3GPP TSG SA WG3 Security – S3#20 **S3-010499**

15-18 October, 2001

Sydney, Australia

3GPP TSG SA WG3 Security — S3#19 **S3-010353**

3 - 6 July, 2001

Newbury, UK

3GPP TSG SA WG3 Security — S3#17 **S3-010040**

27 February - 02 March, 2001

Gothenburg, Sweden

3GPP TSG SA WG3 Security — S3#16 **S3-000709**

28-30 November, 2000

Sophia Antipolis, France

Source: **Gemplus, Oberthur Card Systems**

Title: **USIM functionalities to support PKI architectures**

Document for: **Discussion**

Agenda Item:

In S3-010353 and in two previous input papers, NOKIA mentioned a lack of a large-scale infrastructure to authorize and charge mobile users for new services. The basic need is to allow authenticated and possibly encrypted channels between clients and network external entities.

In order to fill this gap, NOKIA proposed to rely on and to take advantage of the AKA channel that naturally exists between a mobile client and its public land mobile network (PLMN), and building on that, provide an operator driven public key infrastructure .

This input paper aims at proposing a pertinent way of realizing NOKIA's proposal. We proceed by means of an extended use of the USIM application. More precisely, we propose to perform security functionalities needed to support this architecture inside the USIM. Furthermore, we argue on the necessity to locate these features in the USIM.

1. Technical Proposal

As pointed out by NOKIA, there is a need to equip mobile clients with generation of cryptographic asymmetric key pairs. These keys are used first to sign the certificate request and later on to sign the service requests.

We propose to generate the key pairs on-board the card, keeping the private key securely stored in the card, and to perform the signatures in the card with this resident private key.

We further propose to store the certificates and/or links to these certificates in the USIM.

Optionally, the USIM can manage the certificates life cycle (set-up, verification, revocation, deletion, upgrading).

We propose the following ad-hoc functions:

`GenerateKeyPair()`, **`SignText()`**, **`VerifySignature()`**, **`VerifyCertificate()`**, **`SetUpCertificate()`**,**`RevokeCertificate()`**,**`UpGradeCertificate()`**, **`DeleteCertificate()`**.

2. Arguments

We focus on the advantages of proposing security services in the UICC.

- **Tamper-resistance**: UICC is clearly identified as the privileged tamper-resistant part of the mobile client. Therefore, we find it mindful to generate asymmetric key pairs on board the card, to keep their private part on board, and to export a properly signed copy of their public part to an external entity ;

- **Coherency with other works**: such functions as SignText are in line with the Wap Forum working assumptions ;

- **Maturity of on board asymmetric key pair generation (OBKG)**: this technology is mature and can be deployed on a large scale ;

- **UICC as an active cryptographic device**: public key signature production and verification algorithms have been available on board smart cards for quite a long time;

- **High storage reliability**: due to smart card high quality memory management, there exists active integrity checks in the card memory. It turns out that smart card operations are naturally atomic.

- **Strong USIM-Operator link**: the AKA is an obvious operator-USIM link and is the base of the system proposed by Nokia. There, the operator is responsible for the management of the PKI, especially the CA part; to ensure end-to-end security in the system, the keys have to be generated and authentified in the security domain of the operator. The obvious candidate on the client side is then the USIM.