TSGS#24(04)0394

Source: **SA WG3 (Security)**

Title: **CR to 33.310: Removal of unnecessary restriction on CA path length (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Workitem
SP-040394	33.310	002	-	Rel-6	Removal of unnecessary restriction on CA path length	F	6.0.0	S3-040267	SEC1-NDS-AF

3GPP TSG-SA WG 3 Security Meeting #33
Beijing, China, 10-14 May 2004

Tdoc ⌘S3-040267

CR-Form-v7

CHANGE REQUEST

⌘ **33.310** **CR** **002** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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 **X**

Title:	⌘	Removal of unnecessary restriction on CA path length
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-AF
Date:	⌘	30/04/2004
Category:	⌘	**F**
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:	⌘	The specification in section 6.1.2 that the path length of the CA certificate should be at least 2 is unnecessarily restrictive since a path length of 1 would also be acceptable. In fact it should be possible to specify a path length of 1 in deployments to improve security.
Summary of change:	⌘	Change the path length of the CA certificate to "unlimited or at least 1".
Consequences if not approved:	⌘	Unnecessary restriction in the specification which could result in a lower level of security.

Clauses affected:	⌘	6.1.2

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

⌘

Other comments: ⌘

6.1.2 CA Certificate profile

In addition to clause 6.1.1, the following requirements apply:

- The RSA key length shall be at least 2048-bit;
- Extensions:
  - Optionally non critical authority key identifier;
  - Optionally non critical subject key identifier;
  - Mandatory critical key usage: At least keyCertSign and CRL Sign should be asserted;
    - Mandatory critical basic constraints: CA=True, path length unlimited or at least ~~2~~1.