TSGS#24(04)0395

Source: **SA WG3 (Security)**

Title: **CR to 33.310: Correction of 'Extended key usage' extension in SEG Certificate profile (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-040395	33.310	003	-	Rel-6	Correction of 'Extended key usage' extension in SEG Certificate profile	F	6.0.0	S3-040296	SEC1-NDS-AF

3GPP TSG-SA WG3 Security #33
Beijing, China, 10 – 14 May 2004

Tdoc ⌘S3-040296

CR-Form-v7

CHANGE REQUEST

⌘ **33.310** **CR** **003** ⌘**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:	⌘	Correction of 'Extended key usage' extension in SEG Certificate profile
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-AF
Date:	⌘	03/05/2004
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:	⌘	In section 6.1.3 the extension 'Extended key usage' is SEG Certificate Profile is defsigned as 'optional critical'. However, according to RFC 3280 when an extension is optional to support, a received extension marked as critical shall lead to an error if not recognized by the receiving SEG. RFC 3280 defines in section 4.2.1.13 that the extension 'Extended key usage' may be either critical or non-critical. Thus to avoid conflict due to different implementations of optional extensions the extentions should be designed as 'optional non-critical'.
Summary of change:	⌘	Change the extension 'Extended key usage' to 'optional non-critical'
Consequences if not approved:	⌘	An optional extension designed as 'critical' could lead to interoperability problems.

Clauses affected:	⌘	6.1.3

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

⌘

Other comments: ⌘

***** change *****

6.1.3 SEG Certificate profile

SEG certificates shall be directly signed by the roaming CA, i.e. without employing any intermediate CAs. This limits NDS/AF complexity and makes retrieval and validation of intermediate CA certificates by SEGs unnecessary. Any SEG shall use exactly one certificate to identify itself within the NDS/AF.

In addition to clause 6.1.1, the following requirements apply:

- The RSA key length shall be at least 1024-bit;
- Issuer name is the same as the subject name in the roaming CA certificate.
- Extensions:
  - Optionally non critical authority key identifier;
  - Optionally non critical subject key identifier;
  - Mandatory non-critical subjectAltName;
  - Mandatory critical key usage: At least digitalSignature and keyEncipherment shall be set;
  - Optional non-critical extended key usage: If present, at least server authentication and IKE intermediate shall be set;
  - Mandatory critical Distribution points: CRL distribution point;

NOTE: Depending on the availability of DNS between peer SEGs, the following rule is applied:

- subjectAltName should contain IP address (in case DNS is not available);
- subjectAltName should contain FQDN (in case DNS is available).