3GPP TSG SA WG3 Security **S3-000753**

Title: Evaluation of IMS security architectures

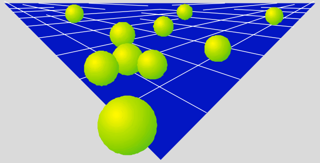
A comparison between the proposals in [S3z000010] (Ericsson) and [S3z000022] (Siemens)

Source: Siemens AG

Document for: Discussion and decision

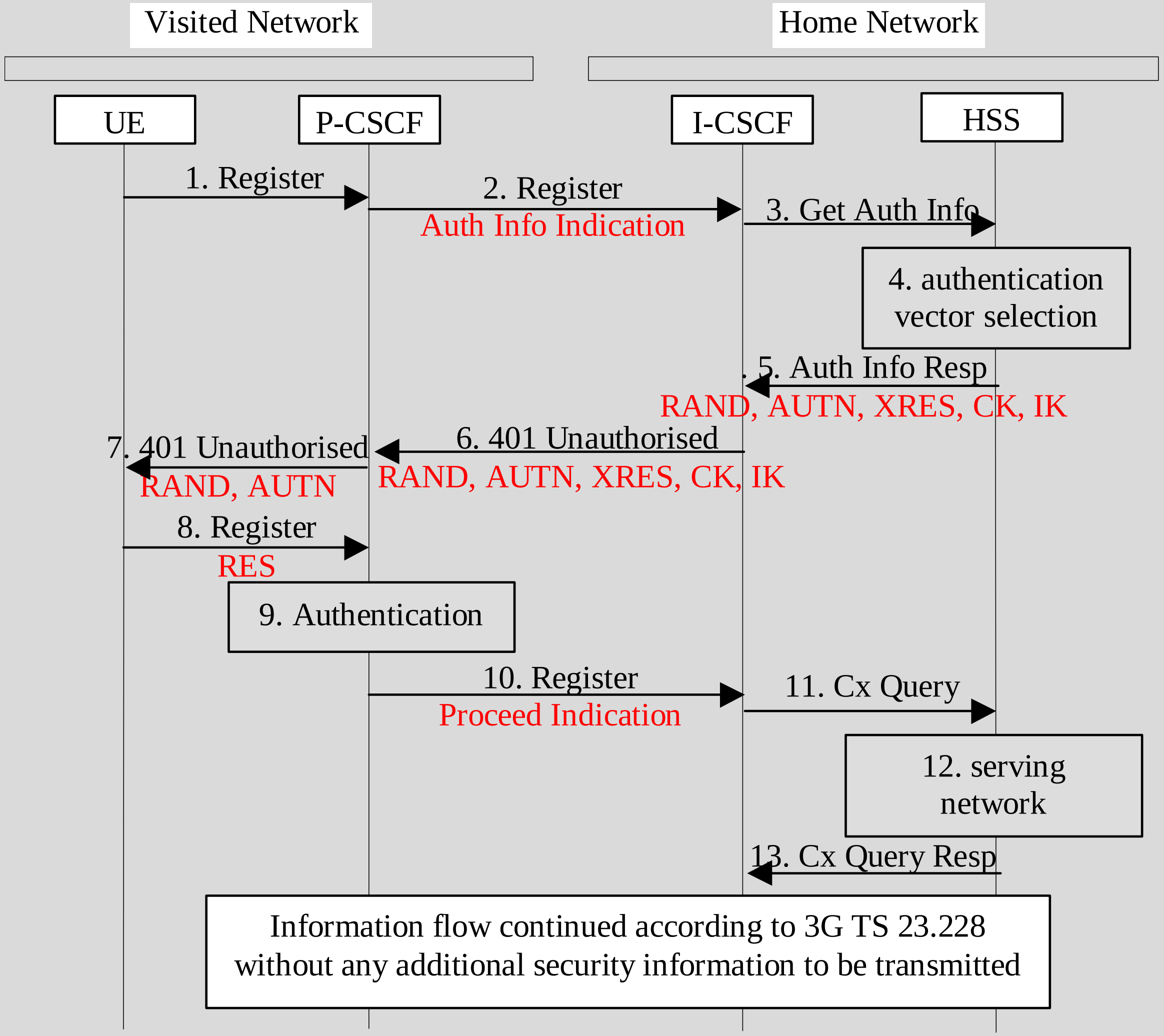
Agenda item: 10.8

Evaluation criteria for IMS access security architectures



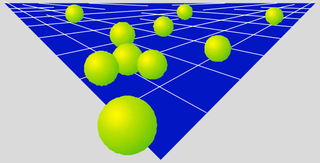
- **Minimise performance impact of IMS security**
- **Minimise system complexity**
- **Allow for access network independence**
- **Minimise number and types of network entities which have trust**
- **Satisfy trust requirements**

SIP Registration: Information flow with authentication (No authentication vectors available at P-CSCF)



Information flow continued according to 3G TS 23.228 without any additional security information to be transmitted

Minimise performance impact of IMS security



- Ericsson proposal [S3z000010]:
  - ➘ Higher HSS load, as for each authentication attempt the HSS has to be contacted
  - ➘ HSS performance could be reduced, as HSS has to send out requests and wait for responses, for a potentially large number of users simultaneously (Change of HSS paradigm from stateless to stateful server)
  - ➘ Integrity protection may have to be performed twice (P-CSCF and S-CSCF)
  - ➘ UE has to carry out security mode set-up procedure twice
  - ➘ WTLS for confidentiality protection in P-CSCF necessitates additional handshake
- Siemens proposal [S3z000022]
  - ➚ No unnecessary overhead by performing all IMS access security in one network entity (P-CSCF)

Minimise system complexity

- Ericsson proposal [S3z000010]:

  ➘ Information flow for security depends on the location of the service control

  ➘ Two procedures to transfer integrity/confidentiality keys from HSS required (to both S-CSCF and P-SCSF)

  ➘ Re-authentication more complicated
  HSS has to be triggered by the visited network and the result has to be distributed to two different entities in the visited network;
  requires synchronisation between both network entities holding the session keys

  ➘ Two security mode set-up procedures required (from S-CSCF and P-SCSF)

- Siemens proposal [S3z000022]:
  ______➚ Always the same information flow , only one procedure

Allow for access network independence

- Requirement loosely specified by SA2;
  no mechanisms available

- Ericsson proposal [S3z000010]:
  - → supported
    - ➚ By performing IMS AKA in the HSS, integrity in S-CSCF in home

- Siemens proposal [S3z000022]:
  - → supported
    - ➚ By performing IMS AKA in the P-CSCF

      P-CSCF may be located in home, integrated with I-CSCF, directly addressable by UE for non-UMTS access,

Minimise number and types of network entities which have trust

- <u>Ericsson proposal [S3z000010]:</u>

  - ➘ HSS as well as S-CSCF and P-CSCF are involved in IMS access security

  - ➘ keys, algorithms have to be stored/executed in both network entities, P-CSCF and S-CSCF

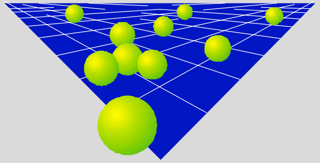
- <u>Siemens proposal [S3z000022]:</u>

  - ➚ Only HSS and P-CSCF are involved in IMS access security

Evaluation of trust requirements (1)

- Both proposals satisfy the trust model implicit in UMTS Rel‘99
- No different trust model for the IM domain has been proposed to S3
- Both proposals locate IM domain specific security functions in home network when access is over a non-UMTS network (e.g. via the Internet)
- The proposals differ in the degree of home control when IM domain services are accessed via a UMTS visited network
- In the latter case, UMTS Rel‘99 trust model should be fine.

Evaluation of trust requirements (2)



- **Usefulness of home control is limited:**

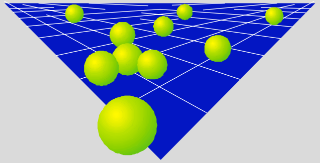
  - home control of authentication does not give information about successful establishment of call;

  - home control of call signalling does not give information about type and grade of service actually provided nor about service usage (amount of data);

  - fraudulent visited network operator could still incorrectly charge home operator;

  - home control is about protecting home operators against “incorrect“ visited operators; what about the converse?

Conclusions



- **Result of evaluation process:**
  - Siemens proposal [S3z000022] has decisive advantages in reducing complexity of architecture,
  - perceived advantages of higher degree of home control in Ericsson proposal [S3z000010] do not justify higher complexity