3GPP TSG SA WG3 Security – S3#26 **S3-020625**

19 - 22 November 2002

Oxford, UK

Source: **GEMPLUS Card International**

Title: **Subscriber digital signatures require the use of smart cards**

Document for: **Discussion and approval**

Agenda Item: **T.B.D**

Abstract

In the scope of the Support for Subscriber Certificate Work Item, this input paper aims at requiring the use of smart cards in subscriber digital signatures management.

1. Introduction

Support for Subscriber Certificates Work Item was created in order to introduce digital signatures in mobile networks. The aim of this document is to show that the smart card is the unique component in the UE (User Equipment) able to deal with digital signatures in secure manner.

2. Required properties of digital signatures

To be valid, digital signatures require properties:

- Authenticity: a valid signature implies that the signer deliberately signed the associated message
- Unforgeability: only the signer can give a valid signature for the associated message
- Non-re-usability: the signature of a document can not be used on another document
- Non-repudiation: the signer can not deny having signed a document that has valid signature
- Integrity: ensure the contents have not been modified

2.1. Unforgeability and no-re-usability

Those two properties imply:

- The secrecy of the keying material,
- The use of strong and secure cryptographic algorithms (e.g. RSA, DSA or other).

So, those two properties require the storage of the keying material and the algorithms in a tamper resistant device protected against attacks. The smart card is a tamper resistant device containing hardware and software countermeasures to protect it against invasive attacks and logical attacks (fault attacks, power attacks, buffer overflows, malicious code

attacks, and ultimately cryptanalysis). The software applications, more and more submitted to Trojan horses and malicious programs, lack those protected mechanisms.

2.2. Non-repudiation

This property relies on the security of the whole system: if there is any way to attack the system a signer can repudiate a signature arguing that the system is not secure.

The security of the weakest link will determine the system's overall security level. When designing a secure system, the security of every component must be taken into account.

So, even if strong security mechanisms are defined to issue certificates and guaranty proof of possession, the non-repudiation property can be "defeated" if the storage of the private key is not secure.

The non-repudiation property requires the storage of the private keys and the execution of the cryptographic computation in a tamper-resistant device protected against attacks. The smart cards are designed to fulfil those requirements

Moreover, smart cards can perform on-board key generation. The on-board key generation feature reinforces the secrecy of the private keys since they never go outside the smart card. No one other than the cardholder can access the private signature key.

2.3. Authenticity

The active participation of the signer in the transaction must be ensured. This active participation can rely on two elements:

- The presence of the smart card owned by the signer
- The validation of a secret code known only by the signer (PIN code or password).

The PIN is a secret that shall be protected in the same way as the keying material; the PIN shall be stored in the smart card.

Conclusion

According to the required properties for digital signatures, the subscriber private keys and the cryptographic computations related to digital signatures shall be managed by the smart card.

3. The signer is the cellular subscriber

In the proposed usage scenarios for subscriber certificates (e.g. S3-020077), the signer is the cellular subscriber. User signatures are the proofs that the cellular subscriber accepted a proposal, an invoice.

Now, in the cellular infrastructure, the physical component representing the cellular subscriber is the smart card, used to deal with sensitive and personal data of the subscriber. So, the operations related to digital signatures, involving the responsibility of the subscriber, shall be executed by the smart card.

Moreover, the smart card allows the subscriber to generate digital signature independently of the device.

4. Conclusion

The smart card, tamper-resistant device protected against attacks and representing the cellular subscriber, is the unique component in the User Equipment able to deal with digital signatures in secure manner.

To take this into account, a security requirement has to be added in the SA3's document issued in the scope of the Support for Subscriber Certificates Work Item.
Security requirement: the subscriber private keys and the cryptographic computations related to digital signatures shall be managed by the UICC.