aSIP-Access Security for IP-Based Services

Krister Boman

Ericsson

Outline of the presentation:

❖ Overview of the updates in TTS33.203

❖ Overview of open issues that need to be resolved

❖ IETF activities

❖ How to proceed to get v1.0.0 in place

Updates of TS33.203

- Overview:

  ❖ The SIP-flows are more generic according to a CN1 requirement

  ❖ The ISIM scenarios as specified in earlier SA3 Liaison Statements have been incorporated

  ❖ The Registration flag indicating *Registered, Unregistered* and *Register Pending* has been included

  ❖ A new section *5.1.2 Re-authentication of the subscriber* has been defined

  ❖ In Section 6.1 the single SA requirement between the UE and the P-CSCF has been incorporated

Updates of TS33.203

- Overview:

  ❖ The IMPI has been moved to the EAP part of the SIP message

  ❖ Integrity protection at SIP level has been included in the Annex

  ❖ Generic Security Setup Procedures

ERICSSON

Open issues in TS33.203

- Overview:
  - ❖ Security for application servers is still open
  - ❖ The scenario that the P-CSCF can resist in the HN is missing
  - ❖ It is still open whether it shall be possible for the P-CSCF to require a re-authentication of IMS subscribers
  - ❖ Lack of contributions for Visibility and Configurability Section. Shall it be removed from the technical specification?
  - ❖ The editors note in Section *5.3 Network Topology Hiding* can be removed
  - ❖ How is the IK and the CK transported in SIP? An LS should be sent to CN1.

Open issues in TS33.203

• Overview:

❖ What does the *Register Pending* really mean?

❖ In Section *11.4.1.5 Network-initiated reauthentication* in 24.229v080 there are security requirements defined that are not in line with TS33.203

❖ In Section TS33.203 in *Security association set-up procedure* section should it in order to be generic allow Integrity Mechanism List and Confidentiality Mechanism List?

❖ Is there a potential threat that a user could in an INVITE send an IMPU that has no relation to the IMPI of that user?

ERICSSON

Open issues in TS33.203

• Overview:

❖ Security measures for the ISC-interface is still open

❖ Define a list of parameters that are tailored to the ISIM. This shall be put into the TS33.203

❖ What scenarios should be covered in the Release 5 framework for the UE functional split?

❖ Contributions on IP-address anonymity

❖ Contributions on Hiding Mechanisms required

❖ Lifetime of the Security association between the UE and the P-CSCF shall be defined

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 v1.0.0 in place:

❖ It is proposed that the rapporteur includes the decisions from this meeting into the TS33.203 and submits it to the SA3 reflector for email approval.

❖ SA plenary is scheduled for December 17-21 (Week 51)

❖ A draft TS33.203v1.0.0 shall be available on the SA3 reflector December 5 and allow for about one week email discussion

❖ TS33.203v1.0.0 available on the reflector December 14

How to proceed to get v1.0.0 in place:

❖ There is a common understanding in SA3 how the security architecture is defined however there are open issues left related to IETF