3GPP TSG-SA-WG3 Meeting #31
18th – 21st November 2003, Munich, Germany

Tdoc ⌘S3-030795

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.221 CR CRNum ⌘rev** ⌘ Current version: ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Results of risk analysis in the "Key Pair Storage" informative annex
Source:	⌘	Gemplus, Giesecke&Devrient, Oberthur, Schlumberger
Work item code:	⌘	Support for subcriber certificates
Date:	⌘	08/11/2003
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The content of the section on "Results of risk analysis" is missing since the current version of this annex corresponds to non controversial text after an email discussion.
Summary of change:	⌘	Completes the section "Results of risk analysis"
Consequences if not approved:	⌘	The content of the section on "Results of risk analysis" section is missing.

Clauses affected:	⌘	Key Pair Storage informative annex

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

Annex <A> (informative): Key pair storage

A.1 Introduction

The storage of the public/private key pair associated to the requested subscriber certificate is relevant to the procedure of issuing subscriber certificates.

The key pair storage can be performed in different ways. The nature of this storage may have impacts on the trust level associated to the subscriber certificates.

This annex provides a key pair storage security risk analysis in different scenarios.

A.2 Key pair storage use-cases

There are different scenarios to store the public/private key pair associated to the requested subscriber certificate.

A.2.1 Key pair storage on the ME

A possible place for the storage of the key pair is the Mobile Equipment.

The extension of the scope of the subscriber certificates outside the cellular domain to SIMless terminal introduces two alternatives for the key pair storage on the ME: key pair storage on the MT or on the TE.

A.2.2 Key pair storage on the UICC

Another solution for the storage of the key pair is the UICC.

For the following study we will consider only two key pair storage use-cases: on the ME or on the UICC.

A.3 Threats associated with the key pair

A.3.1 Key pair generation

The key pair generation is a very sensitive operation for the secrecy of the private key. The key pair generation has to be of good quality and the exchange, between the device where the key pair generation took place and the device where the key pair will be stored, has to be protected to avoid private key cloning/disclosure. UICC provides a greater level of protection, compared to ME, against unauthorized access to the private key itself.

A.3.2 Unauthorized usage of the private key

There are two kinds of threats associated with unauthorized usage of the private key:

1. An attacker getting hold of the private key, and
2. An attacker using the private key of the victim without getting hold of that key.

With respect to threat 1, having the key in UICC offers better protection than having it in the ME. However, an attacker who can compromise the ME can possibly *use* the private key for unauthorized purposes even if it is in the UICC because the UICC does not have direct trusted path to the user.

Attacks due to threat 2 always require an interaction with the UE to gain access to the UICC. While with the threat 1, as soon as the key is retrieved, the associated attacks do not requires any intereaction with the UE to use the retrieved private key.

A.3.3 Portability

If the key pair is stored on the Mobile Equipment there is a threat in case of a new UICC inserted in this ME. There will be on the ME personal and sensitive data that do not belong to the new user. Since access to private keys is protected by PINs or passwords, the new user cannot access the private key of the old user unless he knows the PIN or the password.

Also, an important aspect of enrolling subscriber certificates based on AKA is the use of short-lived certificates. With short-lived certificates, even if the new user can access the old user's private key, it could happen that he cannot masquerade as the old user in authorization transactions because he can no longer get subscriber certificates for the key pair on behalf of the old user if the subscriber certificate expired. Moreover, if the key pair in ME is short-lived, owner of the new UICC will not be able to use that key pair after the pair expires. But there is no assumption that the subscriber certificate/key pair expired when the new user gets access to the old user's private key. In general, short-lived keys – on UICC or on ME – are useful for identity and privacy protection. Frequent change of key pair prevents outsiders from linking together transactions made by same user.

A.3.4 Environment

The threats to the key pair depend on the environment, the place of the key pair storage.

All implementations on mobile terminal, PC, MAC or PDA leave potential risks such as the possibility to load Trojan horses, worms or virus. Software applications lack the protective mechanisms existing in smart card (tamper resistance, physical encapsulation of critical circuitry). Reverse engineering techniques, such as extracting program code and disassembly/debugging methods, are simplified greatly in a software environment, allowing a token's secret components such as cryptographic algorithms, private keys, and other assumed secure information to be recovered.

Currently, the Mobile Equipments do not have all the hardware and software countermeasures that are built into UICC to protect them against invasive and non-invasive attacks performed to retrieve secrets. But mechanisms lide code signing are already being taken into use.

A.3.5 Threat to the required properties for digital signatures

To be valid, digital signatures require the following 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

Those properties involve the secrecy of the keying material, having a trusted input/output path to the user, and the use of strong and secure cryptographic mechanisms.

So, the trust in the digital signatures depends on the storage of the key pair and the related cryptographic computations and the security of communication between the user and the module performing private key operations. The impacts of the key pair storage are studied in the following chapter.

A.4 Security risk analysis related to key pair storage

There are many different subscriber use-cases describing the range of applications or services utilizing subscriber certificates. But, the level of trust associated to the proposed services depends on the key pair storage. This will be presented in the following security risk analysis.

A.4.1 Subscriber certificate use-cases

The use-cases for subscriber certificates can be divided into 2 main categories:

A.4.1.1 Secure services

Those services provide convenient way of authenticating cellular subscribers to services. These services can be provided by cellular operators, corporations, or 3rd party content providers. Secure services may also support billing.

The different subscriber use-cases could be:

- Person-to-person authentication: per-to-per authentication
- Corporate services: authentication to corporate intranet applications.
- Person-to-content
    - Access to Presence services
    - Self-service management
    - Access to operator's Web services
    - Access to 3rd party content services
    - Enhanced LCS privacy
    - Notifications through cellular network
    - MBMS security
    - Support of Liberty Alliance use cases
- Small to medium payment through cellular operator

A.4.1.2 Secure connectivity

This service utilizes cellular infrastructure and existing operators customer relationships to authenticate users:

- Alternative access authentication
    - Corporate WLAN access authentication
    - Broadband access, e.g. DSL or cable access
- Service authentication: e.g. VPN authentication

A.4.2 Security risk analysis in some scenarios

All subscriber use-cases do not require the same level of security for the key pair storage since they propose services that have different features in terms of:

- Added value: high or low valued services
- Involved partners and trust relationships: there is agreement between different cellular network operators or between cellular network operator and service provider or 3rd party content provider
- Type of required certificates (short-lived or long-term certificates)

This section presents some scenarios where the nature of the key pair storage has security impacts on the service.

A.4.2.1 Scenarios involving subscriber's personal data

An example of scenario involving subscriber's data could be the self-service management.

A.4.2.1.1 Self-service management

This scenario allows user to authenticate to a Web portal, run by operator, to achieve secure access for self-provisioning. Secure end-to-end (TLS) tunnel from the terminal to the Web portal can be established (subscriber's private key and the certificate are used in standard fashion, i.e. no changes needed in TLS components). The user can have either mobile or fixed network access (e.g. GPRS, WLAN, or xDSL). The main use cases are billing information queries and modifying one's subscription profile.

User experience:
The authorization may be based directly on subscriber certificates, or on a combination of authentication with subscriber certificate and access control list in the Web portal. In the first case the self-management server

- Receives an assertion signed by the data owner, which contains a public key and set of access rights,
- Verifies that the sender of the assertion holds the matching private key and
- Allows the secure access (e.g. TLS connection) only if the verification succeeds

A.4.2.1.2 Security Risk Analysis in this scenario

The security risk analysis is performed according to the unauthorized usage threats identified in A.3.2 section.

Unauthorized usage by using the private key of the victim without retrieving the private key

- Potential attack:
  So, an attacker could get usage of the subscriber private key to authenticate to the Web portal and access for self-provisioning. The attacker could for example modify the subscription profile of the subscriber.

- Feasibility
  The attacker requires an interaction with the UE to gain access to the UICC.
  The attack applies in case of:
  - Key pair storage on the ME
  - Key pair storage on the UICC

Unauthorized usage by getting hold of the private key

- Potential attack:
  So, an attacker could retrieve the subscriber private key to authenticate to the Web portal and access for self-provisioning. The attacker could for example modify the subscription profile of the subscriber.

- Feasibility
  Once the key retrieved, the attacker does not require any interaction with the UE equipment to gain access to the UICC.
  The attack applies in case of:
  - Key pair storage on the ME
    This attack is based on the key retrieval. So, as the UICC is tamper resistant device so the attack does not apply to UICC.

Consequences of these attacks

The self-service management is low added value and the consequences of the key pair storage on the UE are limited.

A.4.2.2 Scenarios involving payment and agreement between operator and service provider

Some scenarios deal with payment and agreement between cellular network operator and service provider, 3rd party.

A.4.2.2.1 Notifications through cellular network scenario

The subscriber authorizes the operation of sending notifications by service provider through the cellular network. The service provider does not need to know subscriber's identity. If there is no identity information in the certificate, then the subscriber may remain anonymous towards the service provider. However, subscriber may pay for the notification

through his phone bill. Subscriber authorizes such payment and the charging is triggered when the service provider sends a notification.

User experience:
During a transaction UE sends to the service provider an assertion, i.e. signed authorization, to send a notification message to that UE through the cellular network, and subscriber certificate or subscriber certificate URL. The service provider verifies the authorization text and UE's signature with the aid of subscriber certificate. If the signature and the authorization text are correct, then the service provider will send a positive acknowledgement to the UE.
At a later time, for example when a certain sport's event takes place, the service provider creates a notification and submits it to the operator together with the signed UE's authorization and subscriber's certificate. The operator verifies the signed authorization. If the verification succeeds the operator will forward the notification text to the subscriber in an SMS or MMS message.

A.4.2.2.2 Small to medium payment through cellular operator scenario

The subscriber authorizes payment for a service through his phone bill (or with separate bill). Note that the provider of the service does not need to know subscriber's identity. If there is no information in the certificate, then the subscriber may remain anonymous towards the service provider. The service may be e.g. non-cellular access in a environment where the operator's traditional billing mechanisms are not directly applicable, e.g. non-cellular access is provided by 3rd party.

During a payment transaction the UE sends to the service provider a signed invoice and subscriber certificate (or subscriber certificate URL). The service provider verifies the UE's signature with the aid of subscriber certificate. If the signature and the invoice are correct, then the service provider will grant UE access to, or deliver the requested service.

In the settlement phase the service provider forwards the signed invoice to the operator for verification. If the verification is successful then the operator will reimburse service provider and charge the subscriber the price of the service through his phone bill (or with separate bill).

Prerequisite:
The service provider has a business relationship with operator that issued subscriber's certificate and it knows operator's signature verification key.
If the service provider (e.g. visited access network provider abroad) does not have a direct relationship with the subscriber's home network, the certificate should come from the visited network. The independent access network provider trusts the visited operator as well as the subscriber authentication and certificate from that operator.

User experience:
The subscriber trusts the billing from the home operator and payment is convenient. During the service usage he will have to type in the payment PIN for configured amounts. The terminal may automatically sign very small amounts. In this case only larger amounts and cumulative sum above a threshold trigger the PIN query.

A.4.2.2.3 Security Risk Analysis in these scenarios

These secure services deal with payment and an agreement between a cellular network operator and a service provider. The nature of the key pair storage has consequences. The security risk analysis is performed according to the unauthorized usage threats identified in A.3.2 section.

Unauthorized usage by using the private key of the victim without retrieving the private key

- Potential attacks:
  If the ME is not sufficiently secure, the attacker may have a program that shows the user a certain message ("payment of €1") but ask the UICC to sign a different message ("payment of €100). Also if the attacker's program discovers the PIN, it can command the UICC to generate signatures even without the user being aware of it.

- Feasibility
  The attacker requires an interaction with the UE to gain access to the UICC.
  These attacks apply in case of:
    - Key pair storage on the ME
    - Key pair storage on the UICC

Unauthorized usage by getting hold of the private key

- Potential attacks:
  If an attacker manages to discover the subscriber's private key then an attack could consists in sending signed authorizations to the service provider, then the subscriber would have to pay for services he did not ask for.

- Feasibility:
  Once the key retrieved, the attacker does not require any interaction with the UE equipment to gain access to the UICC.
  The attack applies in case of:
    - Key pair storage on the ME

  This attack is based on the key retrieval. So, as the UICC is tamper resistant device so the attack does not apply to UICC.

Consequences of these attacks

- Forgeability: the subscriber could pay for services he did not ask for.

- Repudiation: The cellular network operator and the service provider are not paid for the service they provided.

  If there is any way to attack the system a signer can repudiate the performed signatures arguing that the system is not secure. So, if it is possible to use the subscriber's private key without his deliberate consent, then the subscriber can repudiate the signatures sent for authorization, and not pay the associated phone bill. So,

  - The operator and the service provider could not be paid for the proposed service
  - The trust relationship between the operator and the service provider can be destroyed. The service provider has no guaranty of security, he would no longer trust the subscriber certificates issued by the cellular network operator and the associated signatures

- If there is any problem due to some unauthorized usages of the subscriber private key then the trust in 3G PKI may be lost.

- High valued services involving payment and relationship with service provider or 3rd party content provider often require the use of long-term certificates. The issuance of long-term certificates requires more security constraints than the issuance of short-lived certificates. So, according to the unauthorized usage threats present on the UE, the security level may not satisfy the security requirements for long-term certificates issuance and usage

A.4.3 ~~Results~~ Summary of risk analysis

To prevent the identified unauthorized usages of the private key the following ~~requirements~~ recommendations need to ~~shall~~ be addressed:

- The storage of the private key and the related cryptographic computations ~~shall~~ to be done in ~~the most~~ a secure manner
- The solution ~~shall~~ should provide a secure path to the private key usage

~~It is agreed that~~ The UICC provides the most secure location for storage and usage of the private key in terms of security (in the form of, e.g. the WIM application). This does not preclude the use of other locations for certain services. On the other hand, the ME can provide a secure path to using the private key (e.g. with mechanisms such as code signing). The combination of solutions will provide a complete secure solution and enable the deployment of secure services.