3GPP TSG SA WG3 Security — S3#21 **S3-010638**

27 - 30 November, 2001

Sophia Antipolis, France

Work Item Description

Title: Support for subscriber certificates

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

3 Justification

Digital signatures are the best way to secure mobile commerce, service authorization and accounting. But digital signature by itself is not enough: we need a global support for authorization and charging. The simplest way to introduce digital signatures in mobile networks is to make use of infrastructure that exists in those networks. Thus, we shall use global and secure authorization and charging infrastructure of mobile networks to support local architecture for digital signatures.
Subscriber certificates provide a migration path towards global Public Key Infrastructure (PKI). On the one hand, operators and service providers don't have to wait for a world - wide PKI to benefit from public key technology. Local architecture for digital signatures can be deployed incrementally; an operator can choose to deploy independently of the others. On the other hand, the existence of subscribers and service providers that use digital signatures makes it easier to build global PKI.
The concept relies on the authentic signaling between mobile terminal and serving network and thus has to be standardized. The terminal and the serving network can interact only over standardized interface. This is in scope of 3GPP.

4 Objective

To make it possible to issue subscriber certificates in 3GPP systems in order to authorize and account for service usage both in home and in visited network. This requires specification of:

1. Signaling procedures to issue temporary or long-term certificates to subscribers.
2. Standard format of certificates and digital signatures.

5 Service Aspects

Subscriber certificates support services whose provision mobile operator assists, as well as services that mobile operator provides. There is no need to standardize those services. Also, the communication between service provider and the operator (in the role of certificate issuer) need not be standardized.

6 MMI-Aspects

User experience in receiving certificates and signing transactions should be consistent. There should be a clear distinction between e.g. browsing and creating a digital signature.

7 Charging Aspects

Operator may convert digitally signed transaction records into CDRs. However, there is not necessarily any need to modify CDR structure or 3G charging mechanism.

8 Security Aspects

This is a security work item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes	X	X		X	
No			X		
Don't know					X

10 Expected Output and Time scale (to be updated at each plenary)

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102		Adding signaling procedure for certificate requests	SA#15	
33.102		Adding a format of certificates	SA#15	

11 Work item raporteurs

Valtteri Niemi, Nokia

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Nokia, Orange, Qualcomm, Gemplus, Telenor (?), Oberthur (?), BT (?), FT (?)

14 Classification of the WI (if known)

	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)