CR-Form-v7.1

PSEUDO CHANGE REQUEST

⌘	**33.878** CR **CRNum**	⌘rev	**-**	⌘	Current version:	**0.0.3**	⌘

*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 **X**   Radio Access Network ☐   Core Network **X**

Title: ⌘	Early IMS indication	
Source: ⌘	Nokia	
Work item code:⌘	Early IMS Security	***Date:*** ⌘ 16/11/2004

Category: ⌘ **C**	***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:
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: ⌘	To better quarantee flexibility towards different kind of terminal implementations the Authorization header must be allowed for the UE to be included. Explicit indication in the network is useful in order to support the possible new authentication mechanisms in the future. To avoid the changes to the Cx interface, the I-CSCF and the S-CSCF generate the private user identity from the public user identity received in the Register message.
Summary of change:⌘	Authorization header may be included in the initial Register message, P-CSCF adds an early IMS indication to Authorization header. The I-CSCF and S-CSCF generate the private user identity from the public user identity.
Consequences if not approved: ⌘	Potential interworking problems in IMS Security with different kind of terminals.

Clauses affected: ⌘	7.2.4

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

Other comments: ⌘	

********** START OF CHANGE **********

7.2.4   Interworking cases

It is expected that both fully 3GPP compliant UEs implementing the security mechanisms in TS 33.203 [2] (denoted "fully compliant" in the following) and UEs implementing the early IMS security security solution specified in the present document (denoted "early IMS" in the following) will access the same IMS. In addition, IMS networks will support only fully compliant UEs, early IMS UEs, or both. Both UEs and IMS networks must therefore be able to properly handle the different possible interworking cases.

Editor's note: The interworking solution described in this clause is agreed as a working assumption in SA3. An alternative approach based on explicit identification of early IMS support on UEs has been suggested, but a detailed proposal has not yet been developed. If compelling reasons are found to replace the working assumption with this alternative approach, then this will be done at SA3#36 (23-26 November 2004).

Since early IMS security does not require the Ssecurity.Client headers specified for fully compliant UEs, thisese headers shall not be used for early IMS. The Register message sent by an early IMS UE to the IMS network shall not contain the Ssecurity-Client headers specified by TS 33.203 (Authorization and Security-Client).

As a result, early IMS UEs shall not add an explicit indication for the security used to the IMS signaling. An IMS network supporting both early IMS and fully 3GPP compliant UEs shall use early IMS security for authenticating the UE during registrations that do not contain the Ssecurity-Client headers specified by TS 33.203 (Authorization and Security-Client).

Without sending an Authorization Header in the initial Register message, early IMS UEs only provide the IMS public identity, but not the IMS private identity to the network (this is only present in the Authorization header for fully compliant UEs). The IMS private identity shall therefore be derived from the subscriber's public identity in the HSS.

Authorization header may be included to the initial Register message as specified in TS 33.203. If Authorization header is present and Security-Client header is not present in the initial Register message, the P-CSCF shall add early IMS indication to the Authorization header. A new parameter called 'Early IMS' is added to Authorization header. If Authorization header is not included to the initial Register message then the P-CSCF shall add the Authorization header with the early IMS indication.

During the process of user registration, the Cx interface carries both the private user identity and the public user identity in Cx-MAR requests (sent by I-CSCF and S-CSCF). To avoid changes to the message format in the Cx interface, the I-CSCF and the S-CSCF shall generate the private user identity from the public user identity received in the Register message. For early IMS, only the public user identity shall be sent to the HSS within these requests, and the private user identity shall be empty. This avoids changes to the message format to the Cx interface.

If the S-CSCF receives an indication that the UE is early IMS, then it shall be able to select the "IP-based" authentication scheme in the Cx-MAR request. The Cx interface shall support the error case that the S-CSCF selects the "Digest-AKAv1-MD5" authentication scheme based on UE indication, but the HSS detects that the subscriber has a SIM instead of a USIM or ISIM. In this case the HSS shall respond with an appropriate error command. The S-CSCF will then respond to the UE with a 403 Forbidden message. If the UE is capable of early IMS then, according to step 5, the UE will take this as an indication to attempt registration using early IMS.

For interworking between early IMS and fully compliant implementations during IMS registration, the following cases shall be supported:

1. Both UE and IMS network support early IMS only

   IMS registration shall take place as described by the present document.

2. UE supports early IMS only, IMS network supports both early IMS and fully compliant access security

   The IMS network shall use early IMS security according to the present document for authenticating the UE for all registrations from UEs that do not provide the fully compliant security headers.

3. UE supports both, IMS network supports early IMS only

   If the UE already has knowledge about the IMS network capabilities (which could for example be preconfigured in the UE), the appropriate authentication method shall be chosen. Fully compliant security shall be used, if the network supports this, otherwise early IMS security shall be used.

If the UE does not have such knowledge it shall start with the fully compliant Registration procedure. The early IMS P-CSCF shall answer with a 420 "Bad Extension" failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial Register message (this header cannot be ignored by the P-CSCF).

The UE shall, after receiving the error message, send an early IMS registration, i.e., shall send a new Register message without the fully compliant security headers. The network shall respond with a 200 OK message according to the registration message flow as specified in clause 7.2.5.1.

4.   UE and IMS network support both

The UE shall start with the fully compliant IMS registration procedure. The network, with receiving the initial Register message, receives indication that the UE is fully compliant and shall continue as specified by TS 33.203.

5.   UE supports early IMS only, IMS network supports fully compliant access security only

The UE sends a Register message to the IMS network that does not contain the necessary security headers required by fully compliant IMS. In this case the IMS network will answer with an error message (403 Forbidden with "Authentication Failed" reason phrase) indicating to the early IMS UE that the authentication method is incorrect. After receiving the error message, the early IMS UE shall stop the attempt to register with this network, since early IMS is not supported.

6.   UE supports fully compliant access security only, IMS network supports early IMS only

The UE shall start with the fully compliant IMS registration procedure. The early IMS P-CSCF shall answer with a 420 "Bad Extension" failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial Register message (this header cannot be ignored by the P-CSCF). After receiving the error message, the UE shall stop the attempt to register with this network, since the fully 3GPP compliant security according to TS 33.203 is not supported.

********** END OF CHANGE **********