CR-Form-v7

CHANGE REQUEST

⌘ **33.cde** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **0.5.0** ⌘

*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:	⌘	Authentication of IMS subscriptions for Presence Service
Source:	⌘	Nokia
Work item code:	⌘	PRESNC
Date:	⌘	10/07/2003
Category:	⌘	
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:	⌘	The current trust management mechanisms in IMS should be re-used for IMS watcher authentication. The enhancement based on presentity's password is weaker than IMS provided security so it can not provide extra secure.
Summary of change:	⌘	1. Update the reference 2. IMS subscriber (watcher) shall be authenticated based on IMS mechanism 3. For non-IMS subscriber, the Presence Server may authenticate the watcher using HTTP Digest. The use of HTTP Digest AKA and LCS specific security are for further study.
Consequences if not approved:	⌘	Security is not enhanced, the mechanism is redudant for IMS subscriber.

Clauses affected:	⌘	2, 8.1, 8.2

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

Other comments: ⌘

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.141: "Presence service; Stage 1".

[3] 3GPP TS 23.141: "Presence service; Stage 2".

[4] Common Presence and Instant Messaging (CPIM) Presence Information Data Format, Internet Draft http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-pidf-~~05~~08.txt, May ~~2002~~2003.

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[5] Session Initiation Protocol (SIP) Extensions for Presence, Internet-Draft http://www.ietf.org/internet-drafts/draft-ietf-simple-presence-~~07~~10.txt, ~~May 2002~~ January, 2003.

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[6] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[7] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[8] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[9] IETF RFC 3265: "Session Initiation Protocol (SIP) Event Notification"

[10] A SIP Event Package for List Presence, Internet-Draft, http://search.ietf.org/internet-drafts/draft-ietf-simple-presencelist-package-00.txt, June 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[11] IETF RFC 2778: "A Model for Presence and Instant Messaging".

[12] IETF RFC 2779: "Instant Messaging / Presence Protocol Requirements".

[13] IETF RFC 2406 (1998) "IP Encapsulating Security Payload (ESP)".

[14] IETF RFC 2401 (1998) "Security Architecture for the Internet Protocol".

[15] RFC 2451 (1998): "The ESP CBC-Mode Cipher Algorithms".

[16] RFC 3329 (2003): "Security Mechanism Agreement for the Session Initiation Protocol".

[17] Draft-ietf-sip-privacy-general-01: A Privacy Mechanism for the Session Initiation Protocol (SIP), June 6, 2002.

[18] Draft-ietf-sip-asserted-identity-02: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network, June 21, 2002.

8 Security mechanisms

8.1 IMS related security mechanisms

********** skipped**********

8.1.3 Subscriber anonymity mechanisms

8.1.3.1 Anonymity of SIP dialog initiator

The anonymity mechanism is optional for implementation in UA. The UA may provide anonymity for the subscriber following the privacy mechanisms described in [17, and 18]. This includes populating the SIP headers with values that reflect the privacy requirements of the subscriber, as well as requesting further privacy from the network.
The UA may use the following priv-value types of the Privacy header in [17, and 18]:

a. ‘none’
b. ‘id’
c. ‘critical’
d. ‘user’

[Editors note:priv-value types ‘header’ and ‘session’ are FFS.]

The home network (e.g. S-CSCF or an Application Server) may provide the anonymity on behalf of the UA using the following priv-value type [17]:

e. ‘user’

P-CSCF and the edge proxy (e.g. I-CSCF) must implement the following priv-value types of the Privacy header in [17, and 18]:

f. ‘none’
g. ‘id’
h. ‘critical’
i. ‘user’

[Editors note:priv-value types ‘header’ and ‘session’ are FFS.]

P-CSCF and the edge proxy shall monitor the privacy requests in all terminating SIP requests, and provide the requested privacy (e.g. hide the identity of the subscriber). P-CSCF and the edge proxy shall not provide privacy for originating SIP requests.

8.1.3.2 Pseudonym IMPU

Subscriber may use pseudonym IMPU to obtain some degree of anonymity. From system point of view, the pseudonym IMPU is like any other IMPU. All existing rules related IMPUs shall apply.

Note: Unprotected SIP REGISTER messages include identity information that may be intercepted by unauthorized parties when sent over the air-interface. These messages may be used to combine the IMPU and IMPI information, and consequently this information may reveal the parallel IMPUs related to the pseudonym IMPU.

[Editors note: There may be a need for additional rules related to the registration of pseudonym IMPUs.]

8.1.4 ~~8.1.4~~ Subscription authentication mechanism

For IMS subscriber, the watcher is authenticated based on her IMS subscription. In this case, the SUBSCRIBE request contains a P-Asserted-Identity header inserted by an trusted IMS domain. The procedure is defined by 3GPP TS 24.229. The PS is aware of the identity of the watcher and no extra actions are needed.

8.2 Non-IMS related security mechanisms

8.2.1 Subscription authentication mechanism

[Editors Note: The use of HTTP Digest AKA is FFS:

- *HTTP Digest AKA: If the watcher belongs to the same home network than the presentity, HTTP Digest AKA could be used for authentication. In this case, the related session keys IK and CK would also be available for end-to-end integrity and confidentiality protection if needed. Note that it is also possible to change the IMS/Presence security architecture in the way that all subscriptions are always routed via the Presence Server, and that the communication between the IMS sub-domains is done only between the Presence Servers.*

]

Subscription Authorization Policy may require that the Presence Server must authenticate the Watchers during the subscription phase. The Subscription Authorization Policy shall define which authentication method and credentials are used in the authentication. The following mechanisms shall be supported:

a. HTTP Digest

NOTE: Distribution of HTTP Digest passwords is outside the scope of this specification. There are many known solutions, e.g. the presentity (or principal/subscriber) can take responsibility of the key distribution, or the watchers may need to register to Presence Servers via HTTP.

8.~~2~~ 3 HTTP related security mechanisms

[Editors Note: This is a placeholder for HTTP security mechanisms]

8.~~2~~3.1 Authentication mechanisms

[Editors Note: This is a placeholder for HTTP authentication mechanisms]

[Editors Note: The re-use of USIM for authentication is not perceived as secure if the AKA session keys (IK/CK) are not somehow tied to the security solution. For example, the use of RFC 3310 (HTTP Digest authentication with AKA) with the algorithm version "AKAv1" shall not be used if the related session keys (IK and/or CK) are not also used in the solution.]

[Editors Note: At least the following authentication solutions should be further studied:

a. *Presence is limited to the re-use of ISIM with HTTP Digest AKA v1.*
b. *A new version of HTTP Digest AKA algorithm is developed. In this case, the re-use of USIM with HTTP Digest AKA v1 is secure.*
c. *HTTP authentication with HTTP Digest passwords is appropriate.*
d. *Solutions with client certificates (e.g. with TLS, OMA/WAP) are appropriate.*
e. *Some password based Single-Sign-On solutions could be applied.*
f. *Integration of HTTP security to IMS registration should be further studied. This may imply some kind of Single-Sign-On solution.]*

8.~~2~~3.2 Integrity protection mechanisms

[Editors Note: This is a placeholder for HTTP integrity protection mechanisms]

8.~~2~~3.3 Confidentiality protection mechanisms

[Editors Note: This is a placeholder for HTTP confidentiality protection mechanisms]