**A Proposed NFC Payment Application**

**Near Field Communication**

NFC technology is based on short range radio communication, enabling users to exchange data between device

* Enables contactless payments
* Enables data exchange between devices

NFC has some underlying limitations/issues, which mainly stem from security concerns with Secure Element (SE) personalisation, management, ownership and architecture, which may be exploited by attackers.

**NFC Cloud Wallet – A Complete Transaction Mechanism based on NFC and GSM Networks**

This model is based on **cloud computing** for management of payment applications in secure element within the NFC ecosystem.

The authentication mechanism of the extended model is based on GSM.

The cloud is being managed by MNO.

Existing security features of GSM is used to achieve authentication, data integrity and data confidentiality.

The **SIM** is the secure element which is being managed by the MNO.

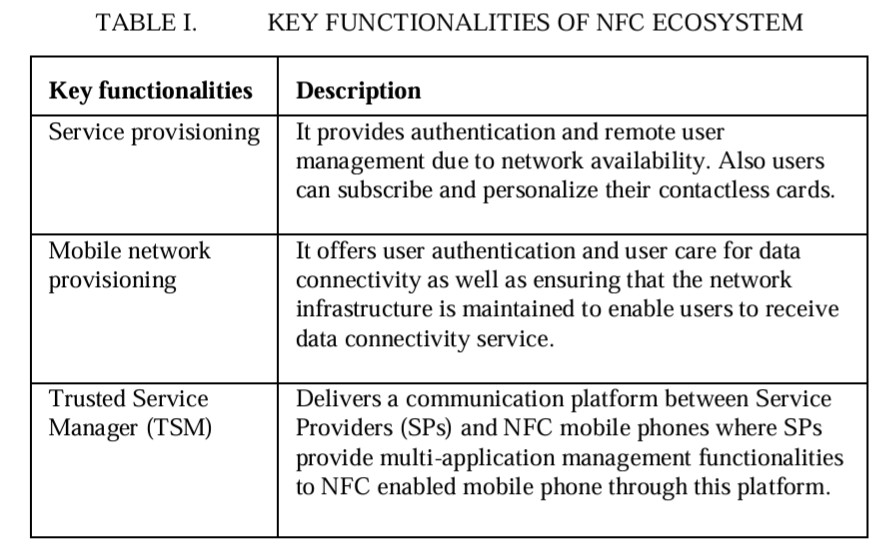
**NFC and NFC Ecosystem**

Near Field Communication is a technology in which data is transferred from one NFC-enabled device to another over a short-range communication channel.

The concept of an NFC mobile phone is shown below



The NFC mobile ecosystem is quite successful due to it being based on the relationships between involved parties, where those relationships have to be clearly defined. The key functionalities of an NFC ecosystem is shown below:



**Secure Element**

NFC security is usually provided by a security controller component that is in the form of an SE. The SE is an attack resistant microcontroller similar to the chip found in smart cards.

SE provides storage within a mobile phone and it contains hardware, software, protocols and interfaces.

It provides a **secure area for protection of payment assets** and the execution of other applications.

SE can also store other applications that require security mechanisms, and it can also be involved in authentication processes.

**The installed operating system of the SE must have the capability of personalising and managing multiple applications that are provided by multiple service providers (SPs), preferably Over-The-Air (OTA).**

**UICC (Universal Integrated Circuit Card)** is one of the most reliable components to act as an SE in NFC architecture.

Benefits of UICC:

* Removable
* Provides the same security as a smart card
* Can run multiple applications issued by multiple service providers
* Compliant with all smart card standards
* Supports GSM and UMTS networks
* The most appropriate SE in terms of GSMA guidelines

**SE Life Cycle**

* **Initialisation:** The SE can be initialised by different SE issuers, e.g. credit card companies, Mobile Network Operators (MNOs), financial institutions or retailers. The **SEI** can also act as a platform provider. If the SE does not have any applications when issued, it means that a platform manager was not assigned to the SE. A platform manager cannot deal with SE applications without having various certifications, such as Visa PayWave certification
* **Activation:** This takes place when the SE is inserted into the phone. The SE then communicates to the NFC controller, and the NFC controller sends a confirmation message to the platform manager to let them know about the successful insertion of the SE into the phone. **Only the platform manager** will have access to the SE keys for data configuration. The NFC controller’s identifier is also stored in the SE to inform the SE if it was inserted into another phone.
* **Applications Upload:**
  + **Phase 1:** The service provider, SP (in this case, also the Application Issuer, AI), contacts the MNO, who is the only party who is in charge of the Mobile Station International ISDN Number (MSISDN). MSISDN is the only way to classify the external party for Over-The-Air (OTA) transactions with NFC phone
  + **Phase 2:** The MNO then forwards the SP request to the platform manager that is in charge of the SE. If there is no SE in the phone, the MNO will inform the SP regarding the issue.
    - If there is no SE, the application upload process immediately terminates
    - If the platform manager is positive with the request, it will send an offer directly to the SP to upload its application.
  + **Phase 3:** The SP then selects one or more platform manager to load its data to the security domain area, which is also controlled by the same platform manager(s).
* **Deactivation:** The deactivation procedures are also managed by the platform manager. The manager can then deactivate the SE, OTA in the case of theft or loss.

If the SE is installed in a new device, then the activation process should be renewed.

**NFC Cloud Wallet Model**

This model incorporates cloud computing in order to manage NFC payment applications. Such a model brings the following benefits:

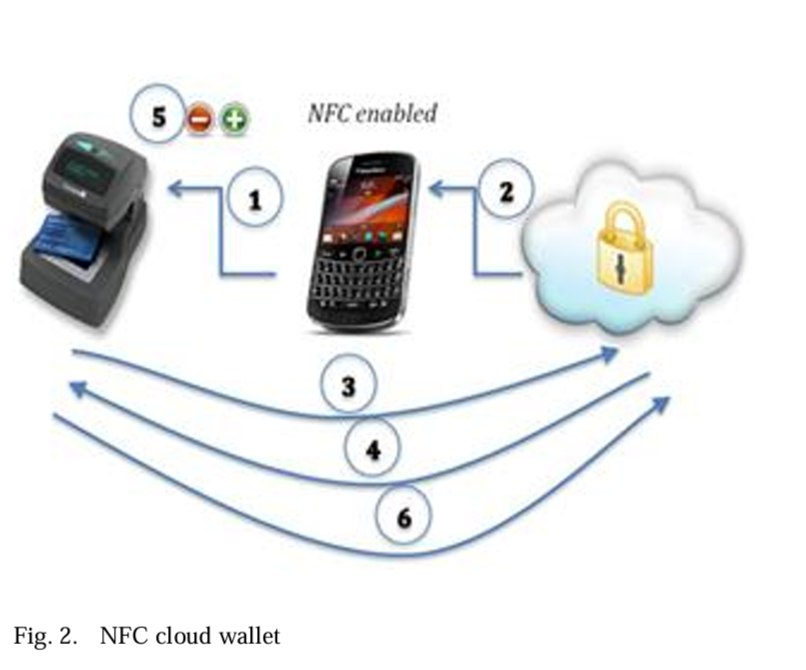
* Flexible and secure management of applications
* Personalisation of applications
* Ownership of applications
* Easy management of multiple users
* Delivers personalised contents to each user.
* Intelligent profiling functions by managing customised information relevant to each user in certain environments, which updates the service offers and user profiles dynamically
* With ideal MNO network reception, deployment of the service takes about 1 minute
* Can be scaled to any number of users

Approach of the model: Every time a customer makes a purchase, the payment application, which contains the customer's credentials, is downloaded into the mobile device (SE) from the cloud, and after the transaction it is deleted and the cloud will update itself to keep a correct record of customers’ account balance.

**Execution of NFC Cloud Wallet**

1. Customer holds the NFC phone near the POS terminal to make payment
2. The payment application is downloaded onto the customer’s mobile phone SE
3. The reader communicates with the cloud provider to check if the customer has enough credits in balance or not.
4. Cloud provider delivers the required information to the reader
5. Depending on the information received by the reader, the transaction is either approved or declined
6. Readers communicates with the cloud to update the customer’s balance
   1. If the transaction was approved, the amount from the transaction will be deducted from their account
   2. If the transaction was declined, the account balance will remain the same

An additional security measure is also suggested with step 1: when the NFC phone sends a request message to the cloud to get permission to make a payment, the cloud provider may send an SMS requesting a PIN, which the customer can send back as an SMS in order to ensure legitimacy of the user.



There are two possible methods to extend the NFC Cloud Wallet Model:

1. The **financial institution can be the cloud owner** from which the payment application can be downloaded from/into the customer’s mobile device. Hence, the MNO can be linked to the financial institution, or it can stand as a separate party.
2. The **financial institution can have a contract with a third party company** such as PayPal, which has its own cloud infrastructure (MNO can be linked with them, or stand as a separate party), or the financial institution can use other company’s cloud services, such as IBM, Microsoft, etc. (same details of MNO as before)

**GSM Authentication**

* When a mobile device signs into a network, the MNO first authenticates the device (specifically the SIM)
* The **authentication stage** then verifies the identity and validity of the SIM and ensures that the subscriber has authorised access to the network.
* The **Authentication Centre (AuC)** of the MNO is responsible for authenticating each SIM that attempts to connect to the GSM core network through the **Mobile Switching Centre (MSC)**
* The AuC stores two **encryption algorithms, A3 and A8, and a list of all the subscribers’ identities along with a corresponding secret key Ki**
* This secret key is also stored in the SIM. The AuC first generates a **random number R.** The R number is then used to generate two responses, **signed response S and key KC**.
* **Important: S = EKi (R) using A3 algorithm, and KC = EKi (R) using A8 algorithm.**
* The generated AuC values, R, S and KC are known as the **Authentication Triplet**. The AuC sends this triplet to the MSC.
* Once the MSC receives the triplet, it sends R to the mobile device.
* The **SIM** of the mobile device computes S using the given R, its stored secret key Ki and the encryption algorithm A3.
* Once the SIM has calculated S, it sends this calculated value to the MSC. If the sent value of S matches the S value stored in the MSC, the mobile device is authenticated.
* The KC value is used for communication encryption between the mobile station and the MNO.

A diagram of a diagram

AI-generated content may be incorrect.

The following table contains the descriptions of the abbreviations for the proposed model

A list of information on a white background

AI-generated content may be incorrect.

**Proposed Model**

The proposed model is an extension of the NFC Cloud Wallet Model, and makes the following assumptions:

* SE is part of the SIM
* Cloud is part of the MNO
* MNO is managing SE/SIM
* Banks, etc. are linked to the MNO

**Proposed Protocol**

* It is based on cloud architecture, in which the cloud is being managed by the MNO. The cloud and banking sector are subsystems of the MNO, in addition to the other subsystems of the MNO. It is assumed that the communication between different parts of the MNO is secure.
* The shop POS terminal, which is registered with one or more MNO, shares an MNO specific key KP with the corresponding MNO. This key is issued once the shop is registered with the MNO.
* The bank details of the shopkeeper is also registered with the MNO for monetary transactions
* The communication between the shop POS terminal and mobile device is wireless through NFC, provided the mobile device has a valid SIM.
* The existing authentication method for GSM is used for mutual authentication

The proposed protocol executes in three different phases: **authentication, keys generation and transaction.**

The protocol is initiated when the customer places his cell phone for the payment after agreeing to the total price displayed on the shop POS terminal.

**Phase 1: Authentication**

**Step 1:** Once the user places his mobile device, an NFC link between the mobile device and the shop POS terminal is established. The shop POS terminal sends an ID request message to the mobile device.

**Step 2-3:** The mobile device sends the TMSI and LAI as its ID to the shop POS terminal. Once the POS terminal receives the info from the mobile device, it can determine the user’s mobile network. The **network code is available in the LAI** in the form of **MCC (Mobile Country Code)** and **MNC (Mobile Network Code).** The MNC is used in conjunction with the MCC to uniquely identify the mobile phone operator/carrier.

**Step 4-5:** The shop POS terminal then sends the TMSI, LAI and shop ID to the respective MNO for customer authentication and shop identification.

**Step 5.1:** If the TMSI is incorrect, a declined message is sent.

**Step 6:** If the authentication is correct, the MNO generates a set of authentication triplet (R, S, KC) and sends R to the mobile device via the shop POS terminal.

**Step 7-8:** The SIM computes KC from R. The SIM then generate a random number RS and concatenates this with R, encrypting it with KC before sending it back to the MNO.

**Step 9-10:** The MNO checks the validity of the SIM. When it receives the encrypted message EKC (R||RS), which it decrypts using the KC key it calculated based on the TMSI and LAI it received from the shop POS terminal. The MNO then compares the R with its computed R to check if they are the same. If they do not match, the MNO sends a “Stop” message, and the protocol execution stops. If they do match, the mobile device with the SIM is authenticated. The MNO then swaps R and RS and encrypts with KC before sending it back to the mobile device.

**Step 11-12:**  In these steps, the mobile device authenticates the MNO by decrypting the message EKC(RS||R) that it receives from the MNO. After decrypting using KC, if both the R and RS match between the mobile device and MNO, the MNO is authenticated as well, and a “successful authentication” message is sent to the MNO.

**Phase 2: Key Generation and PIN Verification**

**Step 13-14:**