Technical Specification Group Services and System Aspects **_TSGS#17(02)0558_**
Meeting #17, Biarritz, France, 9-12 September 2002

Source: **SA1**

Title: **Release 6 CR to 22.105 on subscriber certificates**

Document for: **Approval**

Agenda Item: **7.1.3**

SA Doc	Spec	CR	Rev	Phase	Cat	Subject	Old Vers	New Vers	SA1 Doc
SP-020558	22.105	039		Rel-6	B	CR to 22.105 on subscriber certificates	5.2.0	6.0.0	S1-021782

3GPP TSG-SA-1 Meeting #17
Durango, USA, 12-16 August 2002

Tdoc ⌘S1-021782
Agenda 5.1.1

CR-Form-v7

CHANGE REQUEST

⌘	**22.105**	**CR**	**039**	⌘ **rev**	**-**	⌘	Current version:	**5.2.0** ⌘

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⌘ ☒ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Subscriber Certificates		
Source:	⌘	SA1 (Nokia, Openwave)		
Work item code:	⌘	Subscriber certificates	***Date:*** ⌘	13/08/2002
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:	⌘	SA1 highlevel service requiremetns on Subscriber Certificates (SA3 WI).
Summary of change:	⌘	Reference, brief explenation and new requiremetns added. (New chapter 11)
Consequences if not approved:	⌘	SA1 requirements missing.

Clauses affected:	⌘	2.1 and 11				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	33.102
				Test specifications		
				O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

2.1 Normative references

[1] 3GPP TS 22.001: "Principles of circuit telecommunication services supported by a Public Land Mobile Network (PLMN)".

[2] 3GPP TS 02.002: "Circuit Bearer services supported by a Public Land Mobile Network (PLMN)".

[3] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)".

[4] 3GPP TS 22.004: "General on supplementary services".

[5] 3GPP TS 22.038: " SIM toolkit Stage 1".

[6] 3GPP TS 22.057: "Mobile Execution Environment (MExE); Service description; Stage 1".

[7] 3GPP TS 22.060: "General Packet Radio Service (GPRS) stage 1".

[8] 3GPP TS 22.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL); Service definition - Stage 1".

[9] 3GPP TS 22.101: "Service principles".

[10] 3GPP TS 22.121: "Virtual Home Environment (VHE), Stage 1".

[11] 3GPP TS 22.135: "Multicall, stage 1".

[12] 3GPP TS 33.102: "3G Security, Security Architecture".

2.2 Informative references

[12] ITU-T Recommendation F.700: "Framework recommendation for audio-visual/multimedia services".

11 Certificates

Certificates may be used for a global scale authorization infrastructure for various applications and services based on the 3GPP system security architecture. Services may be provided by parties that are not necessarily trusted by the cellular operators nor by cellular subscribers. Therefore technical means to securely deliver and authenticate services from other parties are necessary. For 3GPP, only the certificates issued by operators are relevant. There are two types of such certificates: subscriber certificates are issued to cellular subscribers and operator CA certificates are self-signed or issued to other operators. Issuing subscriber certificates allows operators to offer authorization and accounting of other services. Operator CA certificates obtained via a trusted channel can be used as root certificates.

In addition to these certificates, there are other types of certificates. For example, service provider certificates (provided by service providers), and third party certificates (provided by third parties, e.g. Value Added Service Providers) etc. These certificates are described and standardized by other fora such as IETF PKIX working group and WAP forum.

Authorization of such services may be based on credentials like digital signatures. The service provider and the network operator shall use subscriber certificates to verify these credentials. The UE may also use operator CA certificates and other certificates to verify the credentials supplied by service providers and third parties. Operator-issued certificates in 3GPP must be such that they are compatible with other systems that allow the storage, selection, and use of certificates (e.g., WAP, LCS).

Example usage scenarios of the subscriber certificate feature are payment via subscriber phone bill and location information offered by the operator to other service providers. It should be noted that the service using this feature may be outside of scope of 3GPP or implemented using existing 3GPP toolkits.

The 3GPP system shall provide support for issuing certificates to the UE over the authenticated network connection. This feature shall be based on existing 3GPP system security principles and mechanisms as far as possible. The certificate management procedures must be authenticated and integrity-protected. It shall be possible to issue certificates for service usage both in the home and visited networks. It should be possible for the home operator to exercise control over service usage in the visited network.

For further information on certificates see TS 33.102[12].