aSIP-Access Security for IP-Based Services

Krister Boman

Ericsson

Open issues in TS33.203

- Overview (Text in Read identifies **outcome from SA3#21bis**):

  ❖ The content in Section 8 ISIM need to be stabilized **(Open)**

  ❖ No solution in the main body on how to protect SIP signaling **(Open)**

  ❖ 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 **(Approx. Profiling left)**

  ❖ HTTP Digest will not solve confidentiality of SIP messages. Is this a critical issue in Release 5 time frame? **(Closed)**

  ❖ IMS UE-split for Release 5? Remove from TS33.203? **(Open)**

ERICSSON

Open issues in TS33.203

- Overview:

  ❖ The SA_ID and the handling of SAs should be specified in more detail **(Open)**

  ❖ The requirements on IPSec in relation to encryption of SIP signaling needs to be specified further **(Closed)**

  ❖ What is the IETF view on signaling port numbers in SIP when SAs are switched in the IPSec case? **(Open)**

  ❖ Reduce the number of editors notes **(Open)**

  ❖ Requirements on unprotected re-registrations and SA-handling **(Open)**

ERICSSON

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

❖ 3GPP Requirement IETF drafts related to security
❖ Digest AKA
❖ Algorithm agreement
❖ Extended HTTP Digest

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

Proposed order:

❖ Discuss status in **IETF** and agree on **updates to TS33.203** reflecting the status in IETF

❖ Agree on working assumption for **SIP signaling protection** i.e. IPSec or Extended HTTP Digest

❖ Agree on principles on **unprotected re-registration** and **SA handling**. Accept that details can be sorted out by **CRs** at future meetings.

❖ Evaluate the working assumption that a **wrong RES** is not sent to the authenticator

❖ Agree on **ISIM** requirements

ERICSSON ≋

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

Proposed order:

❖ **Drafting session** Tuesday evening (Everyone encouraged to propose items for an agenda)

  ❖ Review and agree on **TS33.203v110** as in S3-020078 and other contributions or general comments on e.g. Editorial Notes etc.

  ❖ Refer to IETF drafts or include them in an Annex?

  ❖ Depending on chosen mechanism but should TS33.203 in order to help CN1 include an Annex for profiling Extended HTTP Digest?

  ❖ + any other raised issue

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

Updating of TS33.203:

❖ Editor aims to send out a **new version** on Monday **March 4**

❖ **Editorial comments** allowed until Wednesday **March 6**

❖ A version **ready for approval** to SA plenary SA#15 available on Thursday **March 7**