3GPP TSG SA WG3 Security — S3#22 **S3-020096**

February 25th– February 28th, 2002

Bristol, UK

Agenda Item:	TBD
Source:	Ericsson
Title:	On Service Requirements of Presence Service
Document for:	Information

1. Scope and objectives

This contribution discusses on the current security and privacy requirements of the presence service as stated in 3GPP TS 22.141.

2 Background

During S3#21 meeting (Nov´01), a LS from S1 (Tdoc S3-010593) was received and discussed.

SA1 asked SA3 to review and comment on the security and privacy requirements of the presence service in S1 TS 22.141 (and accompaining CRs).

After a brief review during the meeting, no major problems were identified with any of the privacy and security requirement sections and proposed CRs. However, it was agreed to consider whether further elaboration or clarification of the privacy and security requirements is necessary.

It is assumed that proposed CRs attached to LS from S1 were approved at SA#14 and incorporated in a further version of TS 22.141. CONFIRM THIS !!!!

3 Discussion

The relevant requirements regarding privacy and security in TS 22.141 v5.0.0. can not only be found in chapters 6 and 7. It is the opinion of the author of this contribution that other sections of the specification also includes other requirements regarding access control which might be also subject for S3 review.

Therefore, the relevant requirements in TS 22.141 v5.0.0 (and accompaining CRs) could be grouped in the following way:

Authentication

7. *It shall be possible to authenticate presentities and/or watchers at any time.*

   It shall be possible to authenticate a principal before allowing registration to the presence service.

   It shall be possible to authenticate a watcher requesting access to the presence service. Existing security mechanisms as well as mechanisms specific to presence service may be used.

Confidentiality, Integrity and Anty-Replay Protection

7. *It shall be possible to protect the following items from attacks (e.g., eavesdropping, tampering, and replay attacks):*

   - *Presence information and notifications*
   - *Requests for presence information, e.g., requests for subscription and requests for presence information retrieval.*

Fraud

7. The presence service shall support measures to detect and prevent attempts to maliciously use or abuse the services

Access control requirements (authorisation)

General

5.4. a) The presentity shall have the ability to accept or reject a request for presence information on a per watcher basis, with the option:

i) once only per watcher (e.g. set up access rules for known watcher, groups of watchers, anonymous watcher-subscriptions, etc.),
ii) for each presence information request (e.g. for watchers that are unknown or not set up in the current access rules).
iii) it shall be possible for the presence service to make access control decisions on behalf of the presentity (e.g. when the presentity is out of contact) subject to the presentity's privacy

5.4.b)iv) An unauthorised third party shall not be able to cancel a subscribed-watcher's watcher-subscription to a presentity's presence information

5.5.iii) It shall be possible for the presentity to configure the presence service to deny a subscribed-watcher's subscription, whilst appearing to the subscribed-watcher as if the subscription has been granted (this is sometimes called "polite blocking")

7. It shall be possible to authorise a watcher's watcher-subscription request to a presentity's presence information.

Privacy

5.4.c)v) it shall be possible for the watcher to withhold their identifier (e.g. in the case of anonymous watcher-subscription).

5.4.c)vi) If the subscribed-watcher so chooses, the subscribed-watcher's watcher-subscription to a presentity's presence information shall not be revealed to other watchers.

5.4.c)vii) It shall be possible for a watcher to define which parts of a presentity's presence information it receives, subject to the principal's privacy requirements.

6.1. A principal of a presentity shall, at any time, be able to control to whom, for how long and what (all or part of) presence information of the presentity is provided, and a principal of a watcher shall, at any time, be able to control to whom, for how long and what (all or part of) watcher information of the watcher is provided

An operator shall, at any time, be able to override subscriber, possessor and principal privacy preferences if required to do so by local authorities.

Access Rules

6.2. Access rules shall define:

- *a watcher or groups of watchers allowed access to the presentity's presence information. For example: watchers x and y are allowed, or only watchers in group z are allowed, or all watchers and groups are allowed…*
- *the validity of the access authorisation granted for a given watcher or groups of watchers. The access to the presentity's presence information can be restricted for a certain period (i.e. duration or number of requests), or during specific periods of the day.*
- *the attributes of the presentity's presence information that can be made available to a given watcher or groups of watchers.*
- *the ability to provide different presence information (i.e. both number of attributes and values of attributes) based on the watcher, and principal's preferences (e.g. its availability). For example: watcher x receives 'Online/Instant Messaging/im:a@there.com', while group y receives 'Offline/Instant Messaging/im:a@there.com'.*

A set of default access rules shall be defined by the principal.

Regulatory Requirements

The Home Environment shall be able to override the privacy requirements if needed. (c.f. legal interception requirement in clause 5.3)

3.1 Analysis

An analysis of the above set of requirements might bring the following conclusions:

- The list seems fairly complete.
- Some redundancies could be avoided, mainly regarding privacy, access rules and access control requirements.
- Fraud requirement is rather ambiguous so that a specific solution can be proposed.
- Clause 5.3 is refered for legal interception but it is not clear which is the refered requirement.

4 Conclusions

Current status of S1 specification on Presence Service looks therefore acceptable and stable enough. S1 should be informed about this also including the minor findings highlighted by this contribution and potentially some others raised during S3#22.

S2 is currently largely working in the definition of the presence architecture based on S1 service requirements. Seems that architecture for presence service could reuse concepts, mechanisms and protocols from IMS architecture. However these principles do not seem to be yet mature enough.

It is Ericsson impresion that S3 can do very littlle more for the moment on this subject, until further details on the final architecture for Presence are completed in S2.