

CHANGE REQUEST

33.221 **CR 005** rev - Current version: 6.1.0

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:	☞ Visited network issuing subscriber certificates		
Source:	☞ Nokia		
Work item code:	☞ SEC1-SC	Date:	☞ 27/09/2004
Category:	☞ B	Release:	☞ Rel-6
	Use <u>one</u> 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 <u>one</u> of the following releases: Ph2 (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) Rel-7 (Release 7)

Reason for change:	☞ Roaming subscribers shall be able to request subscriber certificates and CA certificates from the visited network. Subscriber's home network shall be able control whether the visited network is allowed to do this.
Summary of change:	☞ Roaming subscribers are able to request subscriber certificates and CA certificates from the visited network. Subscriber's home network is able to control this by using application-specific user security setting's authorization part.
Consequences if not approved:	☞ Whether visited networks are allowed to issue subscriber certificates to roaming subscribers is left open.

Clauses affected:	☞ 4.4.3, 4.4.4										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;"> </td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	X			X		X	Other core specifications	☞ TS 24.109
	Y	N									
	X										
	X										
	X										
		Test specifications									
		O&M Specifications									
Other comments:	☞										

===== BEGIN CHANGE =====

4.4.3 Roaming and service network support

The roaming subscriber shall be able to request subscriber certificates and operator CA certificates from the home network.

~~Editor's note: Certificate requests to any than home network may be supported in later phase of the present specification.~~

The roaming subscriber shall be able to request subscriber certificates and operator CA certificates from the visited network. The home network shall be able to control whether the visited network is allowed to issue subscriber certificates to its roaming subscribers (cf. subclause 4.4.4).

4.4.4 Home operator control

Home operator shall be able to control the issuing of subscriber certificates. The control includes to whom the certificates are allowed to issue and the types of issued certificates.

Operator control is supported by information in the GBA user security settings. For each type of subscriber certificate, i.e. for different key usage in WAP Certificate and CRL Profile [7], subscriber's PKI portal specific user security setting shall contain a flag that allows or disallows the issuing of that type of certificate to subscriber. According to WAP Certificate and CRL Profile [7], there are two types of certificates for users (i.e. subscribers): user certificates for authentication and user certificates for digital signatures (i.e. non-repudiation).

Delivery of operator CA certificates is always allowed.

~~Editor's note: When visited network may issue certificates, standardized way of transferring the control information from home network to visited network is needed.~~

===== END CHANGE =====