NFC APPLICATION SECURITY

By Mr. Tan Keng Boon, Advanced Card Systems Ltd

Smart card application is closely related to security-one is able to perform a transaction offline without the need to rely on the expensive online infra-structure which does not necessarily operate as quickly.

Vendors develope the chip operating system (COS) with all the security taken into considerations, and together with the user manual and development tools to guide application developers into correct usage of the smart card-minimising the possible security loopholes.

The emergence of Java smart card entrusts a new responsibility of developing secured smart card application from the COS developer to the smart card application developer. Now, with the emergence of NFC phone, which has all the resources offered by a GSM phone but can be viewed as a dual - a "super smart card" and a personal contactless smart card terminal that also works as a mobile phone. There is a concern that while this trend draws more application developers into NFC applications, many may not know enough about smart card security. Without a good understand of smart card security and smart card application security, there comes a risk of security loopholes and pitfalls.

Security is something that few people know and think about until fraud occurs. A seurity oversight is a costly problem.

This paper attempts to list down the security principles and concepts used in smart card COS and smart card application securities design so that NFC application developers may be able to adopt to make the application more secured and reliable.

1. Internal Authentication

In a smart card application this is also known as smart card authentication. In an NFC application it verifies that the NFC phone is an authentic device. This is typically implemented by the external environment sending a random number to be encrypted by the target using the internal authentication key. The external environment can perform an encryption and if the result is the same, it implies that the target knows the authentication key and is therefore a genuine device.

2. External Authentication

External authentication allows a slave target to be able to authenticate the external world in return. This is done asking the target for a random number so that the external device can encrypt it with the external authentication key, and the result sent back to the target for verification. In the case of a smart card, the card becomes blocked after successive number (e.g. 3 times) of failed authentication.

3. Session Key For Secured Channel

After successful internal and external authentication a secured channel can be established using a session random session key to protect the data confidentiality (encryption) or integrity (MAC) during communication between the external device and the NFC phone. The session key is typically a combination of random number generated by the NFC phone and the external device. Obviously the exchange of the random number cannot be in plain (otherwise the session key is leaked) but is encrypted by the authentication keys (internal and external authentication key) on the random numbers and the complement of the random number, for example.

3.1 Session Key Usage - Non Replayable Data Integrity

The session key can be used to enforce data integrity against tampering using message authentication code (MAC) on the data to be protected. It must also prevent replay by using the previous MAC as the initial vector in the MAC computation..

3.2 Session Key Usage - Non Replayable Data Confidentiality

If data confidentiality is required, the session key can be used to implement data confidentiality by encrypting the data using the session key.

4. One Key For One Purpose

A security principle of key usage is that one key is only used for one purpose. The same principle is also adopted in our daily life e.g. the main door key, bed-rook key, wardrobe key and the safe key are all different. If the same key is used for multi-purposes, there can be a security weakness. Thus in the system there will be many keys - external authentication key, internal authentication key, session key for communication confidentiality and integrity, credit key, debit key, device transaction signature key etc.

5. Key Diversification

There are many devices in the system. Whenever possible key diversification is used so that the key in each device is unique. This can be achieved by using a master key and the device unique ID to derive a unique diversified key in each device.

6. Stored Value Security

Stored value function is going to be a very important of NFC application. It is therefore important to know the security requirements and considerations related to a stored value application. In a payment system there are a number of entities, including the purse holder, merchant, acquirer, purse provider and clearing house. These entities are different entities and in an electronic transaction processing system, trust should only be based on cryptography rather than just pure reliance on electronic data which can be tampered or faked easily.

6.1 Debit & Credit Access

Just like read and write access for a data file, a stored value access is about debit and credit access. A debit access is only able to reduce the balance in a stored value file and a credit access is able to increase the balance. The access right is only available after successfully authentication of the debit or credit key.

6.2 Blacklist Management

A payment system must has a blacklist management in place so that any fraudulent purse can be blacklisted. The blacklist must be up-to-date before the payment terminal can be operational.

6.3 Terminal Transaction Signature

The acquirer provides the payment terminal to the merchant and handle the transaction on behalf of the merchant. The acquirer will therefore need to ensure that transaction from the payment terminal has not been tampered and was not previously settled. Thus a terminal transaction signature protecting all details in a transaction record is required and this is generated by the payment device.

6.4 Debit Signature

Debit signature is a cryptogram that certifies that the transaction amount is indeed debited from the purse by the payment terminal. Technical speaking, the debit signature is an encryption of the transaction amount and terminal transaction signature by the debit signature key inside the purse. The stored value amount is simultaneously reduced when the debit signature is generated, in an atomic transaction.

6.5 Verification Of Debit Signature

The payment terminal must verify the debit signature in order to prevent fraudulent transaction.

6.6 Credit Certificate

At some point in time the stored value runs low and need to be topped-up. A NFC phone containing a stored value application is ideal as top-up can be done easier via the communication network. The security mechanism to perform a top-up requires a non re-playable credit certificate to be computed by the backend host computer after the corresponding top-up amount is debited. This credit certificate allows the top-up amount to be credited onto the purse.

6.7 Backend Audit

Because of the security offered by the front-end devices (e.g. smart card or NFC phone), transaction is able to be conducted offline, transaction batch uploaded so that the backend computer system can perform audit and clearance. In an unlikely event that a fraud is detected, the purse is blacklisted.

7. Key Renewal

In a smart card system keys in the smart card is never updated because it is quite impossible to get the cardholder back to have the keys updated. As a smart card is a limited life-span, the keys inside a smart card automatically retires when the card expires. Each year, smart cards are issued with a new set of master keys and hence the keys used in the system automatically renews. For a NFC phone, the keys renewal can adopt the same method.

Conclusion

Stored value function is going to be a very important of NFC application. NFC application developers have to know how to design the system security correctly, especially when the transactions are done offline. Developers need to understand both internal and external authentication on how to protect the data confidentiality or integrity during communication between the external device and the NFC phone.