3GPP TSG SA WG3 Security — S3#22 **S3-020185**

14 - 17 May 2002

Victoria, Canada

3GPP TSG-SA5 (Telecom Management) **S5-022008**
Meeting #27, Cork, IRELAND, 2 - 5 April 2002

Title:	**Reply LS on "support for subscriber certificates" from SA3 (S3-020163)**
Source:	**SA5**
To:	**SA3, SA1**
CC:	**CN1, CN4, T2, T3**
Contact:	**dave.milham@bt.com**
Attached:	**updated WID of "Support of subscriber certificates" (S3-020163)**

S5 note the above communication and have agreed to handle subscriber certificates requirements as proposed by S3 as part of its activities on the definition of specification for User Equipment Management and Subscription Management.

3GPP TSG-SA5 (Telecom Management) **S5-020313**
Meeting #27, Cork, IRELAND, 2 - 5 April 2002

Agenda Item: 4.4

3GPP TSG SA WG3 Security — S3#22 **S3-020163**

25 - 28 February 2002

Bristol, UK

Source:	**S3**
To:	**S1**
CC:	**CN1, CN4, SA5, T2, T3**
Title:	**Reply LS on support for subscriber certificates**
Contact:	Valtteri.Niemi@nokia.com
Attached:	updated WID of "Support of subscriber certificates" (S3-020153)

S3 thanks S1 for their LS S1-020645 (=S3-020120) and their effort on identifying potential use cases for subscriber certificates in 3GPP systems.

The following action was requested from S3:

" SA1 asks SA3 to identify where the requirements for *Support for subscriber certificates* are defined. SA3 should consider how the above usage could be co-ordinated in such a way that it will allow cost efficient implementation of the security support of the UE, a 3GPP UE “security toolbox”.

The basic requirement for the feature is defined already in the WID: " 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."

Support for subscriber certificates is a capability rather than a service and it will be used as a tool when mechanisms are specified to meet security requirements associated to various 3GPP work items. In this light, the following approach of S1 is appreciated: " SA1 currently makes no formal requirements in its technical specifications (i.e. TS 22.xxx) for the explicit support of subscriber certificates. It is considered by SA1 that potential use of subscriber certificates is a Stage 2/Stage 3 matter, and that SA1 only generates requirements which other working groups in turn could potentially support through the use of subscriber certificates."

The need to allow a cost efficient implementation of the security support of the UE is acknowledged by S3 and the work item description is updated based on the studies and advice from S1.

3GPP TSG SA WG3 Security — S3#22 **S3-020162**

25 - 28 February, 2002

Bristol, UK

(Updated) Work Item Description

Title: Support for subscriber certificates

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

Potentially: MMS, DRM, OSA, GUP, LCS

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 signalling 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. Signalling procedures to issue temporary or long-term certificates to subscribers.
2. Standard format of certificates and digital signatures, e.g re-using wireless PKI.

The mechanism shall allow a cost efficient implementation of the security support of the UE. It will also enable a user anonymity towards the service, whilst the user invoking the service can be identified by the network.

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.
The following services are identified which could potentially use subscriber certificates (not an exclusive list): Multimedia Message Service (MMS), Digital Rights Management (DRM), Open Service Architecture (OSA), Generic User Profile (GUP), Location services, Presence, Push, services provided by VASPs. Also, access by alternative access technologies could be secured using subscriber certificates.

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
						See comment below

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102		Adding signalling procedure for certificate requests	SA#17	A new TS may be created instead of CRs if found more appropriate
33.102		Adding a format of certificates	SA#17	'' ''

11 Work item raporteurs

Valtteri Niemi, Nokia

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Nokia, Orange, ~~Qualcomm,~~ Gemplus, Telenor, Oberthur, BT Group, Motorola

14 Classification of the WI (if known)

X	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

None at present. This may require BBs from CN1, CN4, SA5 and T3.

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)