TSGS#27(05) 0267

Source: **SA3**

Title: **CR to 33.978 on Correction of use of 401 Unauthorized and 399 Warning headers (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050267	33.978	001	-	Rel-6	F	Correction of use of 401 Unauthorized and 399 Warning headers	6.0.1	6.1.0	S3-050305

3GPP TSG SA WG3 Security — S3#38 **S3-050305**
April 26-29, 2005, Geneva, Switzerland

CR-Form-v7

CHANGE REQUEST

⌘ **33.978** **CR** **001** ⌘ **rev** **-** ⌘ Current version: **6.0.1** ⌘

*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:	⌘	Correction of use of 401 Unauthorized and 399 Warn-code
Source:	⌘	Siemens
Work item code:	⌘	SEC-IMS
Date:	⌘	29/04/2005
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:	⌘	401 Unauthorized and 399 Warn-code are not everywhere used according to RFCs
Summary of change:	⌘	In interworking case 5 of section 6.2.6, it is proposed to use 403 (forbidden) instead of 401 and 399. This seems adequate as a correctly implemented UE should always check first whether a USIM or ISIM is available before starting IMS procedures fully compliant with TS 33.203.
Consequences if not approved:	⌘	Conflict with RFCs 2616, 2617 and 3261

Clauses affected:	⌘	6.2.6, bullet 5

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

Other comments:	⌘	-

6.2.6 Interworking cases

For the purposes of the interworking considerations in this clause, it is assumed that the IMS entities P-CSCF, I-CSCF, S-CSCF and HSS reside in the home network and all support the same variants of IMS, i.e. all support either only early IMS security, or only fully compliant IMS security, or both.

NOTE: It is compatible with the considerations in this document that the UE uses different APNs to indicate the IMS variant currently used by the UE, in case the P-CSCF functionality is split over several physical entities.

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

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

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

Without sending an Authorization Header in the initial REGISTER request, early IMS UEs only provide the IMS public identity (IMPU), but not the IMS private identity (IMPI) to the network (this is only present in the Authorization header for fully compliant IMS security UEs).

During the process of user registration for early IMS security, the Cx interface carries the public user identity in Cx-UAR requests (sent by I-CSCF) and Cx-MAR as well as Cx-SAR requests (sent by S-CSCF). The private user identity within these requests shall be generated according to section 6.2.5.1. This avoids changes to the message format on the Cx interface.

If the S-CSCF receives an indication that the UE is an early IMS UE, then it shall be able to select the "Early-IMS-Security" authentication scheme in the Cx-MAR request.

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

1. Both UE and IMS network support early IMS security only

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

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

   Early IMS security according to this annex shall be used for authenticating the UE for all registrations from UEs that do not provide the fully compliant IMS security headers.

3. UE supports both, IMS network supports early IMS security 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. The UE shall use fully compliant IMS security, if the network supports this, otherwise the UE shall use early IMS security.

   If the UE does not have such knowledge it 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 request.

NOTE: The Proxy-Require header cannot be ignored by the P-CSCF.

The UE shall, after receiving the error response, send an early IMS registration, i.e., shall send a new REGISTER request without the fully compliant IMS security headers.

4. UE and IMS network support both

   The UE shall start with the fully compliant IMS security registration procedure. The network, with receiving the initial REGISTER request, receives indication that the IMS UE is fully compliant and shall continue as specified by TS 33.203 [2].

5. Mobile equipment and IMS network support both, UE contains a SIM

   The UE might start with the fully compliant IMS security registration procedure. However, when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that the UE contains a SIM and return an error.

   The S-CSCF shall answer with a ~~a 401 (Unauthorized) with a Warning: header containing a warn-code 399 and the warning text "Early security required". The UE then retries using early IMS security.~~403 (Forbidden). After receiving the 403 response, the UE shall stop the attempt to register with this network.

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

   The UE sends a REGISTER request to the IMS network that does not contain the security headers required by fully compliant IMS security. The fully compliant IMS security P-CSCF will detect that the Security-Client header is missing and return a 4xx responses, as described in clause 5.2.2 of TS 24.229 [7].

7. UE supports fully compliant IMS security only, IMS network supports early IMS security only

   The UE shall start with the fully compliant IMS security 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 request. After receiving the error response, the UE shall stop the attempt to register with this network, since the fully compliant IMS security according to TS 33.203 [2] is not supported.

8. UE supports fully compliant IMS access security only, IMS network supports both

   The UE shall start with the fully compliant IMS registration procedure. The network, with receiving the initial REGISTER request, receives indication that the IMS UE is fully compliant and shall continue as specified by TS 33.203 [2].

9. UE supports both, IMS network supports fully compliant IMS access security only

   The UE shall start with the fully compliant IMS registration procedure. The network, with receiving the initial REGISTER request, receives indication that the IMS UE is fully compliant and shall continue as specified by TS 33.203 [2].

10. UE supports both, IMS network supports fully compliant IMS access security only, UE contains a SIM

    The UE might start with the fully compliant IMS registration procedure. However, when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that the UE contains a SIM and return an error. The S-CSCF shall answer with a 403 (Forbidden). After receiving the 403 response, the UE shall stop the attempt to register with this network.

11. Both UE and IMS network support fully compliant IMS access security only.

    IMS registration shall take place as described by TS 33.203 [2].