Design and technical verification of a new type of subscriber identity module card for internet of vehicles

Yimeng Li¹,a*, Xiaoming Ren¹,b, Zuhui Yue¹,c, Hui Liu²,d, Lanhai Ding³,e

¹China Mobile Research Institute, Beijing, 100053, China
²China Mobile Research Institute, Beijing, 100053, China
³China Mobile Research Institute, Beijing, 100053, China

a*e-mail: liyimengyjy@chinamobile.com, b*e-mail: renxiaoming@chinamobile.com,
c*e-mail: yuezuhui@chinamobile.com, d*e-mail: liuhuiyjy@chinamobile.com,
e*e-mail: dinglanhai@chinamobile.com

*Corresponding author’s e-mail: liyimengyjy@chinamobile.com

Abstract. The Internet of Vehicles communication security aims to solve the V2X communication security problems under several scenarios, including direct communication and communication based on cellular network, and provides guaranteed communication security for the achievement of business goals such as vehicle-road information collaboration and road safety. Currently, V2X communication security mostly adopts digital certificate technical proposal based on public key infrastructure and is implemented through the HSM security module. However, this solution requires to preset security data such as digital certificate in the HSM module of the vehicle terminal, which has high demands on the production line of the enterprise, the difficulty is predictable. This paper designs a new type of SIM card for Internet of Vehicles based on high performance chip, which can implement the writing and updating operation of security parameters (certificates, keys, etc.) online, which can reduce the requirements for the transformation of the production line of car companies and at the same time, the security of data management is also improved. The validation result indicates that the new SIM card can realize functions such as login authentication, certificate download, signature verification, etc., and its performance meets the requirements of V2X secure communication.

1. Introduction

V2X technology uses real-time data from perception and collaboration among vehicles, roads, people, and clouds to realize the integration of intelligent traffic management, intelligent dynamic information services and vehicle intelligent control, thereby it can provide users with road safety, efficient transportation and entertainment, meets the needs of people's traffic information consumption.

While V2X technology implements vehicle networking, the information of vehicles and people will be directly exposed to the network. This gives new requirements and challenges for safely applying V2X, including the identification of various vehicles and cloud platforms, the authenticity of broadcast messages from vehicles or road test equipments, the protection of vehicle and personal privacy data, vehicle driving data, high-precision positioning data, etc.

In order to meet the security requirements of V2X application and realize the security of IoV communication, the system needs to ensure the source authentication, authorization verification,
integrity, replay resistance, privacy of the message, protect the privacy of user identification and location information, and fulfill other safety requirements on the communication interface of the vehicle-mounted terminal.

Currently, digital certificate technology based on public key infrastructure is mostly used at home and abroad to protect V2X messages through digital signature/verification methods on application layer.

2. Analysis of existing schemes
The realization of the current Internet of Vehicles security is mainly based on the hardware security module HSM. The HSM can store security parameters (private keys or digital certificates, etc.) while also having the basic conditions for performing security authentication, signature/verification calculations, and encryption and decryption processing. The performance of HSM is decent, but in order to realize these functions, it is necessary to configure the relevant sensitive parameters in a safe manner before the OBU or RSU equipment is used, so that each device can have its own characteristics.

At present, this process is implemented by offline-preset methods on the production line. The entire process has strict safety requirements on the production line's production environment and management process. For this reason, companies need to invest more cost and time to meet those requirements, including the transformation of production lines and production processes, as well as ensuring the safety of the system in the operation and maintenance phase, which will bring greater challenges and technical difficulties to them, and to a certain extent, restricts the rapid development of the Internet of Vehicles industry.

Therefore, there is an urgent need for a more flexible way to realize the writing and updating of sensitive parameters, which can greatly reduce management costs and optimize management capabilities. The new type of SIM card for the Internet of Vehicles is proposed based on the above requirements.

Therefore, if the existing safety infrastructure of the vehicle can be used to write and update the safety parameters, then for car companies, it can greatly reduce their management cost and difficulty. The new type of SIM card for the Internet of Vehicles is proposed based on the above requirements.

3. Design and technical verification of new type SIM card

3.1. New Type SIM card
The SIM card allows subscribers to use their mobile devices to receive calls, send SMS messages, or connect to mobile internet services. And this is also true in traditional vehicles. However, with the development of the Internet of Vehicles V2X technology, the SIM card can be used as the core security carrier on the device. It can store security sensitive parameters and at the same time, it can also support richer functions to provide a full range of security services for vehicles. The most important thing is that, relying on its remote communication capabilities, SIM card can write and update sensitive parameters such as certificates and keys through online communication methods such as cellular network, which greatly optimizes the existing offline preset solutions and avoids Large-scale transformation of enterprise production lines to achieve rapid deployment capabilities.

However, the current traditional SIM card cannot fully meet these requirements. Therefore, it is necessary to upgrade the traditional SIM card to implement the V2X security function. This article designs a new type of SIM card for the Internet of Vehicles based on an independent high-performance HSM module. Relying on the SIM card's communication, multi-application management and basic security capabilities, it implements functions such as cellular communication, GBA and V2X certificate initialization, message signature and verification.

3.2. Architectural Design
The new SIM card uses high-performance security chips as the basic hardware, integrates SIM card
capabilities and V2X security capabilities, and uses high-speed communication interfaces to provide external services. The overall Architecture is shown in Figure 1.

Figure 1. A New Type of SIM Card Architecture

The new SIM card not only supports the original V2X security functions such as message signature and verification, but also adds support for traditional application functions of the SIM card (such as network authentication), namely the SIM application and V2X application in the architecture, which respectively implements the network authentication function, signature verification and certificate download etc. The communication between the new SIM card and the LTE-Uu module is based on the I2C interface, and the communication module internally finish the interaction with the baseband chip, thereby implement cellular communication and GBA functions. Through the SPI interface, the new SIM card can communicate with the AP chip, so as to implement the functions of certificate initialization, V2X message signature and verification. And the new SIM card uses the SM2 algorithm to finish the signature and verification of V2X messages.

Based on the SIM function, the new type of SIM card expands to support the V2X security function, which are the SIM application and the V2X application in the architecture respectively implement the network authentication function, signature and verification, and certificate download related functions. On the basis of the original interface (IF2/IF3/IF4), the new SIM card adds a new high-speed interface IF1 for communication with APs, thus implement the functions of certificate initialization and V2X message signature and verification. At the same time, one or more channels can be configured to meet the needs of various high-speed or extremely high-speed data processing.

3.3. Technical flow-process
The technical process mainly includes the GBA process, the certificate application/download process, and the message signature/verification process of the direct communication process.
4

OBU Application

New Type SIM

Module Baseband

OBK Application

BSF

NAF

CA Server

Figure 2. V2X Security Technical flow chart of new type SIM card

- **GBA process.**
  This process complies with the 3GPP TS 33.220 and TS 33.102 standards. After the GBA process, the new SIM card and NAF negotiate to generate Ks_int_NAF, and Ks_int_NAF is stored in the SIM card to ensure its security.

- **Certificate application and download**
  This process can be based on Ks_NAF to protect the certificate application request and response data, and finally implement the function of downloading the certificate to the new type of SIM card, and the new type of SIM card stores the certificate data at last.

- **V2X direct communication**
  The OBU terminal application receives the signed direct communication message and requests the new type of SIM card to verify the signature. The SIM card uses the certificate public key to verify the signature, and returns the verification result to the OBU terminal application.

  The OBU terminal application constructs the data to be signed, requests the SIM card to sign it, and then SIM card uses the certificate private key to generate the signature, and returns the signature data to the OBU terminal application at last.

### 3.4 Verification and Test

In order to verify whether the V2X function and performance of the new SIM card meet the requirements of the car-level security chip after the SIM function is added, this article is designed a end-to-end verification scheme, which includes the SIM card, OBU, module, CA and GBA network elements. Figure 3 is the overall architecture of this verification system.
In this verification procedure, a mainstream vehicle-mounted high-performance chip was used as the basic hardware of the new type of SIM card, and using the mainstream vehicle networking board IMX6 as the OBU terminal for testing.

### 3.4.1 Function verification

The overall goal of functional verification is the V2X secure communication function and the V2X OBU access cellular network function, including the V2X certificate download, signature and verification function, the V2X end-to-end secure communication function, and the SIM card application login authentication function.

During the verification process, the certificate application on the AP side of the OBU terminal (including X-OBU and V-OBU) initiates the certificate application process. Through interacting with the certificate service system, the OBU terminal can finish the certificate application and download process, and at last the new type of SIM card saves the certificate. The test result show that the V2X certificate can be downloaded to the new SIM card and the procedure of certificate application and download is successful. During the signature and verification test, the V2X request data is constructed through the V2X application of X-OBU, and this request is signed through the V2X card application in the SIM card, and then the V2X communication request (signed) is sent to the V-OBU through the V2X communication module, and then the V-OBU SDK send the communication request to the V2X card application in the SIM to verify the signature. The testing result is that the V2X card application can implement the signature and verification procedure. For the SIM function, the system controls the login authentication function of the OBU terminal through the Login authentication test procedure (located in the LTE-Uu communication module), simulates the process of login authentication and location update during the base station switch process when the vehicles is moving. The final results show that the new type of SIM card can achieve the above functions.

### 3.4.2 Performance verification

Because V2X has high performance requirements for signature verification and is also a key feature provided by the security chip, this performance test is mainly aimed at verifying whether the performance of the verification signature of the new type SIM card meets the relevant requirements of the V2X vehicle-level chip.

- **Signature verification performance test**

  The verification process of signing verification performance is to create verification request data through the V2X application on the AP side, send the request to the V2X application on the card side, test sending 2 million requests and repeat 10 rounds to calculate the total length of successful verification. And at last calculate the frequency of verification. The result of each round of signing verification time is shown in Table 1 (the data of the duration shall be kept to two decimal places).
| Round number | Length (s) |
|--------------|-----------|
| 1            | 695.90    |
| 2            | 696.35    |
| 3            | 696.12    |
| 4            | 696.12    |
| 5            | 696.02    |
| 6            | 696.50    |
| 7            | 698.08    |
| 8            | 695.88    |
| 9            | 696.24    |
| 10           | 696.65    |

Calculate the frequency of signature verification based on the length of ten rounds of signature verification and the calculation method is as follows:

$$\text{Frequency} = \frac{(\text{Total numbers of request}) \cdot (\text{Total verification length})^{-1}}{(1)$$

After calculation, it can be known that the verification frequency of the new type SIM card is equal to 2871.97 times per second, and the result is greater than 2000 times per second, which meets the verification performance requirements of the V2X vehicle-level security chip.

4. Conclusions

V2X technology realizes vehicle networking and also puts forward new requirements for security. At present, the realization of V2X communication security is mostly based on the implementation of digital certificate technical solutions based on public key infrastructure. Car companies need to write security parameters in advance through offline presets, and which puts higher requirements on the production lines of companies, and at the same time requires companies to invest more in management costs. Based on the existing high-performance security chip, this paper designs and implements a new type of SIM card that meets the requirements of vehicle-level V2X security chips which can be applied to the Internet of Vehicles environment and relying on its characteristics, the new type SIM card can write and update security parameters in a secure online manner, which can reduce the requirements for the transformation of the production line of car companies and improve the security of data management. This paper explained the implementation of the new type SIM card from the aspects of architecture and technical process, and designed a set of experimental verification system to verify the new type SIM card functions of certificate downloading, V2X secure communication, login authentication and signature verification performance. The test results show that the new type of SIM card can achieve all functions mentioned above and the performance meets the relevant requirements of V2X. The project team will continue to optimize this solution based on the security capabilities of the new SIM card, and further verify its application in the actual V2X scenario. In the future, as the Internet of Vehicles industry chain improves and matures, the various indicators of this solution will be more excellent and will better support the application of V2X in various scenarios.

References

[1] Ye Tian. (2020)A new initial security configuration scheme of C-V2X car networking terminal. Telecommunications Engineering Technology and Standardization, 33:59-64.

[2] Ze Hong.(2020)Encryption engine chip design for car networking information security, Network Security Technology and Application, 02:36-38.
[3] Yun Lin. (2021) Design of Vehicle Data Encryption Terminal Based on THD89 Encryption Chip. New Product & Tech, Single Chip Microcomputer and Embedded System Application, 03: 59-63.

[4] Beijing Nebula Link Technology Co.Ltd. (2020) C-V2X large-scale terminal communication field test report. Beijing Nebula Link Technology Co.Ltd, Beijing.