

# Host Card Emulation

Nishant Prakash

\* Research and Development, Syscom Corporation Ltd. (A Safran Morpho Company)

*Payment system is the mechanism that enables the smooth transfer of finances between buyers and sellers, or between banks. In the contemporary society, no monetary activities are possible without the transfer of paper currency. It can readily be said that payment system is one of the most important social infrastructures. Gone are the days when payments were used to be in cash only, slowly and gradually cheque came into picture and after that internet banking. After Internet banking mobile banking or mobile payment, in this way we can say money is transformed from paper to card to mobile and now to software. Now we hear the term contactless or proximity payment in which payment is done via NFC. Evolution of money brought the changes in security aspect also These technologies are getting wider day by day, NFC uses Secure Element for the transaction but now a days, payment can be done without involving Secure element (i.e.) only by the help of software that is build in the Operating system of the mobile phones.*

**Index Term – HCE, NFC, SE, Mifare.**

## I. INTRODUCTION

Mobile Wallet and The Near field communication (NFC) technology have conventionally stored all the statistics needed to make a transaction on a physical secure element (SE) within mobile equipment. This has given the rights to the operators who own the Security Element (SE) – such as / mobile network operators (MNOs) or mobile equipment manufacturers – as the gatekeepers, in terms of permission to access the SE as well as charging to access it. Since there are many SE owners operating around the world, each and everyone with a exclusive business and technical depiction, operators must retain the relationship with each other in order to make delivery of their services via NFC. Many industry genius recognize the challenges surrounding integration between many of the key players in the NFC ecosystem; this is why mass market NFC services are yet to be deployed. The Payment industry has been hugely applauded with the introduction of host card emulation (HCE): it allows NFC-based applications to be added to mobile devices and operate successfully without having to get connected with the Secure Element.

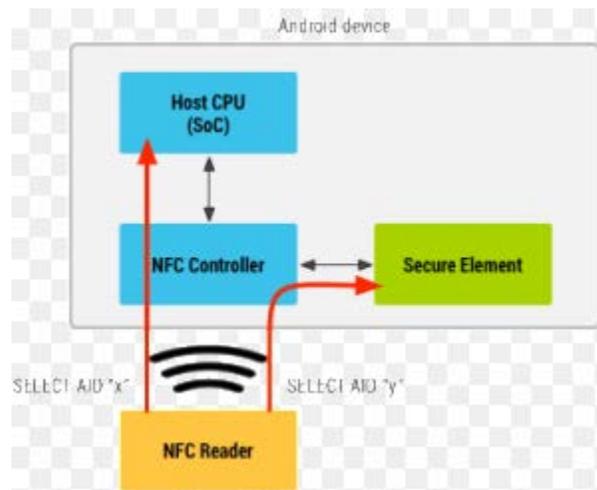
## II. WHAT IS HCE

Host card emulation (HCE) is the software design that provides accurate virtual representation of different electronic identity (access, transit and banking) cards using only software. Before HCE architecture, NFC communication was principally carried out using secure elements, which were incorporated into operator-issued SIM cards. HCE enables mobile applications running on supported operating systems with the facility to propose payment card and access card solutions separately of third parties while leveraging cryptographic processes conventionally used by hardware-based secure elements without the need for a physical secure element. This HCE technology enables the dealers to present payment cards solutions more easily through mobile closed-loop contactless payment solutions, offers real-time allocation of payment cards and, more strategically, allows for an easy installation of the scenario that does not require changes to the software inside payment terminals.

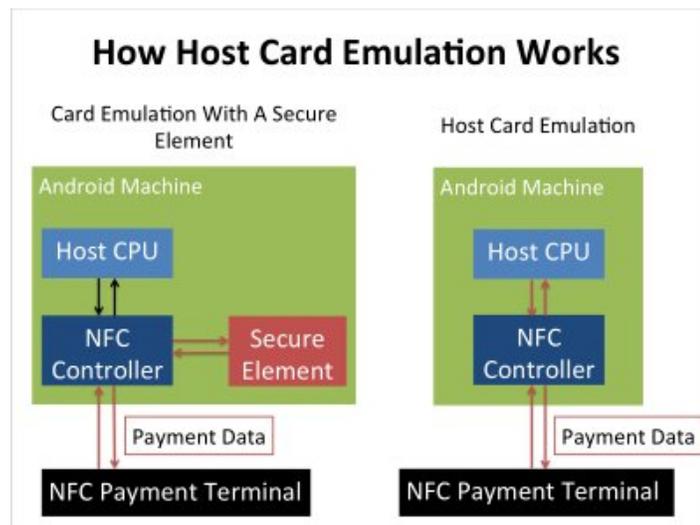
Mobile payment testimonial have traditionally been stored locally on the mobile equipment inside a piece of hardware called the secure element (SE). An SE is tamper defiant hardware platform, competent of securely hosting applications and storing confidential and cryptographic data. Hence it plays a very significant role in secure mobile computing.

In the payment industry SEs are used to host personalized card applications and cryptographic keys required to perform payment (EMV) transactions at a point-of-sale (POS) terminal. SEs used in the ID market may hold biometric data or certificates which can be used for signing documents. Whatever the reason is, the secure environment provided by the SE protects the user's credentials ensuring the safety of the user's data. The presence of a Secure Element in the equipment creates dependencies and complexities that make it complex and costly for entities in an NFC ecosystem to assist competently. For example, an application provider would need to have agreements with a number of SE providers, who in turn need to connect with different types of mobile equipments. HCE technology emulates a financial card on mobile equipment using only software. Through mobile operating system it enables a 'virtual' SE (Secure Element) to be present outside the mobile equipment. By moving the SE to a remote location (environment), the

technicalities and associated costs can be overlooked: application providers can directly deploy their applications to a virtual SE without any intermediary involvement.



The picture above represents physically present Secure Element in the device through which transaction takes place. Basically NFC Card Emulation with Secure Element.



In the above picture, we can easily distinguish how it was in NFC card where secure element was present and how it is now through Host Card Emulation.

### III. IMPLEMENTATION OF HCE

HCE is currently supported by BlackBerry and android, it is creating many opportunities and solutions in the industry. These endorse choices and give service providers/operators the capability to effortlessly and successfully set up NFC services to their clients in a manner that supports their financial objectives, industrial capabilities and security requirements. As well as delivering alternative payment technologies, HCE may also encourage Mobile Network Operators (MNO) to cooperate on cross solutions which are less tedious to implement. This will speed up the progress of NFC services and may be the channel needed to deliver the benefits of this proximity technology to both the industry and the clients they serve.

At present, two HCE NFC models available to operators:

#### 1. Pure HCE

In this issuer offers an alternative solution where cost of physical SE on the mobile equipment is justified, like low value payments, loyalty, couponing, access control, transportation and other low value applications. The Payment application is hosted remotely within security of cloud and hence it does not require SE in the mobile equipment. it simulates the SE in its communication with a POS terminal when making a transaction using pure HCE, and will receive the data required to make a payment after connecting to cloud. The card issuer holds the responsibility of the manager of the payment with responsibility for risk in payment ecosystem while the role of data carrier is played by the MNO.

#### 2. Hybrid HCE

Hybrid HCE has all profits of HCE which is coupled with the security of a physical Secure Element and is used only for the authentication purposes only. The main feature of this model is that it can be implemented on wide range of mobile devices without the involvement of Mobile Operator or Mobile Manufacturers. The owner of the SE has the responsibility of loading applet into the SE. The lifecycle management of the applet is managed on cloud hence MNOs are barely involved and also they don't require any big database to manage. Also to use NFC capability, SIM replacement is not required as the data is already on the cloud.

### IV. Business Benefits of HCE

In the NFC Ecosystem, everyone wants to work under beneficial and productive relationships which will boost the technology and value addition will be done. The prime benefit of HCE is that it allows the operators to be in control of costs, security, stake holders and lifecycle management of applet's position.

Other benefits that HCE offers:

#### 1. Issuers Independent

By installing services to HCE, no mediators are required to access the SE. This will minimize the gap between application issuers and customers, ensuring a reliable brand and customer experience across all accessible NFC services.

## 2. Easy Deployment

Since the MNO (Mobile Network Operator) are in control of SE and this allows integration easy with any third party issuer and business model which includes device manufacturers and service managers.

## 3. Less costly

Secure Element integration in mobile equipment is expensive business. By installing the SE remotely, the NFC value chain will be reduced as fewer parties in the ecosystem need to be involved; this leads to lower installation and maintenance costs.

## V. MIFARE Vs HCE

Mifare chips are recognized in NFC readers and smart cards whereas through HCE, NFC transactions is completed with handsets without the hardware component or SIM. Also, it is important to note that, Host Card Emulation (HCE) cannot emulate most of the Mifare protocols.

To be more precise, HCE can only emulate the ISO/IEC 14443-4 protocols, and most of the Mifare chips do not work on any of these protocols. So, many HCE enabled handsets are unable to do transaction with the Mifare terminals.

HCE is good for dealers too, but many dealers around the world using Mifare based readers are not able to accept payments from the customers who have HCE software in their mobile devices.

## VI. SOLUTION

There are two entities

- 1) Mifare Technology – Uses secure element for the transaction
- 2) HCE Technology – Didn't use Secure Element and protocols which were used by Mifare.

HCE is in the operating system of the Mobile Phone whereas Mifare is in the SE which can be used in a SIM or in the handset.

If we can use Mifare in the SIM using ST libraries and HCE in the operating system of the handset then may be the above mentioned problem can be solved.

## REFERENCES

- [1] <http://www.letstalkpayments.com>.
- [2] <https://members.nfcworld.com>
- [3] [www.hcesummit.com](http://www.hcesummit.com)
- [4] <http://www.sequent.com/host-card-emulation/>

## AUTHORS

**First Author** – Nishant Prakash, B.E. (E.E). Syscom Corporation Ltd.