Leveraging Object Linking and Embedding for Processes Control Unified Architecture Standards with Smart Card Technology for Secure Applications and Services

Yuankui Wang (Matr.-Nr.: 6670785)

University of Paderborn wangyk@mail.upb.de

Abstract. Object Linking and Embedding for Process Control Unified Architecture, known as OPC UA is the recent released industry standard from OPC Foundation, which compared with his predecessors is equipped with a list of charming new features, with whose help OPC UA is capable of developing a common communication interface for devices which participate in automation system. Meanwhile, the technology of smart card is widely used in information security fields of finance, communication, personal and government identification, payment. Therefore it is meaningful and promising to develop OPC UA standard compliant application on embedded smart card secure device, for the purpose of secure remote control, enterprise resource planning and etc. Since the storage and compute capacity of chip card is limited, OPC UA product will consist of two essential parts, namely client/server application code, realized as Android or other application, and communication stack, realized as Javacard Applet based on Remote Application Management from GlobalPlatform. The implemented demonstration scenarios and corresponding analysis show the possibility of developing OPC UA standard compliant application on devices embedded with smart card to benefit customers.

1 Introduction and Motivation

According to the *Mobile Economy 2013* from *Global System for Mobile Communications Association*, at the end of year 2013 there are over 3.2 billion mobile subscribers in total, which means one half the population of the earth now enjoy the social and economic convenience brought by mobile technology. Moreover by 2017 700 million new subscribers are expected to be added. And the number of mobile subscriber will reach 4 billion in 2018. Mobil technology opens nowadays a promising market.

Mobile products play an irreplaceable role at the heart of our daily life. With the help of mobile technology, the user's world in many domains such as, education, financial transactions, health and etc. are inter-connected. Mobile users are enjoying the advantages of mobility. Services, like 24/7 monitored home security, full control about the management of home humidity and temperature, exist not only in science fiction film but also could be realized by today's technology.

At the same time, mobility in industry and business world is also a critical assert, which can not only increase efficiency and productivity but also drive new revenue generation and competitive advantage. The most convicting example here is Machine to Machine communication, that is also referred as M2M technology. In M2M communication, machines which are usually embedded with smart cards exchange gathered date with each other to accomplish common task using wireless or wire networks. M2M technology is widely employed in different industry spheres such as factory automation, remote access control and sensor monitoring. It boosts the efficiency of corresponding processes, offers centralized service support and date management, minimizes system response time.

But in order to enjoy the aforementioned features, two tough issues must be resolved. First, how to achieve a common interface for the devices that participate in the system. And second how to guarantee system security under different communication environments with variant date complexity.

2 Contents

In this master thesis, I am going to address solutions for questions mentioned in section *Introduction and Motivation* and design a smart home system for the purpose of demonstration. In this smart home system, home owner using smart phone is capable of experiencing 24/7 home security service, remotely managing inner home environment parameters and assigning access permissions. This system consists of smart phones with Universal Integrated Circuit Cards (UICC smart card), digital door locks, electronic home devices (such as coffee machine, air conditioner), environment sensors. Moreover each above mentioned device is equipped with smart card, which acts not only as secure token, that saves user credentials, but also is in charge of construction and management of the communications with other devices.

In particular, I will introduce the newly released industry automation standards object linking and embedding for processes control unified architecture(OPC UA standards) to build a application level communication interface for devices that are mentioned above and design communication stack for OPC UA standards on UICC smart card., whose duties are: creation and management communi-

cation between OPC client/server application, entity authentication and secure messaging.

3 Implementation Resources

The communication stack is developed as UICC applet, the UICC is a Java Card, which contains OS from Morpho. This OS is built based on JavaCard 2.2.2 and GlobalPlatform.

As develop and test IDE, Jacade (Java Applet Development Environment IDE) from Morpho is used.

For OPC UA client application, the Android Platform is chosen.

Devices which participate in demonstration scenario are simulated by computer with MCR CardReader from Morpho.

4 Objectives

- Introduce foundation technologies
- Review and compare potential solutions
- Summary of the advantages offered by OPC UA standards
- Summary of the benefits of UICC smart cards, protocol and applications
- Develop OPC UA communication stack as UICC Applet on smart card
- Design basic OPC UA server application for the purpose of demonstration
- Design android App as OPC UA client application at the smart phone user side
- Simulate OTA server that realizes communication between smart cards
- Use aforementioned components to build a simulation system for Smart Home
- Analyze the stability and performance of demonstration system
- With help of Attack-Tree-graph, analyze potential attacks and propose appropriate countermeasures

5 Table of Contents

6 Time plan

The master thesis would be registered before 31.06.2014 and expected finished around Decebmer 2014.

– State-of-the-Art and literature review	15.06.2014 to 25.06.2014
– Software architecture design	25.06.2014 to 30.06.2014
– Design communication stack on UICC card	01.07.2014 to 25.07.2014
– OPC UA client/server prototype	25.07.2014 to 15.08.2014
– Integration and test	15.08.2014 to 10.09.2014
– System performance analysis	10.09.2014 to 30.09.2014
– Potential attacks and countermeasures	30.09.2014 to 25.10.2014
– Final thesis	25.10.2014 to 15.11.2014

7 Literature

Eckert, C:IT-Sicherheit (2008)

Wolfgang, R and Wolfgang, E: Handbuch der chipkarten (2008)

OPC Foundation: Opc unified architecture specification part2 security model 1.01.(February 6.2009)

OPC Foundation: Opc unified architecture specification part3 address space model 1.01. (February 6.2009)

OPC Foundation: Opc unified architecture specification part4 services 1.01.(February 6.2009)

OPC Foundation: Opc unified architecture specification part6 mappings 1.01.(February 6.2009)