3GPP TSG SA WG3 Security – S3#29 **S3-030382**

15 - 18 July 2003

San Francisco, USA

Source: **Gemplus**

Title: **Generation and storage of the UE's public/private key pair associated to the requested certificate**

Document for: **Discussion and decision**

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

Abstract

This input paper aims at adding in the SSC TS some security requirements on the generation and the storage of the UE's public/private key pair associated to the requested certificate.

1. Introduction

The TS addressing SSC WID has to deal with the generation and the storage of the UE's public/private key pair associated to the requested certificate.
At SA3#28 Berlin Meeting Gemplus proposed to add some requirements on the generation and the storage of the UE's public/private key pair associated to the requested certificate. This input paper highlights the consequences of generation and storage of the UE's public key pair in the terminal.

2. Digital signatures

2.1. Required properties of digital signatures

Digital signatures require several properties to be valid: authenticity, unforgeability, non-re-usability, non-repudiation, and integrity. Those proprietaries involve the secrecy of the keying material and the use of strong and secure cryptographic algorithms.

At SA3#26 Oxford meeting, Gemplus presented S3-020625 contribution highlighting that the smart card, tamper-resistant device, is the unique component in the User Equipment able to deal with digital signature. The subscriber private keys and the cryptographic computations related to the signatures shall be managed by the smart card. Moreover, the UICC on-board key generation guaranties that nobody can access the private key. SA3 agreed on those principles.

The mechanisms related to the on-board key generation and the storage on the UICC do not need to be specified since there are already defined in the WIM specification standardized by OMA.

In the context of the Support for Subscriber Certificates work item, if the generation of the UE's public/private key pair associated to the requested certificate and the storage of the private key are not performed in the smart card, then there is a low level of security. So, the required properties for digital signatures are not satisfied. The issued subscriber certificates cannot be used to deal with non-repudiable digital signatures

Conclusion:
The smart card is necessary for the generation and the storage of the UE's public/private key pair.

The following chapter presents the consequences due to a low level of security.

3. Consequences due to low level of security

The absence of security requirements on the generation and the storage of the UE's public/private key pair implies the following consequences:

3.1. Low level of trust

A low level of security implies a low level of trust with the following consequences:

1. Only short-lived certificate

The issuance of long-term certificates requires more security constraints on the public/private key pair than the issuance of short-lived certificates.
Without a tamper-resistant device to store the user private key pair, long-term certificates should not be issued.
The absence of long-term subscriber certificates will prevent the subscriber from accessing services only dealing with long-term certificates.

2. High valued service not allowed

High valued services mandate non-repudiable digital signatures. The non-repudiation property is not reached without storage of the private key and secure cryptographic computations managed by the smart card.
So, with a low level of security, the issued subscriber certificate could not be used to access high valued services.

3. No guaranty of security for a Service Provider

A Service Provider is interested in having a high level of trust in the user. Without non-repudiable digital signatures the Service Provider has no guaranty of security.

4. Risk to destroy the PKI initiative

If any problem should come from allowing a low level of security for the generation of the public/private key pair and the storage of the private key then this may impact the image of the 3G PKI, the trust in PKI may be lost. It could kill the initiative to introduce PKI in mobile environment. Moreover, a low level of trust decreases the interest in PKI.

3.2. Upgrade of the system

If the first step of the PKI allows the generation and the storage of the key pair in the terminal there will be the following issues:

1. Complexity

There will be applications dealing with subscriber private keys in the terminal or in the smart cards, public/private key pair generation in the terminal or in the smart card. It will introduce complexity.
Examples of questions we would have to face concerning the private key storage (same questions about the on-board key generation):

- How to select between a storage on the terminal or on the smart card
- Who does decide where the storage of the private key takes place?
- How to prove that the private key is stored on the smart card rather than on the terminal
- Does the storage have to be in the same device than the on-board key generation?

This complexity does not provide a higher level of security.

2. Backward compatibility of the terminal

The terminals could need to implement new functionalities, there will be backward compatibility issue.

3.3. Issue related to portability

If the public/private key pair of a subscriber is stored on the mobile there is a problem in case of a new UICC inserted in the terminal. There will be on the mobile personal and sensitive data that do not belong to the new user.

Conclusion:
The generation and the storage of the UE's public/private key pair in the terminal raises security issues.

4. Usage of the issued subscriber certificates

A means of solving some of the issues could be to have more information on the usage of the subscriber certificates.
What will be the applicative environment to use the issued certificates? What are the associated protocols, mechanisms? Do 3GPP envisage specifying new protocols?

5. Conclusion

There are many issues if the generation and the storage of the UE's public/private key pair associated to the requested certificate are not managed by the UICC.

We kindly ask SA3 to take into account this analysis and to add in the SSC TS some security requirements mandating that the generation and the storage of the UE's public/private key pair associated to the requested certificate shall be managed by the smart card.