Medicon Engineering Themes
Volume 5 Issue 5 November 2023
Article Type: Mini-Review
ISSN: 2834-7218

The Factory Default of eSIM

Yongdong Li*

Rohde & Schwarz China, Product & System Department, China

***Corresponding Author:** Yongdong Li, Rohde & Schwarz China, Product & System Department, China.

Received: October 11, 2023; **Published:** October 28, 2023

DOI: 10.55162/MCET.05.171

Abstract

eSIM will be used widely as it is easy to control, can be filled in for different IMSI requirements, is stable for moving. It can be equipped for vehicles T-Box, post terminal of banks, CPE, and other modules moving. As the secret key is installed in the eSIM, does not open to other people except for operators, the boxes using eSIM are difficult to be checked if they work fine. This problem is from billions of boxes. They will benefit from our solution. The factory default setting of eSIM will save plenty of time and a lot of human resource for testing, at the same time, eSIM can be promoted.

Keywords: eSIM; secret; vehicle; card

Background

Filling the profile of SIM of operators into one buffer, this will make it work like SIM, it is called eSIM. As it can be filled in by software, it is easy to use and defined. At the buffer is one part of the box, it is stable under frequent mechanical oscillation, it can be used in a lot of application. for example, T-box of vehicles, report the data of energy meter, gas meter, video monitor, parking modules.

Problem

In vehicle applications, there are eCall and T-box application need to call set up. For multi-usage and stable, eSIM can read and the authentication of operators is necessary. Operators do not want other person to know the arithmetic and secret key of their eSIM, sot that the eSIM can't be registered to any instrument except to operators' network. This issue makes vehicle venders hard to do the quality inspection, also makes the venders of T-box modules hard to do the testing before shipment. The same problem also be happened in some special modules: energy meter, gas meter, monitor, CPE, etc.

Preparation

Definitions

eSIM - Embedded SIM.
T-Box - The telephone box of vehicle, which can set up mobile call, broadcast radio, video, support navigation indication.
SIM - A mobile compliant "smart" card that contains information about the user that is stored on the user's side.
CPE - Customer Premise Equipment (CPE) Customer premise equipment/customer premise equipment,
It refers to the device that connects the front-end of the user directly to the carrier network.

eSIM secret

1. eSIM means Embedded SIM.

2. The access authentication and communication encryption of SIM will not be transmitted in the air, also algorithms and parameters for performing security functions are written to the card, terminal, and network in advance. The network does not change throughout the card's life cycle.
3. The whole smart card is a relatively closed physical area, which has its own operating system and storage space, so it will not be attacked by external operating systems and application software.
4. In terms of its own physical security, there is no difference with traditional smart cards.
5. Embedded smart card adds remote management mode, root key, IMSI and other core data will be in the operator network and embedded intelligence. there are multiple transfers between the cards, and the security algorithms stored in the smart card need to be dynamically updated.
6. The root key, IMSI, the security algorithms and other core data do not open to others except for operator itself. It makes it impossible for other monitor to capture the updated security algorithms.

What operators think

1. Control the eSIM only by operator itself.
2. Edit the secret parameter by remote.
3. Special application anchored at the operator supplying the application.
4. It is impossible for others to get the secret data.

Quality inspection

1. Factory quality inspection has to do the RF testing to verify if the modules work fine one by one
2. The verification of modules has to check the RF parameters and the functions of the product with the modules.
3. For the testing, the instrument has to set up call with the modules. The register is mandatory.
4. Getting the root key, IMSI, the security algorithms and other core data of SIM card becomes precondition as it becomes possible for modules to register to instrument after getting the data.

Solution

eSIM is impossible for others to get the secret data

1. According to part II, we can know that eSIM is impossible for others to get the secret data.
2. The quality inspection has to find another way to call setup.

Set switch ON/OFF for eSIM

1. We can set one switch for eSIM enable or not.
2. When we do quality inspection, the switch is set to OFF.
3. It can be done by software or hardware. We suggest hardware switch for it as it will be easier to operate.

ON-eSIM work, OFF- factory default work

1. ON-eSIM works like the normal procedure, all register data is secret.
2. OFF-eSIM does NOT work, the factory default is set, the register data (the root key, IMSI, the security algorithms and other core data of SIM card) is published.

Realization

OFF, modules register to instrument to check the RF parameters and all function necessary.

1. ON, eSIM works, it will work during the modulation application.

2. Before delivery, the switch is OFF, we can do the quality inspecting.
3. After completing the inspection, put the switch to ON.
4. The switch is set to OFF when the module has to check.
5. For promotion easier, we suggest it is mandatory standard that there must is one ON/OFF switch for eSIM enable or not.

Feasibility

One-off switch

For more feasibly, the switch of eSIM can be one-off switch. After inspecting, the switch is set to eSIM enable all at once.

Factory default

Anyhow, after the module is set to factory default, the eSIM should be disable (Switch OFF). It will be easy to recover data to the register parameters, so modules will register to instrument easy for RF testing.

Action

Mandatory standard

We should put next two items into mandatory standard:

eSIM switch ON for work, OFF for disable.
When eSIM OFF, normal SIM card works, the register data is fixed, they are published for all person.

Advantage

Easy

The quality inspection becomes easy.

Cost

A few billions of modules testing, the verification, repairing will be faster and easier. It will reduce a lot of coast, time, and human resource.

Conclusion

As eSIM secret data and dynamic updated security algorithms makes it impossible for modules to test by eSIM card. After we setup a mandatory standard that there should be ON/OFF switch for all eSIM cards and open the register data of factory default setting to all person, it will be much easier to do modules RF testing.it will save a lot of cost, time. and human resource. It is pretty helpful for engineering.

Future

In the future, we will research how to realize eSIM by software and the profile can be download from server.

Limitations

It has to carry out by all vehicles and vendors, it has to design at the top of supply chain.

References

1. QIU Jianshu, Kang Jianxiong and Yan Binfeng. “Security Analysis and implementation of eSIM”. Internet World 11 (2016): 5-9.
2. Zhu Yan, Zhu Hongye and Zheng Haixia. “Research on Key Technology and Standard of Embedded SIM Card”. Telecommunication Network Technology 06 (2014): 57-60.

3. ZHOU Daiwei, Zhou Yu and Sun Xiangqian. “Research on Standardization Process and Remote Management Technology of Embedded SIM Card”. Mobile Communications 38.09 (2014): 42-47.
4. ETSITS103.383 SmartCards: EmbeddedUICC Requirements Specifcation.
5. ETSI TC SCP Meeting #59 Sophia Antipolis, France (2013).
6. Ma Jihua. “Why do operators choose different switching eSIM services?”. Journal of communication world 15 (2023): 4.
7. LI Xunhong and JIN Liang. “Progress of eSIM Technology and Application of Vehicle Networking”. Intelligent Connected Vehicle 01 (2023): 90-93.
8. Tan Lun. “Ministry of Industry and Information Technology Research to promote eSIM technology application industry chain for good”. China business news, 2022-09-26 (C03).
9. Ji J H. “Research on multi-scale deep learning methods for image restoration”. Suzhou university (2022).
10. St launches GSMA compatible eSIM card chip for ST4SIM M2M”. Application of single Chip Microcomputer and Embedded system (2021): 94.

Volume 5 Issue 5 November 2023