ERICSSON

S3-010545

aSIP-Access Security for IP-Based Services

Krister Boman

Ericsson

ERICSSON

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

S3#20	October 15-20, 2001	Integration of security architecture
S3#21	November 27-30, 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	IMS stage 3 specifications for approval

ERICSSON

Updates in TS33.203v050:

- SA3#19 in Newbury
  - The working assumption is that authentication shall take place at (Re-) Registrations
  - Network topology hiding included
  - The concept of the ISIM included
  - Error messages shall not be integrity protected. It is too complicated to require full proof DoS attack resistance
  - Working assumption for security mode set-up defined
  - Signalling flows updated

ERICSSON

Updates in TS33.203v060:

- SA3#19bis in Sophia Antipolis
  - Both SIP-level integrity protection and IPSec shall be worked on in parallel
  - New annexes have been created for the parallel work which is taking place in SA3 and in IETF
  - An open issues table tailored to CN1 defined in Annex E
  - Generic security association procedures included in section 7

ERICSSON

SA#13 (SP-010579)

At the SA#13 meeting in Beijing China the following tasks where identified as being essential tasks to accomplish within the Release 5 framework:

- **SIP extensions for integrity protection**
- **IMS impact on UICC**
- **ISC (IM Service Control) interface**
- **User authentication**
- **Network Domain Security**

ERICSSON

SA#13 (SP-010579)

At the SA#13 meeting in Beijing China the following tasks where identified as being not essential tasks to accomplish within the Release 5 framework:

- **UE functional split (what is needed?)**
- **Lawful interception**
- **IMS local services**
- **Support of VHE/OSA by the IMS**
- **Support of Camel by the IMS**
- **IMS emergency sessions**
- **Sh-interface between the HSS and the AS**
- **IMS security i.e. confidentiality protection**

ERICSSON

TR22.941 Stage 0 Release 5

"IP Based Multimedia Services Framework"

- **Several Security issues can be identified e.g.**
  - **(Section 8.1.10) The network should support the option to encrypt the voice component and signalling of a basic voice call.**
  - **(Section 8.14.5) It is required that a single authentication and authorisation enables access to the full capabilities of the corporate environment.**
  - **(Section 8.14.6) It shall be possible to adopt the security of the access to the security of the customer's corporate environment**
  - **etc**
- **Concluded at SA3#20 in Sydney that this TR is for Release 6 and has no impact on the work currently taking place in WI aSIP**

ERICSSON

Open issues (Contributions requested):

- Include material into TS33.203 Annex C on SIP extensions for integrity protection (Essential)
- Resolve the issue on the number of SAs between the UE and the P-CSCF
- Shall it be possible to negotiate different authentication algorithms in order to support the access independence requirement?
- Hiding. Inputs needed. Is this essential for Release 5?
- Configurability and visibility
- Define a list of parameters that are tailored to the ISIM. This shall be put into the TS33.203.
- UE functional split

ERICSSON

Open issues (Contributions requested):

- Handling of authorising IMPUs (S-CSCF or HSS)
- Reducing the number of editors notes in TS33.203
- Reducing the number of FFS in TS33.203
- SA3 shall define solutions to the Multiple S-CSCF architecture as required by SA2
- Make the flows more informational as requested by CN1
- Whenever possible each contributor is encouraged to write ‘CR-like’ contributions like Siemens initiated in Sophia Antipolis

ERICSSON

Open issues (Contributions requested):

- Security mechanisms for the ISC interface between the AS and the S-CSCF
- IP-address anonymity
- Mechanisms for network forced re-registrations (defined by CN1)

ERICSSON

IETF-activities (Status reports required for this and future SA3 meetings):

- Extending EAP with IMS AKA
- Extending HTTP (and SIP) with EAP
- Solutions required in IETF for Security Mode Setup
- Requirements draft to IETF
- Progress on SIP level integrity protection