ISSN 2250-3153

Secure Communication between Card and Server

Bharat Bhanjana

Syscom Corporation Ltd

Abstract- In this paper, a brief description of SECURE COMMUNICATION between the CARDS and the OFFLINE ENTITY (server) are explained. With describing the process, it also introduces with the types of securities that can be implemented to makes Communication secure. And at last, this paper familiarizes with some of the Secure Channel Protocols that are currently being suggested by Global Platform.

Index Terms- Entity Authentication, Integrity and Authentication, Confidentiality, Secure Channel Protocol.

I. Introduction

With thinking the need of this technology i.e. SECURE CHANNEL PROTOCOL, I first gave a thought IS THERE IS ANY NEED OF SECURITY?

With this I took an example to convince myself that How about am I talking to someone and some another person listens all communication and can modify our conversation like I say Hello to someone and in between someone modifies it to CHAL BHAAG. What about the person to whom this data actually delivers, he will surely not reply with Hello.

So, with this thought in my mind I move on to draw some understanding regarding the Secure Channels used in our Smart Cards for SECURE COMMUNICATION between the client (card) and server.

II. Steps to Communicate Securely

To start with I would share the process of how this SECURE CHANNEL works between card and server using the same example I quoted above.

There are basically three steps to communicate SECURELY with an SERVER:

1. **Initiation (technical term: SECURE CHANNEL INITIATION):**

This step includes:

a. Authentication of the server (off-card entity).
b. Exchanges sufficient information to perform the security on the data to be exchange.

So, now if I co-relate this step to the example, then this step basically first authenticate the person to which I wanted to speak to.

Once the person is authenticated, second step is to exchange all the information so that the communication that we need to transfer would be secure (not to be crack by someone and not to be modify by someone)

2. **Operation(technical term: SECURE CHANNEL OPERATION):**

This step includes the exchanging of data between the card and the server (off-card entity) using the security generated from the step 1.

So, again co-relating this with example, it means this step includes the communication that is to be transfer between me and the person to which I wanted to talk to. That is Hello that I wanted to speak to the person and his reply. In this step the data (to be transferred) is secured by the keys and some cryptographic functions that are generated in step 1, remember exchange of some information.

3. **Termination(technical term: SECURE CHANNEL TERMINATION):**

This step includes the termination of the communication. Whenever the card or the server determines that there no more communication needed, then the communication is terminated.

So, last time again co-relating this example, this step pressing the RED BUTTON i.e. terminating the call whenever me or the person to which was communicating feels that yes now there is no more communication needed.

This was a very brief introduction of how SECURE COMMUNICATION happens between the card and sever.

III. Securities offered by Global Platform

Let's move down a little bit more and see ***How are we getting the communication SECURE***. I mean what all securities we are applying in between the communication such that after this I can say ***No one can modify my HELLO to CHAL BHAAG***. Basically there are three types of security provided by Global Platform to make the communication secure. These are:

1. **Entity Authentication:**

This is the security in which either the card or off-card entity needs to provide ***AUTHENTICATION*** to the other entity.

So co-relating it with the example it means either I or the person to which I wanted to talk to need to provide authentication to the other entity.

2. **Integrity and Authentication:**

This is the security in which the message receiving entity actually **verifies the authenticity of the message sender**. Also in addition is also **verifies that the message is not being altered over the communication channel**.

So co-relating it with the example it means when the receiver receives my HELLO, he/she will first verifies that message came from me and not someone else. Also he/she verifies that HELLO is the same data that I sent and that he/she receives.

3. **Confidentiality:**

Last and the most important (in my point of view) is this service. This is the service in which it is being verified that the **message i.e. being transmitted over the communication channel is not being visible to any other entity**.

So for the last time co-relating it with the example, it means the my HELLO will not be visible to any other entity (excluding the receiver)

So, this is all the security that can be implemented in order make **COMMUNICATION SECURE**.

IV. Secure Channel Protocols

I believe this is the right time to introduce you all with SECURE CHANNEL PROTOCOLS. There are different protocols or in layman language I would say ***IMPLEMENTATIONS*** using which the communication taking place between off-card entity (may be server) and on-card entity (may be some application) can communicate SECURELY. **These different implementations are referred as SECURE CHANNEL PROTOCOL**S. Currently there are different SECURE CHANNEL PROTOCOLS provided by ETSI group and Global Platform.

Secure Channel Protocols provided by ETSI group and Global Platform are:

- ✓ Secure Channel Protocol 01
- ✓ Secure Channel Protocol 02
- ✓ Secure Channel Protocol 10
- ✓ Secure Channel Protocol 80
- ✓ Secure Channel Protocol 81
- ✓ Secure Channel Protocol 03

Now we got the process – how we communicate securely, the three securities – applies to make communication secure, the different Secure Channel Protocols – different implementation to implement securities.

Just the last question – **Who is going to implement this?** Is it every off-card entity (e.g.: every application) or Is it someone other entity on card.

To answer this question, Global Platform provided two ways in which application residing on card can use SECURE CHANNEL PROTOCOL:

1. **Direct Handling** (and in simple words IMPLEMENT SECURE CHANNEL PROTOCOL BY THEMSELVES)
2. **In-direct Handling** (and in simple words LET SOME ONE (e.g.: security domain) TAKES CARE TO IMPLEMENT SECURE CHANNEL PROTOCOL FOR YOU)

V. Conclusion

Through this paper, I would like to share my understanding towards SECURE COMMUNICATION between SIM CARDS and SERVER. Also I tried to write down this paper keeping in mind that the knowledge should not only be communicated to DOMAIN PERSON but even if LAYMEN read this paper, he/she will also understand the communication. So, by concluding I would really suggest to SIM CARD Dealers or OTA Server parties to use these PROTOCOLS since in today's world where there is almost to everything hackable, we really need something to be really POWERFUL that can really protect our data and communication.

Acknowledgment

I would like to acknowledge my co-workers for supporting and encouraging me throughout the course work.

References

[1] GP Card Specification 2.2

Authors

First Author – Bharat Bhanjana, Qualification /Experience: Currently working with Syscom Corporation Ltd, a leading telecom company dealing in SIM and SMART cards., Email Address: b.bhanjana@gmail.com