aSIP-Access Security for IP-Based Services

Krister Boman

Ericsson

ERICSSON

Outline of the presentation:

- Aims of AdHoc
- Summary of outcome from SA#14
- Overview of open issues that need to be resolved
- IETF activities
- How to proceed to get the specification stable for submitting it to SA#15

ERICSSON

Aims of Adhoc

- Make progress on TS33.203 and prepare the specification for approval at SA#15
- Make progress on SIP signaling protection and discuss the two alternatives currently placed in the Annex
- Progress the discussion on ISIM taking the output from SA#14 into account
- The rapporteur hopes that this meeting will be productive and that working assumptions can be agreed such that the details can be finalized between this meeting and SA3#22
- The rapporteur assumes that working assumptions defined at this AdHoc may be changed at SA3#22 if enough evidence and compelling arguments are found and presented at SA3#22

ERICSSON

Outcome from SA#14

- The draft TS33.203v100 was presented and noted
- It was agreed that the platform where the IMS security parameters and access functions would reside is the UICC (rather than on the terminal, etc.)
- It was proposed that the ISIM should be considered as a logical set of fields within the UICC in order to provide access to 3GPP Core Network, allowing IMS to be secured in the Rel-5 time frame. This would not preclude future separation of the functionality
- It was agreed that so far, "ISIM" denotes the subscription information and security functions required for IMS. It is believed that the ISIM functionality is essential for Rel-5 in order to make IMS functional.

ERICSSON

Outcome from SA#14

- It is the preference of TSG SA that T WG3 specify a solution that does not preclude that, in future Releases, the IMS subscription could be independent from the basic subscription currently stored in the USIM.

ERICSSON

Open issues in TS33.203

- Overview:
  - ❖ The content in Section 8 ISIM need to be stabilized
  - ❖ No solution in the main body on how to protect SIP signaling
  - ❖ From SA3#21 it was identified that the extended HTTP Digest draft needs to be enhanced such that it can properly resist replay and reflection attacks
  - ❖ HTTP Digest will not solve confidentiality of SIP messages. Is this a critical issue in Release 5 time frame?
  - ❖ IMS UE-split for Release 5? Remove from TS33.203?
  - ❖ The SA_ID and the handling of SAs should be specified in more detail

ERICSSON

Open issues in TS33.203

- Overview:
  - ❖ The requirements on IPSec in relation to encryption of SIP signaling needs to be specified further
  - ❖ What is the IETF view on signaling port numbers in SIP when SAs are switched in the IPSec case?
  - ❖ Reduce the number of editors notes

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

ERICSSON

How to proceed to get TS33.203 for approval to SA#15:

- The **time** requirement is clear TS33.203 shall be submitted for approval to SA#15

- The **scope** of the TS33.203 is currently not clear. There is currently no solution for SIP signaling protection in the main body. A working assumption should be defined as early as possible. Since CN1 is dependent on our Stage 2 requirements the current situation is not satisfactory.

ERICSSON

How to proceed to get TS33.203 for approval to SA#15:

- **Resource wise** it makes sense that SA3 adopts a working assumption for SIP signaling protection as soon as possible such that the detailed work can start

- If the **quality** of the TS is going to be good it is important that SA3 narrows the scope such that the supporting companies can focus. There is not much time left.

ERICSSON

How to proceed to get TS33.203 for approval to SA#15:

- The correct stage 2 flows based on the IETF work are missing since IETF work is currently ongoing. Keep track on what IETF is doing.
- Clear the most of the Editors Note at SA3#22
- Work on the details from now until SA3#22
- Make progress in IETF on SA3 related drafts