Secure Element

An evolution to existing secure technology

Sonal Rohilla, Reaserch & Development, Syscom Corporation ltd., Morpho, Safran

Abstract — This paper outlines the very basic concept of secure element. Also it talks about various types of secure elements, what were the needs which lead to the evolution of each type, how one better over the other, what are the challenges is faced by each step of this technology!

Index Terms — SE (Secure Element), NFC (Near Field Communication), POS (Point of Sale), UICC (Universal Integrated Circuit Chip), SIM (Subscriber Identity Module), TEE(Trusted Execution environment)

1 Introduction

Technology progresses each day each step! A truly justifying example to this statement can of course be NFC technology and associated secure element (SE).

Until few years back we had to carry our ID cards, health cards, payment cards in the form of a typical A4 size paper sheet.

With a further techno step; we moved to carry these cards in the form of a plastic cards some of them being smart as they carry a smart chip inside them.

Again, with a bigger move our world is now ready to migrate to all these cards in the form of the virtual smart cards residing in our mobile phones or other devices.

These mobile phones are NFC enabled i.e. they have the ability to interact with their surroundings without actually making a physical contact with them. Such a communication is often referred as contactless technology and is widely used in NFC i.e. near field communication.

When a user uses an NFC enabled device the NFC controller inside the device goes into the card emulation mode. Just to brief, NFC device have three operational modes.

- **Reader/Writer mode –** Device can read/write any defined NFC tags. In this mode the device can read information stored on smart posters or smart displays. This act as perfect marketing opportunities for various companies, for eg: user can get to know various offers, upcoming sale, can read the various schedules etc.
- **Peer to peer mode –** Two NFC devices can exchange data amongst each other in physical proximity. With this mode the NFC users can share various information qucikly like sharing photos, contacts, links, files, etc.
- **Card emulation mode –** In this mode NFC device acts a contactless smart card which communicates with external often called POS i.e. point of sale. With this mode a NFC device user can easily make payments, do ticketing, use coupons etc.

So, when NFC controller works in card emulation mode, desired information is securely shared between device and a POS terminal. But NFC controller only acts as an interface that allows the secure communication, however an imperative question here is where this information is stored? Where the flow of information is managed? Who claims this information to be secure?

The answer to these questions is Secure Element (SE).

To quote the definition from standard;

"Global platform defines secure element as a tamper-resistant hardware/platform capable of securely hosting applications; their confidential and cryptographic data (e.g. key management) in accordance with the defined rules and security requirements"

To be more explanatory;

SE simply is a secure chip residing traditionally in a NFC-enabled device.

A typical archiecure of a secure chip consists of various components like secure microcontrollers, CPU, operating system, memory RAM – ROM - ERPORM, crypto engines, timers, communication ports etc.

When a NFC application demands high levels of security – such as payment applications – it is stored inside these secure chips called secure element.

SE provides dynamic environment where the application code, its confidential data is stored and the application code is securely executed. For eg: for a payment application all the personal data like account number, expiry date, passwords, card numbers are stored in secure element and then the safety of its secret information can be trusted upon.

To be more specific, application inside the SE performs several tasks like; handshaking with the POS terminal, responding to queries received from terminal, authenticating the card, filtering data to be shared etc; but it is the SE that provides secure execution environment for applications to perform all their defined tasks.

2 Architecture of SE

Secure Element follows the widely accepted HTTP Client – Server communication model. Due to this fact its deployment becomes compatible with existing infrastructure and also inherits the advantages of HTTP communication like scalability and high availability.

To initiate interaction, a communication session is estalished between client and server. All further communication taken place within that session. Often the client is responsible for initiating the communication session.

The main components involved in SE architecture are:

1. Service provider
2. Admin Server
3. Mobile phone
4. Secure Element
5. Application

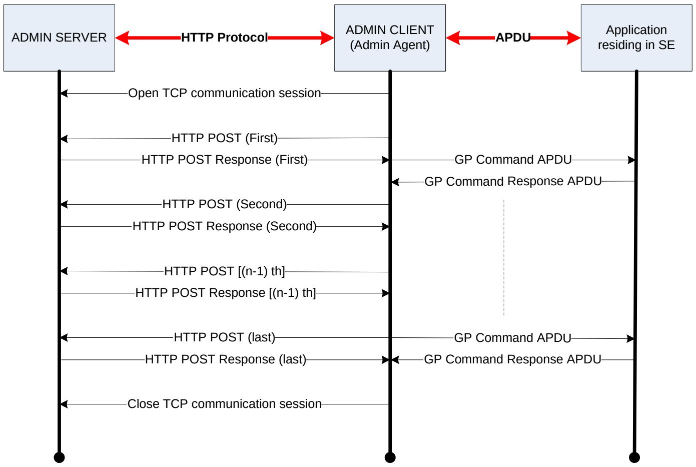
In this arrangement the admin server acts as HTTP server and admin agent act as HTTP client. The communication session is termed as administrative session. The initiation of this admin session can be triggered by:

- a device external event, for example a Push message sent by an Admin Server. Here the request is initiated by admin server
- an Admin Agent internal event, for example a timer. Here the request is initiated by admin agent (client)
- an administered SE application request. Here the request is initiated by application residing in SE.
- a device application request. Here the request is initiated by a mobile application.

The communication between the admin server and admin agent takes place by using HTTP protocol. The admin agent is responsible for interpreting these HTTP responses from server and further converting them into APDUs understandable by application residing in SE. This structure of HTTP request/response and APDUs exchanged between admin agent and application is defined by Global platform specification [1].

Depending on the type of secure element (discussed over later sections of this paper) the admin agent can be implemented in following ways:

1. For UICC SE: Admin agent is implemented in the application security domain i.e. APSD. The application resides in the secure element which inturn resides in the UICC card.
2. For Embedded SE: Admin agent is implemented in the trusted execution environment in mobile phone
3. For a micro SD card SE: Admin commands will be forwarded to SE through mobile application implemented using JSR 177 for java ME.


ADMIN SERVER
HTTP Protocol
ADMIN CLIENT (Admin Agent)
APDU
Application residing in SE
Open TCP communication session
HTTP POST (First)
HTTP POST Response (First)
GP Command APDU
GP Command Response APDU
HTTP POST (Second)
HTTP POST Response (Second)
HTTP POST [(n-1) th]
HTTP POST Response [(n-1) th]
HTTP POST (last)
GP Command APDU
HTTP POST Response (last)
GP Command Response APDU
Close TCP communication session

3 Types of Secure Element

Depending on the place where SE resides inside a NFC device; there are three form factors of SE:

- UICC SE
- Micro SD card SE
- Embedded SE (eSE)

UICC SE

- In this the SE is housed inside the UICC operating system.

- UICC communicates with the NFC controller in the handset through a Single Wire Protocol (SWP)
- Is detachable from the device

Advantages of UICC SE:

- UICC and SWP interface are standardly defined by ETSI so supported by majorly all MNO's. Thus savind additional cost of deployment
- UICC is removable so can be changed among devices. In case of a change the SE and associated application remains with the UICC giving in some way portability and compatibility features.
- Since application resides in SE, SE further in UICC so in case of lost the app secure data can be destroyed thus protecting from threaths and mishandling.

Challenges for UICC SE:

- Quite known fact that memory has always been a critical issue for a UICC or SIM card so in some cases the applications find insufficient memory in UICC. In order to have some more memory some how the compromise has to be done for performnace so again an issue for such secure and critical applications.
- Controlled mainly by MNO so conflicts come with business needs of other entities

Micro SD SE

- SE is stored in a standalone microcontroller chip.
- Chip can be plugged in and out of device as and when needed.
- Can be with or without embedded Antenna
- Issued and owned by a 3rd party (banks, etc.). No involvement of MNO and OEM

Advantages of Micro SD SE

- A minimum NFC device can be converted easily into a highly secure NFC device by just inserting a micro SD card
- Highly portable as it can be easily removed and replugged into a device. Applications can also be easily removed
- Many applications can exists in same SD card

Challenges for Micro SD SE

- Costly as compared to other SE's
- Applications have to share space in SE
- The keys remain with service provider so business conflicts with application providers

Embedded SE (eSE)

- SE is stored in a microcontroller chip which is directly housed into the device mother board.
- Cannot be removed from the device.
- Issued and managed by either the OEM (Original equipment manufacturer) or MNO (mobile network operator)

Advantages of eSE:

- Since it is embedded into the device so offers more performance
- Power consumption is also less

Challenges for eSE:

- An intact dependency on the device manufacturer
- Applications can only be accessed with the same device

All the above described SE's have interdependencies on each other for a complete solution deployment to customer. For eg: an application developer have to depend on the SE manufacture to allow a space in SE. SE has to depend on the handsets for further deployment. All in all, the entire ecosystem is much coupled thereby making the system as complex and less flexible. A solution to breach such dependencies is moving SE to a remote location i.e. Cloud Based SE.

Cloud Based SE

- Sensitive data is stored in the cloud rather than locally on the mobile phone or any other device.

- When the user conducts a transaction, the data is pulled from a remote virtual secure element in the cloud in encrypted format

Advantages of Cloud Based SE:

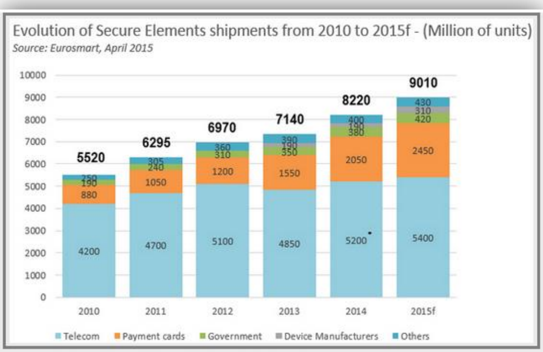
- **Cost Effective:** The cost is directly proportional to the amout of data hold by SE. Since the data increases timely with more and more applications and usgae so the cost of SE significantly increases. Such a cost is avoided in cloud based SE where it will only handle the user and mobile authnetication rather than storing data.
- **Easier delopyement:** Easier to implement the NFC services as there is no need to explicitly integrate the SE in phone.
- **Support multiple applications:** In other SE space is shared with various applications and as discussed above cost α space, so keeping the tradeoff, there exists always a limit to support the number of appicatons. In cloud based, no such limit exists.
- **Single store for all data:** User will be easy to access all applications from a single NFC enabled device as all the data will be stored in a single cloud umbrella.
- **Less chances of stealing:** Since the complete ecosystem is working online in this case so, one it will be easy to detect the crime source and second the stealers would have fear in doing so.
- **Easy for user access via web browser:** Since the virtual seccure element is stored in cloud so user can access their services via any standard web browser. Additionally there is no nedd to maintain a seprate mobile wallet to mange the services.
- **Complete secure even in case of Lost and found:** No threat as everything resides in cloud and nothing on users device.
- **Linking to multiple could SE:** Single NFC device can esily be linked to muliple cloud SE's

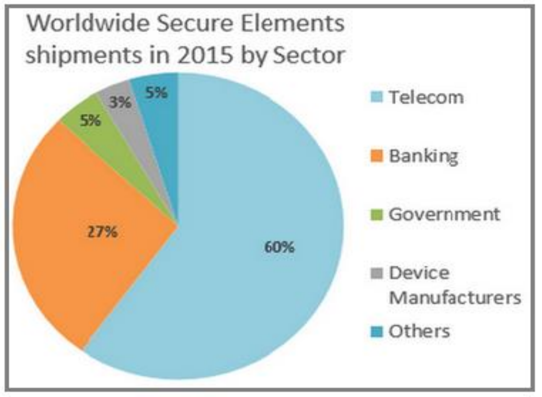
Challenges for Cloud based SE:

Although the processing time will be fast enough as much more computing can be applied on server than on the SE residing on device but it is predicted that it can take much more time for the request initiated from user to reach the cloud and return the response to POS terminal.

4 End Note

To end this paper, it can be just said that Secure element is underneath technology which is showing an escalating growth in various sectors. An evidence to this statement is the below representation collected from web.


Evolution of Secure Elements shipments from 2010 to 2015f - (Million of units)
Source: Eurosmart, April 2015


Worldwide Secure Elements shipments in 2015 by Sector

Being a telecom professional or a simple user of this technology it's worth to know about it..

ACKNOWLEDGEMENT

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

REFERENCES

[1] GlobalPlatform Device , Secure Element Remote Application Management, Version 1.0
[2] NFC Forum
[3] Global Paltform Card Secification v.2, Amendment B

AUTHOR

Author Name: Sonal Rohilla

Qualification /Experience: B.Tech .Currently working with Syscom Corporation Ltd, a leading telecom company dealing in SIM and SMART cards. Syscom is a Morpho, Safran organization. Experience is ~ 9 Years.

Email Address: sonal.rohilla@gmail.com