driver

- Card Manager
- Security Domain
- OPEN

Service Provider

Mobile Device

Secure Element
Updating Process

Workflow of updating

1. The service provider hosts a database containing, for each SE, the version of the installed applet.
Updating Process

Workflow of updating

1. The service provider hosts a database containing, for each SE, the version of the installed applet.
2. Once an update required, the service provider sends a PUSH message to the corresponding mobile device.
Over-the-Internet Architecture

Updating Process

Workflow of updating

1. The service provider hosts a database containing, for each SE, the version of the installed applet.

2. Once an update required, the service provider sends a PUSH message to the corresponding mobile device.

3. The mobile device downloads the new UI app, installs the applet and then installs the UI.
Updating Process

Workflow of updating

1. The service provider hosts a database containing, for each SE, the version of the installed applet.
2. Once an update required, the service provider sends a PUSH message to the corresponding mobile device.
3. The mobile device downloads the new UI app, installs the applet and then installs the UI.
4. At the end, the SE sends a cryptographic ACK to the service provider in order to update its database.
Outline

1. Introduction
   - Smart objects
   - Smart Secure Elements

2. Over-the-Internet
   - Goals
   - Architecture

3. Implementation and Evaluation
   - Implementation
   - Evaluation
   - Perspectives
Implementation

- Samsung Galaxy SII with Android 4.0.3 (ICS) and containing the SmartCard API library;
Implementation

- Samsung Galaxy SII with Android 4.0.3 (ICS) and containing the SmartCard API library;
- Oberthur UICC JavaCard 2.2.2;
Implementation

- Samsung Galaxy SII with Android 4.0.3 (ICS) and containing the SmartCard API library;
- Oberthur UICC JavaCard 2.2.2;
- Android webview, HTML5 and CCS3;
Implementation

- Samsung Galaxy SII with Android 4.0.3 (ICS) and containing the SmartCard API library;
- Oberthur UICC JavaCard 2.2.2;
- Android webview, HTML5 and CCS3;
- SE API implemented in JavaScript (Ajase);
Implementation

- Samsung Galaxy SII with Android 4.0.3 (ICS) and containing the SmartCard API library;
- Oberthur UICC JavaCard 2.2.2;
- Android webview, HTML5 and CCS3;
- SE API implemented in JavaScript (Ajase);
- GlobalPlatform card specification 2.2.1 implemented in Java 7;
Implementation

- Samsung Galaxy SII with Android 4.0.3 (ICS) and containing the SmartCard API library;
- Oberthur UICC JavaCard 2.2.2;
- Android webview, HTML5 and CCS3;
- SE API implemented in JavaScript (Ajase);
- GlobalPlatform card specification 2.2.1 implemented in Java 7;
- Orange OTA platform.
Outline

1. Introduction
   - Smart objects
   - Smart Secure Elements

2. Over-the-Internet
   - Goals
   - Architecture

3. Implementation and Evaluation
   - Implementation
   - Evaluation
   - Perspectives
**Evaluation**

<table>
<thead>
<tr>
<th>Content Management Platform</th>
<th>Average of Download Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTW (Over-the-Wire)</td>
<td>18.2 seconds</td>
</tr>
<tr>
<td>OTI (Over-the-Internet)</td>
<td>25.7 seconds</td>
</tr>
<tr>
<td>OTA (Over-the-Air)</td>
<td>5.42 minutes</td>
</tr>
</tbody>
</table>

Comparison of download time of 9-kilobyte-JavaCard applet
Outline

1. Introduction
   - Smart objects
   - Smart Secure Elements

2. Over-the-Internet
   - Goals
   - Architecture

3. Implementation and Evaluation
   - Implementation
   - Evaluation
   - Perspectives
More thorough evaluation of the OTI platform (i.e. comparison with BIP);
Perspectives

- More thorough evaluation of the OTI platform (i.e. comparison with BIP);
- Integrating users’ permission in the process of creating security domains.
Summary

- The most difficult problem in the NFC ecosystem is not security, but applications management;
- OTI is an efficient management system for secure element based NFC applications in mobile devices;
- OTI does not trade off deployability and security;
- OTI is faster and more reliable than SMS-based OTA platforms.
Thank you for your attention!