Source: **Nokia**

Title: **P-CR for Presence TR 33.abc v0.6.0**

Document for: **Discussion/Approval**

Agenda Item: **Presence**

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.txt, May 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.

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

[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.

[19] IETF RFC 2246 (1999) “The TLS Protocol Version 1”

[20] 3GPP TS 33.109: " Bootstrapping of application security using AKA and Support for Subscriber Certificates".

NEXT CHANGE

5 Presence Security architecture

The Presence Security architecture is based on the IMS Security Architecture as specified in TS33.203 [6].

UE accesses Presence server for user data manipulation over Ut intrface. The overall architecture is given below, where GBA is involved in bootstrapping secret for UE-Authentication Proxy (AP, as a NAF) communication over TLS connection.

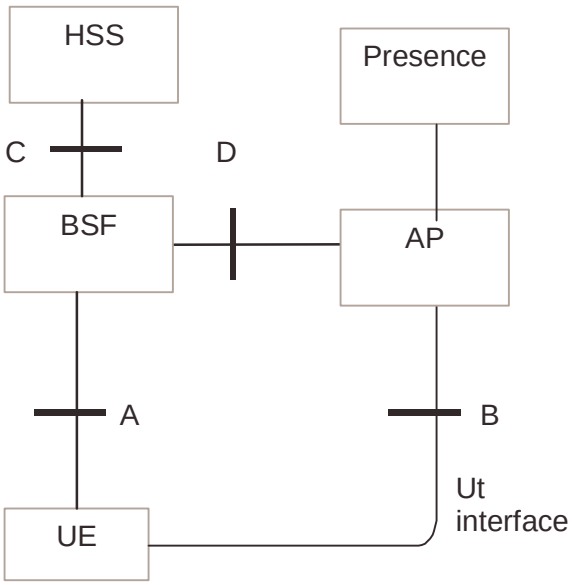

Figure 3: The overall architecture of Ut interface security

The protocol A, B, C and D are specified in [20]. The Presence security shall re-use the established mechanism for Ut interface. The integrity and confidentiality protection of protocol B is described as specific feature in the present specification.

~~The functional architecture is depicted in Figure 2 and this clause specifies the protection methods for the Ut interface.~~

~~[~~

~~*The proposals that have been discussed include:*~~

~~*1.Base it on IMS Registrations, new key management procedures and base the protection on HTTPS*~~

~~*2.Use of AKAv2 and Authentication proxy and TLS*~~

~~3.~~1. ~~*Use of Bootstrapping function for HTTP AKA using TLS]*~~

6 Security features

6.1 IMS related security features

6.1.1 Confidentiality protection

Possibility for IMS specific confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. Mobile Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation when IMS is used for Presence. The following mechanisms are provided at SIP layer:

1. The UE shall always offer encryption algorithms for P-CSCF to be used for the session, as specified in chapter 8.
2. The P-CSCF shall decide whether the IMS specific encryption mechanism is used. If used, the UE and the P-CSCF shall agree on security associations, which include the encryption key that shall be used for the confidentiality protection. The mechanism is based on IMS AKA and specified in clause 6.1 of [6].

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [7].

6.1.2 Subscriber anonymity

6.1.2.1 Initiator of a SIP dialog

The network shall hide the identity of the initiator of a SIP dialog (the SIP URI) in the following cases:

a. The initiator has requested from the network that her identity is hidden from the receiver of the request.

b. The initiator has agreed with the home network that the home network takes care of the identity blocking for certain messages on behalf of the initiator.

Anonymity of the SIP URI shall be provided if the subscriber requests it. The network shall not deliver the message to the receiver if the initiator has set the anonymity request as ‘critical’, and the network is not able to provide the requested anonymity. The same anonymity rules shall apply to all messages within a SIP dialog.

Anonymity shall be provided by the last-hop P-CSCF. If the IMS originated messages are sent outside the IMS trust domain (e.g. to the open Internet), the edge proxy (e.g. I-CSCF) shall provide the anonymity.

Anonymity may be requested with multimedia sessions, or with any other services that will use IMS, such as Presence or Instant Messaging.

6.1.2.2 Receiver of a SIP dialog initiation request

The receiver of a SIP dialog initiation request is able to have some degree of anonymity if she registers a pseudonym as IMPU. In this case, the subscriber shall be responsible for not revealing the relationship between the pseudonym IMPU and her real identity to unauthorized parties. If she reveals her real identity, there is no anonymity.

6.1.3 Subscription authentication

The Presence Server shall authenticate the subscription requests originated from Watchers if required in the Subscription Authorization Policy. The Subscription Authorization Policy shall indicate the method and credentials used in authentication. This password needs to be manually distributed by the Principal of the Presentity (or the subscriber) to the Watcher(s). This can be done by several mechanisms but is left out from this specification. The password should be random and difficult to guess for an attacker however the actual password derivation is under the responsibility of the subscriber (or principal).

6.2 Secure access to HTTP Application Server

[Editors Note: This is a placeholder forHTTP requirements]

6.2.1 Authentication

The following requirements are essential for Ut interface authentication:

- Accessing to user data should be authenticated
- One user shall be able manipulate own and only own data
- The consumption of Authentication Vector should be minimized so as to avoid additional sequence number out-of-synchronization
- The protection should be applicable to other SIP enabled services (over IMS)

~~*[Editors Note: This is a placeholder for HTTP authentication requirements]*~~

6.2.2 Integrity protection

~~*[Editors Note: This is a placeholder for HTTP integrity protection requirements]*~~

- User data integrity over Ut interface should be guaranteed

6.2.3 Confidentiality protection

- User data over Ut interface should be kept confidential against any attacker
- The User data towards to the Presence server should be able to kept confidential against any other application server

~~*[Editors Note: This is a placeholder for HTTP confidentiality protection requirements]*~~

6.3 non-IMS related security features

[Editors Note: This is a placeholder for non-IMS requirements]

NEXT CHANGE

8.2 HTTP related security mechanisms

In Figure 3, the Ut interface is secured by TLS for UE data manipulation such as user groups, subscription authorization policy, and presence lists. When the UE accessing Presence server, the procedure shall re-use the generic authentication procedure described in [20].

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

8.2.1 Authentication mechanisms

The UE and AP shall authenticate each other mutually based on shared keys derived from bootstrapping procedure as depicted in Figure 4 and described below:

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

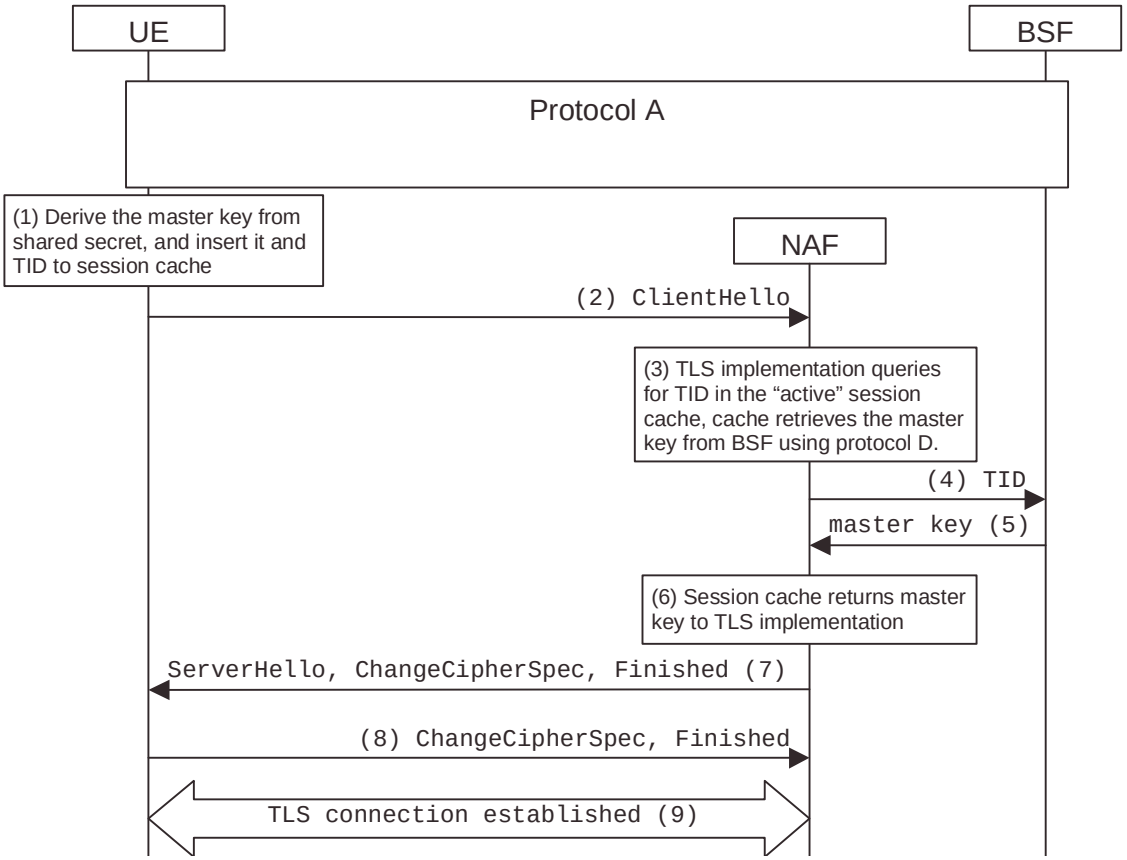

Figure 4: UE and AP authenticate each other in TLS handshake.

the UE starts HTTP Digest AKA or AKAv2 (outside a TLS tunnel) with the BSF. The BSF may contact the HSS to fetch authentication vectors (protocol C). After running protocol A, the UE and the BSF share a secret key and transaction ID (TID), cf. [20].

The UE shall next send an http request towards Presence server. The http request is intercepted by the AP-NAF. The AP-NAF instructs the UE to upgrade the HTTP connection to TLS/1.0. Alternatively, the UE shall send an https request towards AP. In any case, the TLS is terminated in Authentication Proxy (AP) that will forward data manipulation request to the Presence server. Once receive the TID, the AP shall fetche the agreed key from the BSF (over protocol D), as described in [20].

The AP shall check the private ID would associate to the public ID that is papulated inside the HTTP message towards Presence server. The verification shall rely on the user service related data carried over the protocol D (Zn interface) to AP, where all the allowed IMPUs are contained. If it is needed, the

AP shall remove the private ID from HTTP message so as to keep the UE private identity anonymous to external provider's application server.

~~*[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.]

8.2.2 Integrity protection mechanisms

The TLS connection shall provide the required integrity protection by applying propoer cipher suites [19].

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

8.2.3 Confidentiality protection mechanisms

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

The TLS connection shall provide the required confidentiality protection by applying propoer cipher suites [19].