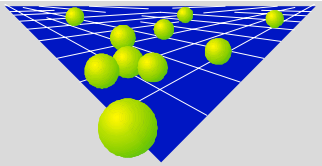
S

3GPP TSG SA WG3 Security
Ad-hoc meeting S3#15bis, Munich, 8-9 November, 2000



S3z000035

IMS authentication and integrity/confidentiality protection

Siemens contribution S3z000022
(Discussion/Decision)

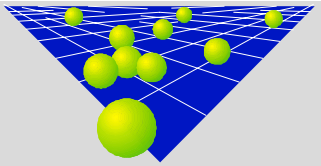
Günther Horn, Dirk Kröselberg, Klaus Müller

Siemens AG, Corporate Technology

Competence Centre Security

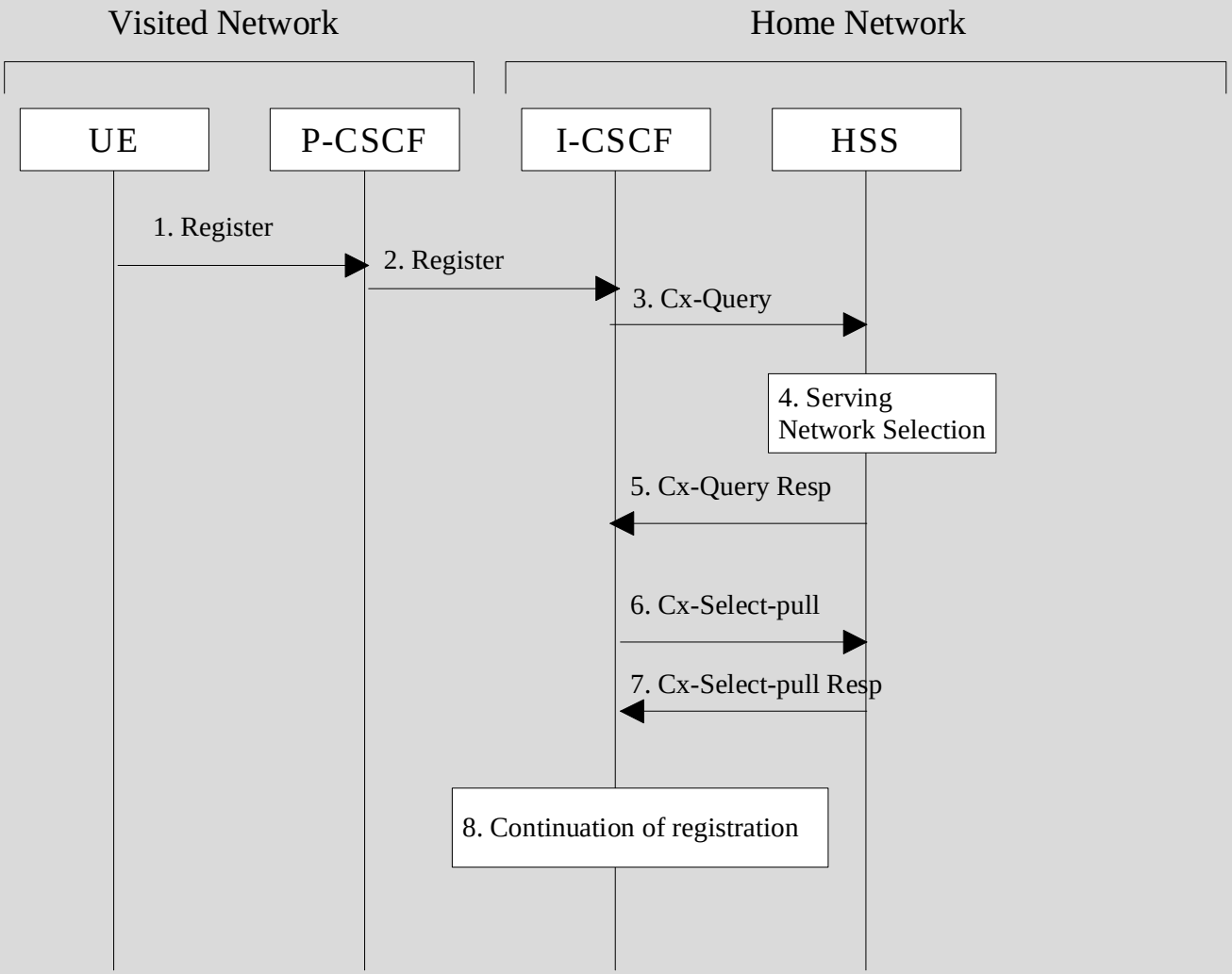
S

S3z000022: Scope and pre-requisites



- **Scope: Questions to be answered**
  - Which network entity should perform authentication and key agreement (AKA) with the UE for SIP registration of a (roaming) user?
  - Which network entity should terminate the access integrity/confidentiality protection of SIP messages with the UE?
- **Pre-requisites: 3GPP SA 3 working assumption from [3G TR 33.8xx, section 8]**
  - UMTS AKA protocol [3G TS 33.102] is performed through the SIP protocol (IMS AKA mechanism)
  - A new authentication mode for SIP has to be standardised
- **Siemens Proposal in S3z000022:**
  - P-CSCF performs the IMS AKA with the UE and
  - P-CSCF is the point of termination for integrity/confidentiality protection of SIP messages from the UE
  - For the further SIP hops in the network, integrity/confidentiality protection shall be provided by network domain security features using IPSec.

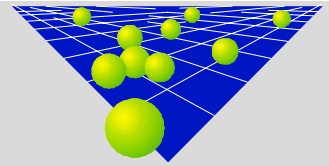
SIP Registration: Information flow without authentication (according to TR 23.228 v1.2.0, 10/2000)

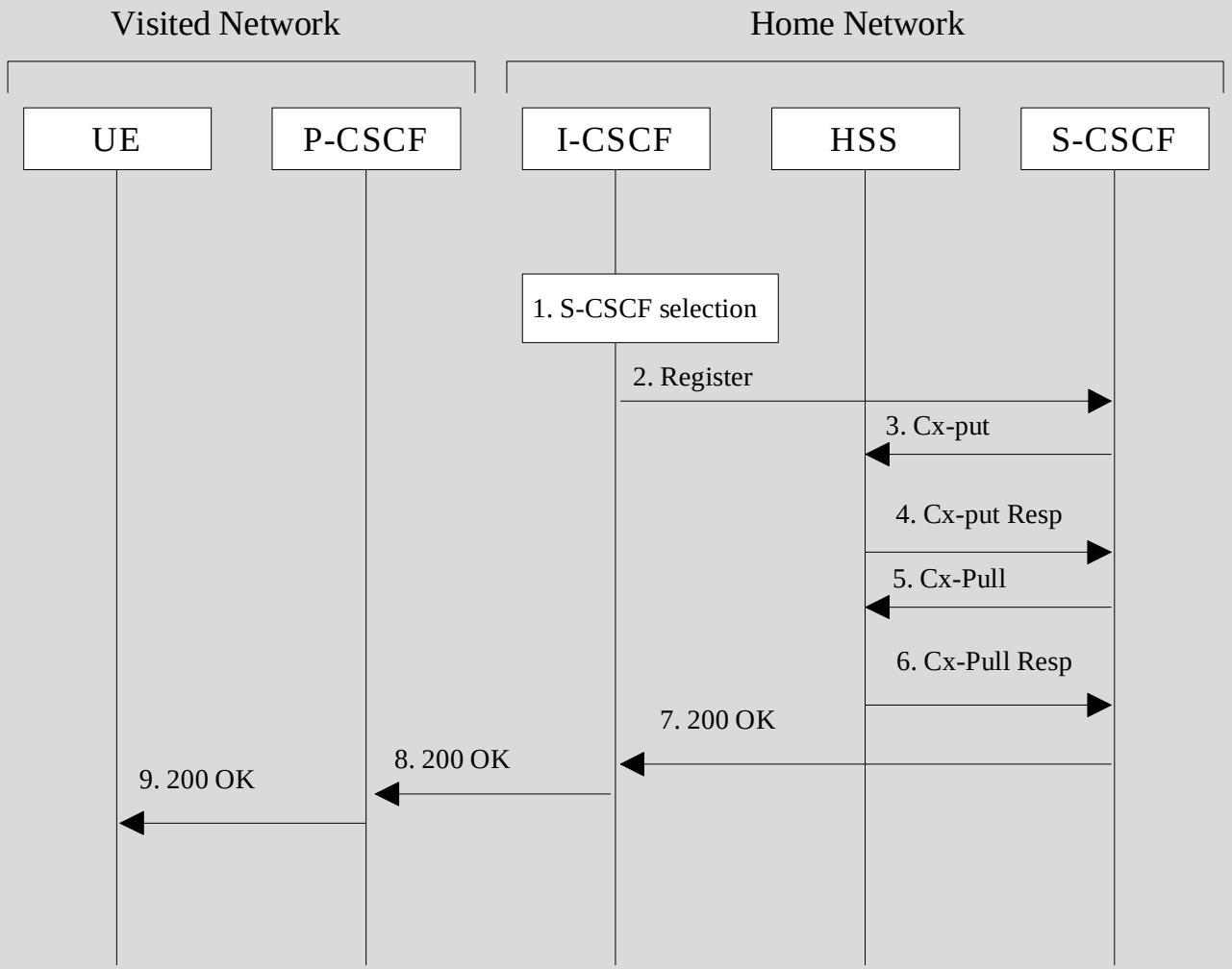


Müller, Kröselberg, ZT IK 3

S

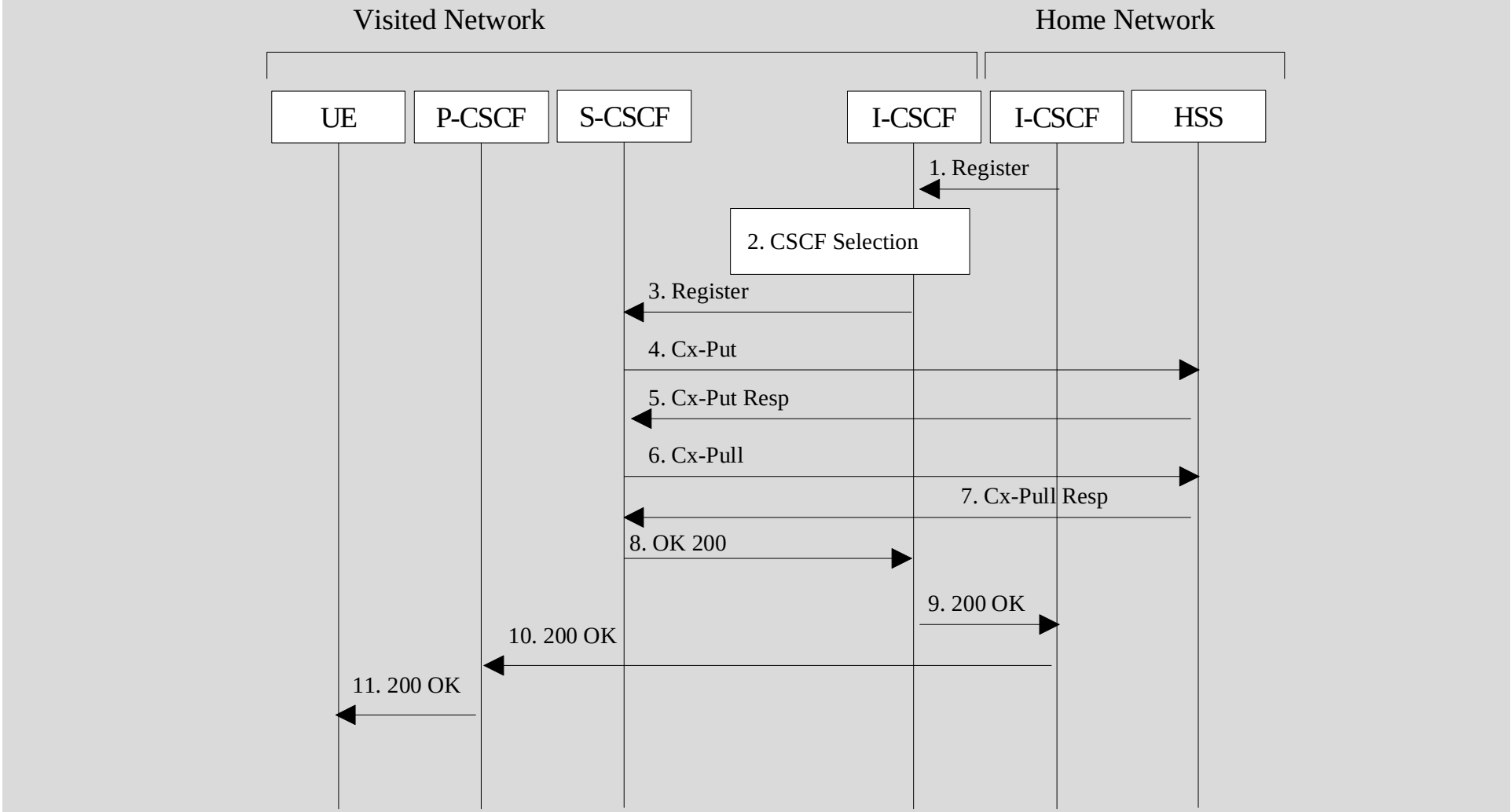
SIP Registration: Information flow without authentication (cont. for case S-CSCF in the home network)





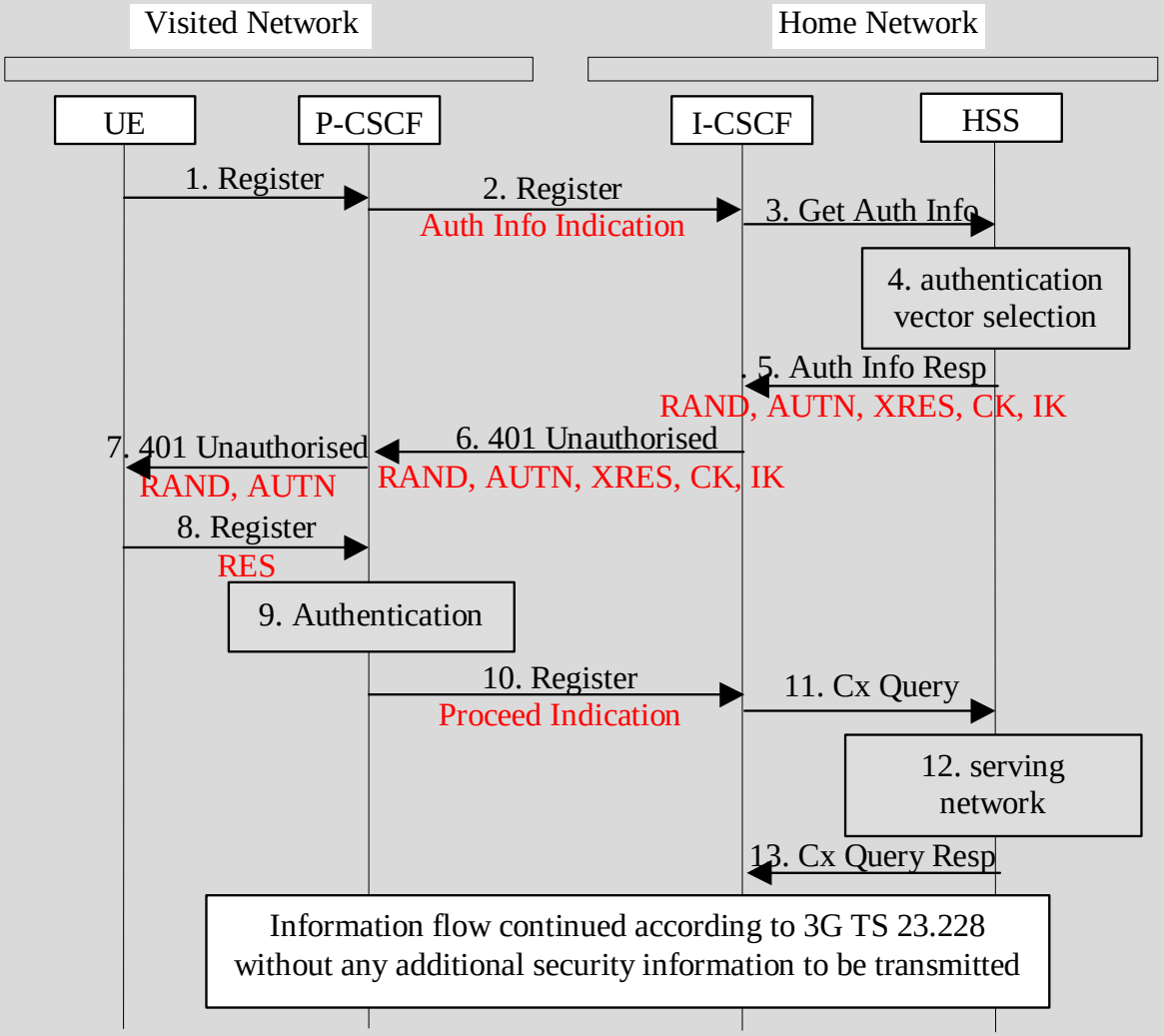
S

SIP Registration: Information flow without authentication (cont. for case S-CSCF in the visited network)



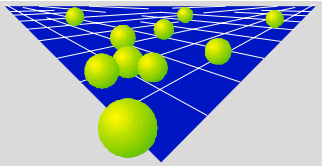
S

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



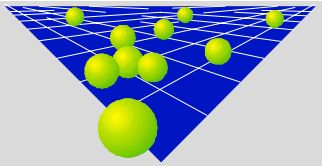
S

Location of integrity/confidentiality functionality for IMS (1)



- **Drawbacks if confidentiality and integrity protection is not co-located in the same network entity**
  - Two different network entities have to be provided with the appropriate security functionality
    - ➔ Additional mechanisms required for control of access, secure storage,reliability, etc.
  - IMS equivalent to security mode set-up procedure in UMTS PS- and CS-domain has to be implemented in both network entities
    (This feature still has to be defined for the IM domain!)
  - UE has to carry out the security mode set-up procedure twice
    (once with each of the two network entities)
  - Key management for integrity and confidentiality keys could become complicated
    - ➔ UMTS re-authentication initiated by VLR or SGSN
    - ➔ Analogous feature required for IMS
    - ➔ Requires synchronisation between both network entities holding the session keys

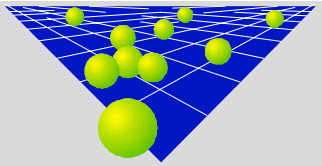
Location of integrity/confidentiality functionality for IMS (2)



- **Additional cons for Ericsson proposal [S3z000010] (additional to the ones mentioned in the last foil)**
  - Two different security related information flows have to be specified
    - ➔ S-CSCF may be located in visited or in home network
  - Not clear why one should have two different mechanisms, one at the application layer and one at the transport layer.
  - Seems odd to integrity-protect SIP messages twice, once at the application layer between the UE and the S-CSCF and a second time (optionally) by means of WTLS between the UE and the P-CSCF
  - Should be questioned whether WTLS is the right choice
    - ➔ WTLS necessitates another handshake to derive confidentiality and integrity keys from *CK* which is used as a master key for WTLS. This seems unnecessary.

S

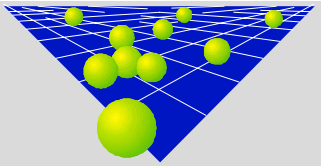
Location of integrity/confidentiality functionality for IMS (3)



- **Reasons for terminating integrity/confidentiality protection with UE in P-CSCF**
  - Access network confidentiality protection with the UE should be terminated in the visited network, at least for lawful interception reasons
    - ➔ Only network entity always available in the visited network is the P-CSCF
- **Pros for Siemens proposal**
  - All the drawbacks on the last two foils are not valid for the Siemens proposal
  - The security related information flow is always the same
    (Independent from the fact where the S-CSCF is located)

S

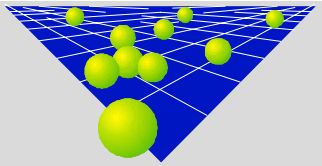
Location of IMS AKA functionality (1)
Comparison between IMS AKA in P-CSCF or in HSS



- **Pros for IMS-AKA in the P-CSCF (Siemens proposal [S3z000022])**
  - Handling of the AKA seems to be a tolerable additional burden for the P-CSCF
    - ➔ P-CSCF has to be enhanced to handle the confidentiality and integrity functions anyway
  - Paradigm for AuC applied so far in UMTS and GSM could be preserved
    - ➔ HSS/AuC is just a database which responds to queries
  - No procedure to transfer the integrity/encryption keys required
    - ➔ All IMS security performed in P-CSCF (AKA as well as integrity/confidentiality protection)
  - Visited network can control lifetime of CK and IK by triggering a re-authentication; possible without having to contact the home network
  - Re-use of the mechanisms e.g. for generating security information in the HSS/AuC but also in the USIM possible
    - ➔ IMS AKA is analogous to UMTS authentication
  - Visited network has control over mobiles roaming in its network

S

Location of IMS AKA functionality (2)
Comparison between IMS AKA in P-CSCF or in HSS



- **Cons for IMS-AKA in the HSS (Ericsson proposal [S3z000010])**
  - Paradigm for AuC applied so far in UMTS and GSM could not be preserved
    - ➔ HSS/AuC is no longer just a database which responds to queries
  - For each authentication attempt the home network HSS has to be contacted
  - Procedure to transfer the integrity/encryption keys required
    - ➔ Integrity/confidentiality protection is located in an entity different from IMS AKA location
  - HSS/AuC performance could be reduced
    - ➔ HSS/AuC has to send out requests and wait for responses, for a potentially large number of users simultaneously
  - Re-authentication more complicated
    - ➔ The HSS has to be triggered by the visited network and the result has to be distributed to two different entities in the visited network