ERICSSON

S3-010385

aSIP-Access Security for IP-Based Services

Activities and timeplan

Krister Boman

Ericsson

Outcome from the Phoenix meeting S3#18:

- Authentication is terminated in the S-CSCF.
- EAP is used for transporting the authentication parameters in SIP. The status on this shall be presented at SA3#19.
- The flows for terminating the authentication in the S-CSCF shall be presented to SA3#19 including failure scenarios
- Contributions on when to start to integrity protect SIP signalling shall be presented at SA3#19
- The dependancy between the 3GPP specs and IETF shall be clarified
- Contributions on Security Mode Setup shall be presented at SA3#19
- A new timeplan was agreed

Current timeplan for WI aSIP agreed in Phoenix SA3#18:

• The previous time plan stated that Stage 3 should be ready in December 2001. The rapporteur for aSIP proposed to move this target date to March 2002.

• It was then argued that this still was to early and not a realistic date. It was therefore proposed, what was believed to be a more realistic target, that Stage 3 should be frozen in June 2002. This was then agreed upon by SA3.

• However the raporteur feels that it is important NOT to delay this work further. Therefore SA3 is encouraged to adopt working assumptions at this meeting.

• It is now important to focus the work on working assumptions and narrow the scope. Most importantly not to loose tempo in order to progress the necessary work especially on IETF related work.

Current timeplan for WI aSIP agreed in Phoenix SA3#18:

S3#19	July 4-6, 2001	Integration of security architecture
S3#20	October 15-20, 2001	Integration of security architecture
S3#21	December 3-5, 2001	Concept presented to CN, RAN, T and GERAN
SA#14	December 17-20, 2001	Stage 2 presented for information
SA#15	March, 2002	Stage 2 presented for approval. The TS shall at this stage be stable in order to freeze Stage 3 specifications in June
SA#16	June, 2002	Frozen TS 33.203 Stage 2 and Stage 3

Activites for the SA3#19 meeting in London:

Agree on:

- Protection mechanism i.e. SIP-level (CMS-based) or IPSec
- The authentication flows including error cases
- Security mode setup
- The updated TS 33.203 v0.4.0
- The principles for the handling of SAs between the UE and the P-CSCF
- If an adhoc session is needed in mid September e.g. a week before the SA plenary in September. The raporteur feels that such a session would add value in terms of keeping a steady progress for the work item.

Activites for the SA3#19 meeting in London:

Open issues:

- Confidentiality protection of SIP is currently optional for implementation. Should SA3 define all mechanisms for integrity and confidentiality protection at the same time. SA3 could e.g. propose the NULL algorithm for R5?

- Replay protection for SIP (the CMS solution)

- What SPI shall be used?

- Shall the UE and the P-CSCF handle only one SA or one SA per each registered IMPU?

Activites for the SA3#19 meeting in London:

Open issues:

- Authentication: during long calls, of session establishments, network initiated, de-registrations

- Visability and configurability

- UE-functionality split

- The ISC interface between the AS and the S-CSCF has thus far not been addressed.

- IP-address anonymity has thus far not been considered. Due to fraud scenarios this has to be further analysed.