

Source: CN4
Title: Updated WID: Support for subscriber certificates, stage 3
Document for: Approval
Agenda Item: 9.3

Work Item Description

Support for subscriber certificates, stage 3

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

- SA3: Support for subscriber certificates [\(33002\)](#)

3 Justification

SA3 is working on Bootstrapping and Subscriber Certificates procedures. There are two interfaces for Bootstrapping: UE-BSF interface [Ub](#) and BSF-HSS interface [ZhBb](#). There are two interfaces for Subscriber Certificates procedures: UE-NAF interface [Ua](#) and NAF-BSF interface [ZnBa](#).

The interfaces [ZhBb](#) and [ZnBa](#) are based on re-usage of 3GPP IMS MM Diameter based messages. The stage 3 usage of this protocol platform is not in the scope of SA3, but is in the scope of CN4.

[The Bootstrapping interface Ub and the Subscriber Certificate interface Ua is in the scope of CN1.](#)

[Other changes to CN1 specifications due to the Generic Authentication Architecture are FFS.](#)

4 Objective

The objective of this Work Item is to create a 3GPP stage 3 technical specification documents.

- ~~TS 29.109xxx~~ that specifies how the 3GPP IM MM Multimedia-Auth-Request/Answer message pair is used in Bootstrapping [ZhBb](#) interface and [Network Application Function Subscriber Certificates ZnBa](#) interface and the corresponding application logics in BSF, HSS, and NAF.
- [TS 2x.xxx that specifies how the messages are used in the Ub \(Bootstrapping\) interface and the Ua \(Subscriber Certificates\) interface together with the corresponding application logics in UE, BSF and NAF.](#)

The stage 2 description of the Bootstrapping and Subscriber Certificate procedures belongs to SA3 TS.

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

No charging aspects behind that are defined in SA3 TS.

8 Security Aspects

This is a security work item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		<u>X</u>		X	
No	X	X	X		
Don't know	<u>X</u>				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
29.109** *	Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Protocol details Bootstrapping and Subscriber Certificates Diameter protocols, stage 3	CN4		CN#23 2	CN#24 3	
2x.xxx	Bootstrapping and Subscriber Certificates protocols, stage 3	CN1		CN#23	CN#24	Note 1
Affected existing specifications						
Spec No.	CR	Subject		Approved at plenary#	Comments	
23.008		For completeness a reference to the new information element in HSS for Generic Authentication Application profiles (e.g. Subscriber Certificate profile) Subscriber Certificate profile must anyhow be added both in text and summary table.			This upgrading is only editorial additions.	

Note 1: [The complete set of changes to CN1 specifications, including names and contents of possible new and existing TS\(s\) are FFS.](#)

11 Work item reporters

Lauri Laitinen
Nokia Corporation
lauri.laitinen@nokia.com
Tel. +358718036551

12 Work item leadership

CN4

13 Supporting Companies

Nokia, Lucent, Siemens, Alcatel

14 Classification of the WI (if known)

	Feature (go to 14a)
X	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)

SA3: Support for subscriber certificates ([unique id. 33002](#))

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

(one Work Item identified as a building block)