3GPP TSG SA WG3 Security — S3#36 **S3-040999**
November 23-26, 2004, Shenzhen, China

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 ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Removal of remaining Editor's Notes		
Source:	⌘	Vodafone		
Work item code:	⌘	Early IMS	***Date:*** ⌘	16/11/2004
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:* *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:	⌘	
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	7.2.4, Annex A			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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 security headers specified for fully compliant UEs, these 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 security 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 security 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.

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). 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.

Annex A: Comparison with an alternative approach – HTTP Digest

An alternative approach would have been to use password-based authentication for early IMS implementations. For example, HTTP Digest (IETF RFC 2617) could have been used for authenticating the IMS subscriber. The HTTP Digest method is a widely supported authentication mechanism. It is not dependent of the GPRS network and it does not require new functional elements or interfaces in IMS network. However, this method would have required a subscriber-specific password to be provisioned on the IMS UE. This alternative is not adopted for use in early IMS systems.

The HTTP Digest method has the following advantages and disadvantages:

Advantages:

- Fully standardized and supported by RFC 3261 [6] compliant implementations and therefore by 3GPP TS 24.229 [7] compliant implementations (SIP protocol mandates support of HTTP Digest).

~~Editor's note: The following bullet point is still under study for inclusion in this section.~~

~~- HTTP Digest enables access via multiple technologies (e.g. WLAN). Note that this is not considered an advantage in the context of early IMS systems since it is specified in clause 5 that it is only a requirement to support secure access over the 3GPP PS domain (including GSM/GPRS and UMTS access).~~

- HTTP Digest can support partial message integrity protection for those parts of the message used in the calculation of the WWW-Authenticate and Authorization header field response directive values (when qop=auth-int).

- HTTP Digest implementations can employ methods to protect against replay attacks (e.g. using server created nonce values based on user ID, time-stamp, private server key, or using one-time nonce values).

Disadvantages:

- HTTP Digest may impose restrictions on the type of charging schemes that can be adopted by an operator. In particular, if a subscriber could find out his or her own password from an insecure implementation on the UE, then he or she could share the IMS subscription with friends. This could impact revenue for the operator if bundled or partly subscription based tariffs are used rather than purely usage based tariffs. For example, a subscriber could take out a subscription for 100 instant messages and then share this with his or her friends. Although contractual obligations could be imposed on customers to prohibit this behaviour, in practice this would be difficult to enforce without employing special protection mechanisms, e.g. disallow multiple binding to a single IP address. If charging were purely usage based then there would be no incentive for the subscriber to do this, therefore using HTTP Digest may not impact on operator’s revenue. The solution specified in clause 7 is flexible in allowing a range of different charging models including bundled or partly subscription based tariffs.

- HTTP Digest provides a weaker form of subscriber authentication when compared with the levels of authentication used for other services offered over 3GPP networks, where authentication is typically based directly or indirectly on the (U)SIM. Subscription authentication depends, among other things, on the strength of the password used as well as on the password provisioning methods, such as bootstrapping passwords into the IMS capable UE. A weak subscriber authentication, vulnerable to dictionary attacks, has implications on the reliability of charging, and on the level of assurance that can be given to the customer that their communications cannot be masqueraded. In the solution specified in clause 7, authentication of the IMS subscriber is indirectly based on (U)SIM authentication at the GPRS level. The level of security is similar to that currently used for certain WAP services, where the user’s MSISDN is provided by the GGSN to the WAP gateway. Security does not rely on the UE securely storing any long-term secret information (e.g. passwords).

- HTTP Digest provisioning is more complex since subscriber-specific information (i.e. passwords) must be installed or bootstrapped into each IMS UE.