Intelligent Computing Technology and Automation
Z. Hou (Ed.)

doi:10.3233/ATDE231215

Remote Management Method of IoT Based on ESIM Card

Hui ZHANG[1], Hui SHI, Yanan ZHANG
Beijing Fibrlink Communications Co., LTD., Beijing, 100071, China

Abstract. In order to meet the high requirements of existing IoT for security assurance and remote configuration management mechanisms, the key technologies and applications of embedded SIM cards in the IoT field are studied. We focus on the business operation mode and supervision direction under the embedded deployment mode, integrated with the embedded SIM card and the near-field communication function, to analyze different solutions for contract management. Then it focuses on the identity authentication function of embedded SIM card technology, the function of supporting the IoTs and the function of local services, and provides the implementation method of the corresponding functional modules. Finally, by establishing an EAPserver experimental environment, testing the system functions, and simply testing the key service processes, it is proved that the scheme is feasible, new and effective..

Keywords. IoT; eSIM; EAP; remote management; authentication

1. Introduction

In recent years, the Internet of Things technology (IoT) has gradually matured, and it has made achievements in the economic field as well as the scientific and technological field. The Internet of Things is developing rapidly, so there emerges a lot of business opportunities. With the development of Internet of Things technology, embedded SIM card has become more and more important. For example, for the power industry, the environment is relatively harsh, so the SIM card should have a good anti-interference ability. With the continuous deepening of the Internet of Things technology and the continuous expansion of the application field, embedded SIM cards have been used more and more. At present, many operators begin to try the integration of embedded SIM cards, which is considered as a new breakthrough point of the Internet of Things technology, and more and more related research [1]. When building the Internet of Things, the purpose is to achieve mutual control and interconnection between end devices. Installing the embedded SIM card in the terminal can improve the ability of the device to cope with harsh and complex environments, thus improving the accuracy and stability of the data exchanged by the Internet of Things. Due to the use of intelligent management and distributed configuration in the perception layer of the Internet of Things, the device can realize automatic operation while having the functions of data encryption and identity authentication [2].

This paper first introduces the definition, technical characteristics and physical indicators of embedded SIM card, and its application status in the management of the Internet of Things. Then, according to the requirements of ESIM in the authentication environment, a remote management platform architecture based on UICC is proposed.

[1]Corresponding Author: Hui Zhang; Beijing Fibrlink Communications Co., LTD., Beijing, 100071, China; zhanghui1fzchb@163.com

For the key modules in the system, such as contract management, security certification and process design, we give specific implementation methods. It also makes use of the introduction of SoftSIM and 802.1x technologies to solve the WiFi access authentication problem. Finally, the feasibility and effectiveness of the scheme in the Internet of Things are verified in a multi AP scenario by building an actual environment. The test results show that this method can help wireless terminals make better access decisions, and it also has better security in remote management.

2. Features and Principles of Embedded SIM Card Technology

2.1 Embedded SIM Card Technology

Embedded SIM card is an integral part of the business system of the Internet of Things. It is located in the network terminal equipment layer and forms the user equipment of the Internet of Things together with the Internet of Things communication terminals to provide services for Internet of Things users to access mobile networks and provide services through the Internet of Things business. The functions supported by embedded SIM are mainly [3]:

1) Provide identity authentication. As the user equipment identity authentication and authentication module, it provides the identity identification of the user equipment accessing the wireless network to complete the security authentication of network access.

2) Provide application support. Load some user equipment applications to meet the business requirements of IoT business monitoring, positioning, command and scheduling, data collection and measurement.

3) Security mechanism guarantee. The smart card security guarantee capability is used to provide security mechanisms for user network access, business access, data transmission, information storage and other functions.

4) Provide local network services. As a network node, it connects with other local user equipment to form a wireless LAN or personal area network to meet local communication requirements and provide corresponding services.

Considering the special requirements of embedded SIM card in the business environment of the Internet of Things, the smart card of the Internet of Things has put forward new requirements in the three-tier system of the Internet of Things. Therefore, with the further improvement of embedded SIM card technology, it has obvious advantages in life cycle, reliability and other aspects, and is more suitable for the IoT business, showing a good market prospect.

2.2 Function and Physical Characteristics of Embedded SIM Card

(1) Identity authentication

The embedded SIM card is still a communication user identification module, which provides the identity and security authentication of the user equipment accessing the wireless network. In the need of accurate and intelligent identification and subsequent control among the massive sensor devices of the Internet of Things, it is necessary to carry out accurate, intelligent, unified and open identity/device identification for sensor devices connected to the Internet of Things system. The characteristics of the identification module of the embedded SIM card itself can

provide the identity authentication function in a large number of terminal devices [4].

(2) Security mechanism guarantee

As the sensing layer devices of the Internet of Things adopt a distributed configuration mode and intelligent management mode, the sensing layer devices will run in an unattended mode, which brings about the need for strict and unified security control of the sensing layer devices of the Internet of Things, which can be flexibly configured for different industries and fields, including identity authentication protocols, data encryption and decryption algorithms, key storage and protection, and many other links.

(3) IoT application support

Loading an embedded SIM card can meet the complex and harsh environment in terms of physical indicators, thus ensuring the stability of IoT applications when using mobile communication networks to complete data interaction and real-time control

(4) Management mode

To adapt to the application of the Internet of Things, the embedded SIM card is issued by using the on-site card writing method, that is, the embedded SIM card does not preset the mobile phone number after leaving the factory. After the integrated welding with the Internet of Things device, the mobile phone number is written and opened on site when the device is sold or installed.

2.3 Business Process Management of Embedded SIM

From the perspective of terminal, embedded SIM card has realized a new operation mode of "integration of machine and card, separation of card industry". From the business perspective, embedded SIM implements a flexible business management process, including initialization, business migration, business change, business termination, etc. These processes are completed through SM-DP and SM-SR. As shown in figure 1, the user's business data is stored in the SM-DP platform, and these data are transmitted to the SM-DP platform by the operator (MNO) for generation. This process is called Profile Ordering; After that, users can download and change business data from SM-DP platform through SM-SR as required. Such process is called signing data download and installation [5].

Figure 1. Data signing logic of eSIM card

3. IOT Remote Management System Design Based on eSIM

3.1 eSIM Remote Management Platform Architecture

Embedded SIM card is not only a new form of general integrated circuit card, it involves the improvement of a complete set of remote management platforms, but also increases the complexity of the operator's internal customer management, customer

service and internal settlement. Among them, user signing management is one of the most critical functions. Subscription Manager (SM) refers to the subscription management of users involved in using embedded SIM devices, as depicted in figure 2. Embedded SIM card signing management means breaking through the traditional UICC linear irreversible process management controlled by operators. The life cycle is redefined, and operators can still be selected after issuance. The realization of SM function will accelerate the development of IoT business, help to build a trusted, sustainable and fair industrial chain and ecosystem, help to build a reliable user contract management model, and protect the security of operators' user data [6].

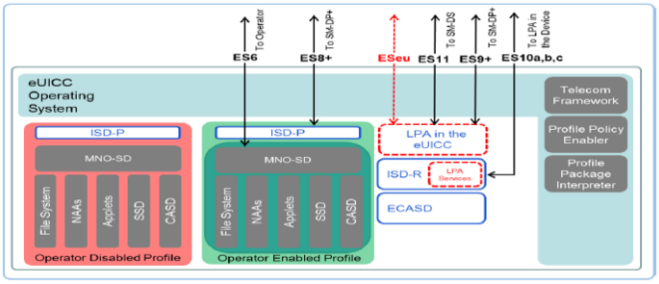

Figure 2. Implementation process of eSIM card in remote management

3.2 eSIM Card Signing Management

The logical structure of the SIM card The files in the SIM card are stored in a hierarchical structure. There are mainly three types: MF (Master File), DF (Dedicated File), EF (Elementary File). The software system in the SIM card is responsible for handling the access and write in of the file data The network architecture schematic model of eSIM is shown in figure 3.

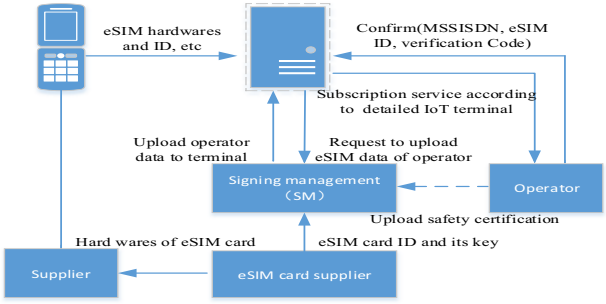

Figure 3. SM deployed network architecture.

It can be seen that SM deployment mainly involves the following logical entities: operators, contract management, embedded SIM card suppliers, and equipment suppliers. Signing management is at the core of network architecture; The remote management of eSIM is mainly realized through the user signing management platform. The network switching request of eSIM is sent to the signing management platform, and then the platform transmits the instructions to the corresponding operators. In addition, SM also completes the process of operator data change and embedded SIM

card replacement.

3.3 Security Certification under WiFi

(1) Principle process

The information of SoftSIM can cut off the connection between users and operators. Instead, terminal providers sell communication services to users. Considering the scenario of mobile terminals accessing the operation level WiFi, the EAP authentication method of 802.1X protocol is adopted to realize the specific access mechanism. The preparation is to migrate hostapd and wpa. When supporting, it is necessary to port openssl and libnl first. We can refer to openssl to ARM Linux and libnl to ARM Linux. EAPOL state machine is implemented as a separate module to interact with EAP peers. One set of wireless modules uses cloud card as the main module to provide operator network access services for WiFi; The other set of wireless modules uses the physical sim card or the built-in SoftSIM card as the auxiliary module

(2) eSIM/SoftSIM module

During the complete authentication process, the EAPpeer state machine interacts with the EAP/SoftSIM module twice. Softsim transparently transmits the received EAP request and AKA 'challenge to the UE, and sends the 5G keyset identifier ngKSI and the anti-aliasing ABBA parameter between architectures to the UE. These two parameters are generated by SEAF (for ngKSI and ABBA parameters, the former is used to create a local security context after successful authentication, and the latter is a version specific security feature indicator to prevent confusion). The EAP authentication framework determines the security of IEEE802.1X authentication. The key of EAP authentication framework is the selection of EAP authentication methods Each access authentication in this mode requires an interactive certificate to verify the identity. The specific description of such process is shown in figure 4.

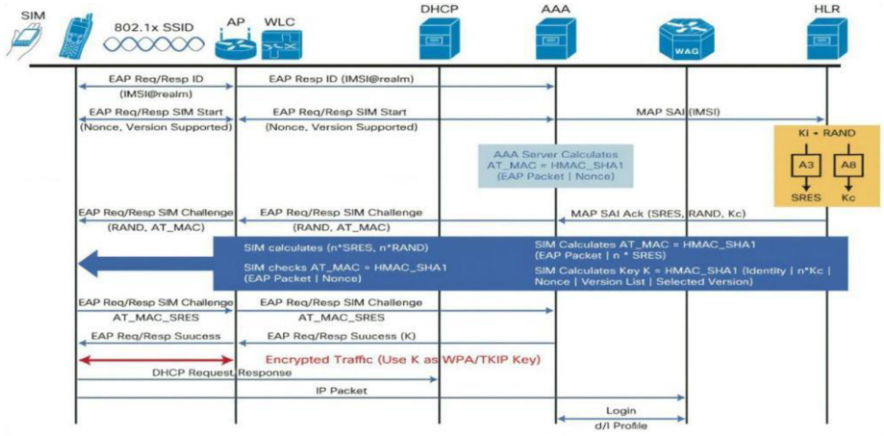

Figure 4. SM deployed network architecture

(3) Implementation of authentication algorithm

In the process of EAP authentication interaction based on eSIM/SoftSIM, the authentication server needs to obtain authentication triplets from the HLR module for subsequent authentication. The VLR needs to query relevant parameters from the user's

HLR, assign a new roaming number (MSRN) to the user, and notify the HLR to modify the user's location information, so as to provide routing information for other users when calling the mobile user [7]. The requester replies EAP Response/Identity message to the authenticator, and the authenticator forwards it to the authentication server. The requester and the authentication server can also communicate using the Radius protocol carried by UDP. Part of the key codes of this process is depicted as follows:

```
scard_get_imsi()
        |-->scard_select_file()
                |-->_scard_select_file()
                        |-->scard_transmit()
                                |-->SCardTransmit()
                                        |-->(1)socket_local_client()-->open socket and connect
                                        |       |-->socket()
                                        |       |-->socket_local_client_connect()
                                        |               |-->connect()
                                        |-->(2)send()
                                        |-->(3)select()
...
```

4. System Test and Analysis

Under the system architecture, in order to realize the remote activation, configuration switching and other mechanisms for eSIM, and with the help of the functions of the above logical entities, a deployment architecture as shown in figure 5 can be established. In this implementation scheme, configuration creation during the user's remote activation process, configuration customization, download and installation during the operator's switching, as well as business reservation and other functions can be realized [8]. In this figure, when the configuration file is created, MNO sends it to SM-DP to generate the general basic configuration in the currently widely used format of word, excel, pdf or xml; In the case of exclusive customization, MNO outputs customized data in combination with user's IMSI, TMSI and other identification information, and finally sends them to the eSIM through SM-SR for installation and activation.

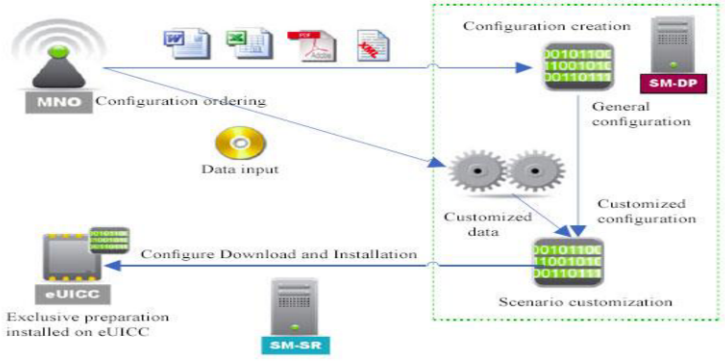

Figure 5. An instance of eSIM configuration management and deployment

On the basis of the completion of the functional test of the key service processes of the WiFi network, this section has simply tested its performance. Run hostapd-2.7 as a network access point; Multiple users share the same authentication server. The central processor of the computer is divided into small time periods. Each time period is called a time. Different terminals are used to send authentication requests to the network at the same time for the performance comparison of authentication methods under the key service flow of the network, as shown in figure 6.

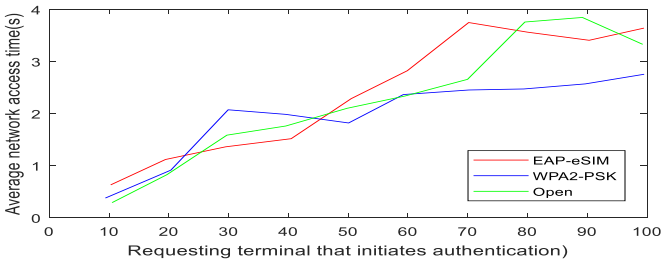

Figure 6. Comparison of average connection time of devices with three different authentication methods

It can be seen that when the authentication request scale increases from 100 to 1000, the average access time of the three non authentication protocols to the SIM card changes. It can be seen from the figure that the more times a channel may backoff in the same time period, the more time it takes to backoff due to competing channels. The eSIM and WPA2-PSK authentication methods will not consume additional performance due to the use of a large amount of link information, and both are within the tolerable range. However, the performance of the traditional Open algorithm has declined significantly. In addition, the EAP eSIM mechanism shows excellent robustness because of its better visa management.

5. Conclusion

As the latest application form of user identification in mobile communication systems, eSIM cards have put forward higher requirements for security assurance and remote configuration management mechanisms, and are now widely used in the Internet of Things and other fields. For embedded SIM card, its implementation mechanism and technical classification are introduced at first; it analyzes the current situation of domestic and international standard formulation; Then the classification of eSIM application scenarios is discussed, and the specific IoT remote management configuration process is given. Finally, the functions of each logical entity of the management system in the authentication environment are studied, and a reference scheme for the implementation of security deployment based on SoftSIM is provided, and its usability is proved through system testing.

Acknowledgments

This work was supported by Beijing Fibrlink Communications Co., LTD. "Research on key technologies of cross-platform SDN network management and communication module for power communication autonomous driving network ", under grant no. 52680021N019.

References

[1] Zang Nanqi, Wang Jiahan. The application analysis of embedded SIM card technology in the Internet of Things, Digital Communication World, 2019, 2:35
[2] Liu Liang. Explore the application of embedded SIM card technology and the Internet of Things, Information communication, 2018, 1: 174-175
[3] Yao Haipeng, Zhang Zhijiang, Liu Yunjie. Research on Embedded SIM Card Technology of Internet of Things. Information Communication Technology, 2012, 5: 52-55
[4] Zhang Bing, Liu Qian. Discussion on Embedded SIM Card Technology and Its Application to Internet of Things. Posts and Telecommunications Design Technology, 2011, 7: 30-34
[5] Huang Yaojun, Nie Yongxia, Tang Juanjuan. The embedded SIM and key issue of applying in Internet of things. Telecommunication Engineering Technology and Standardization, 2016, 2: 31-34
[6] Zhu Yan, Zhu Hongye, Zheng Haixia. Research on key technologies and domestic and foreign standards of embedded SIM card. Telecommunication network technology, 2014, 6: 57-60
[7] Praveena M, Christy A, Helen L S, et al. Smart Car based on IOT. Journal of Physics: Conference Series, 2021, 1770(1):12-21.
[8] Wei, Zhou Yu and Sun Xiangqian. Research on embedded SIM card standardization process and remote management technology. Mobile Communication, 2014, 38(9): 42-47