ERICSSON

S3z010040

An analysis on where to perform the authentication of an IMS subscriber

A presentation to SA3 by

Krister Boman

Ericsson

Status from SA3#17 meeting in Göteborg:

- Authentication shall take place in the Home Network
- It was left for further study if authentication should take place in the HSS or in the S-CSCF
- The working assumption has been (for some time) that the authentication mechanism is based on a SIP extension, the so called SIP AKA or IMS AKA

Scope of presentation:

This presentation analyses the proposal to authenticate an IM subscriber in the S-CSCF as in S3z01003 (Siemens) and the proposal to do it in the HSS as in S3z010025 (Ericsson).

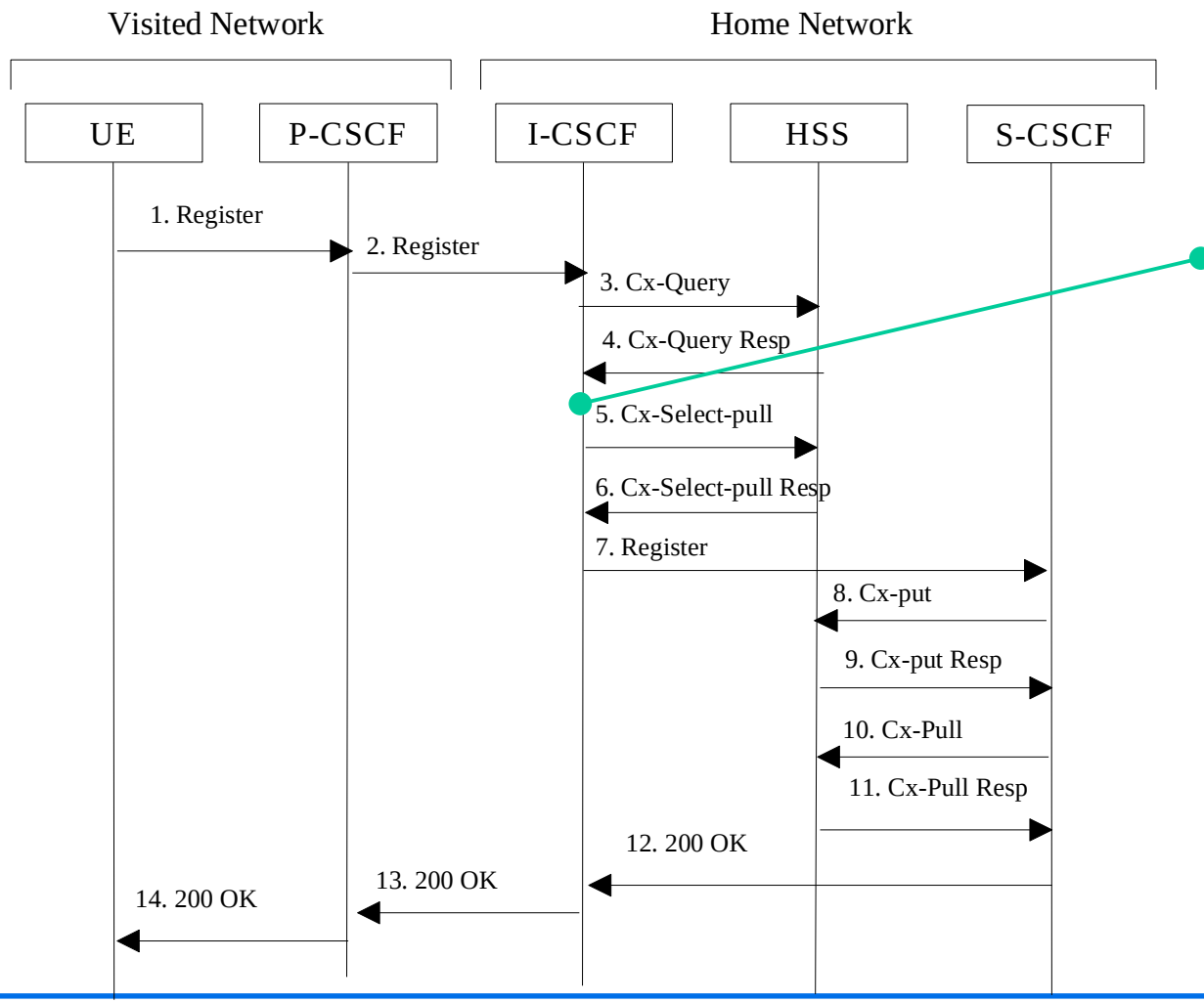
This presentation is based on S3z010025 (Ericsson) with Session Establishment Authentication included which is not covered by S3z010025 (Ericsson).

Outcome of the analysis:

- Perform authentication in the HSS
- To perform it in the HSS as in S3z01025 is compliant with the 23.228 v500 and no changes are needed
- To perform it in the HSS is the most efficient solution in terms of amount of signaling and use of network resources
- To perform it in the S-CSCF as in S3z01003 is not compliant with the 23.228 v500 and changes are needed. The sensitivity to DoS attacks is increased

Requirements from 23.228v500:

Registration – User not registered

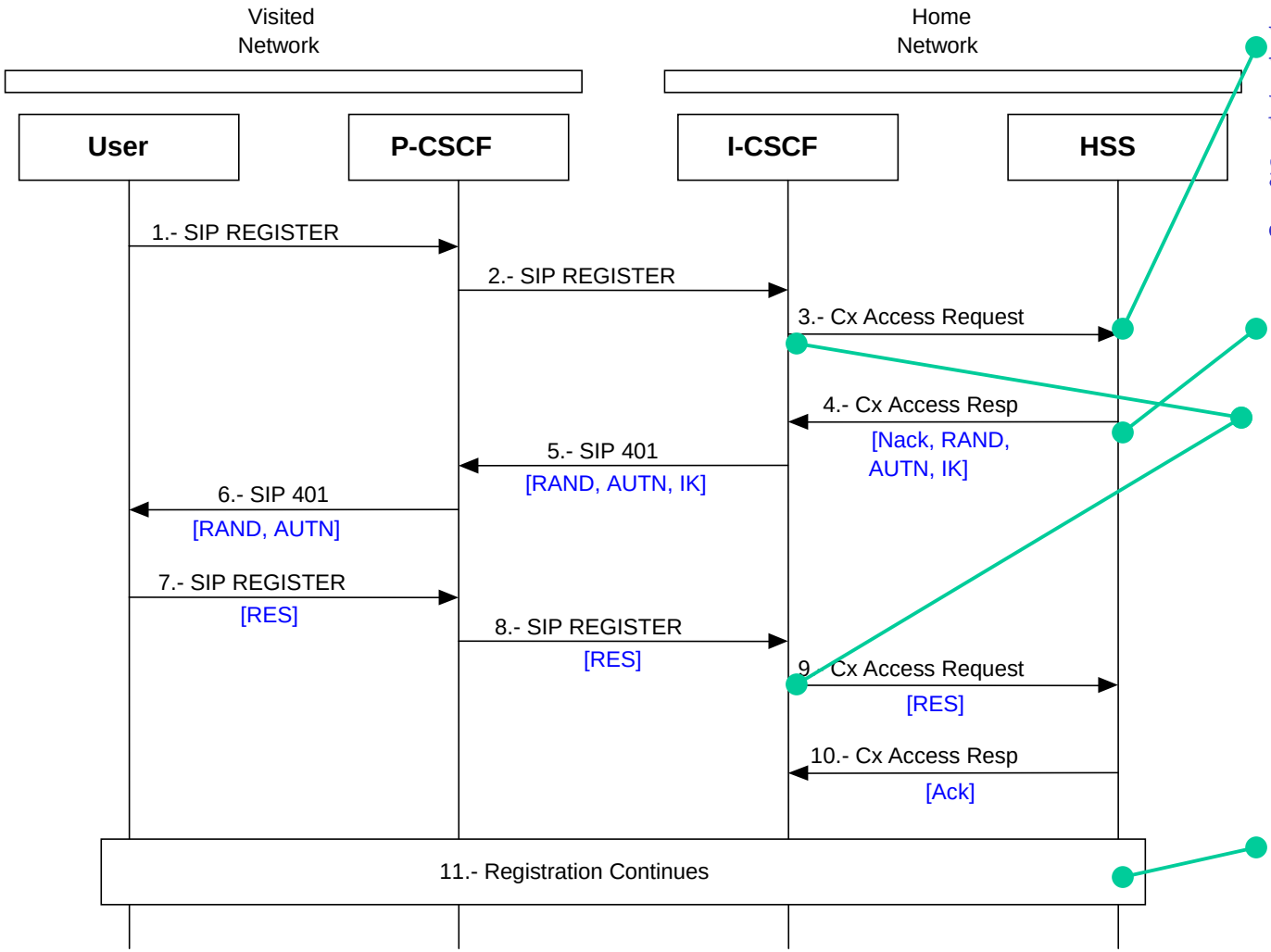


At this stage or earlier the user has been authenticated according to 23.228

Requirements from 23.228v500:

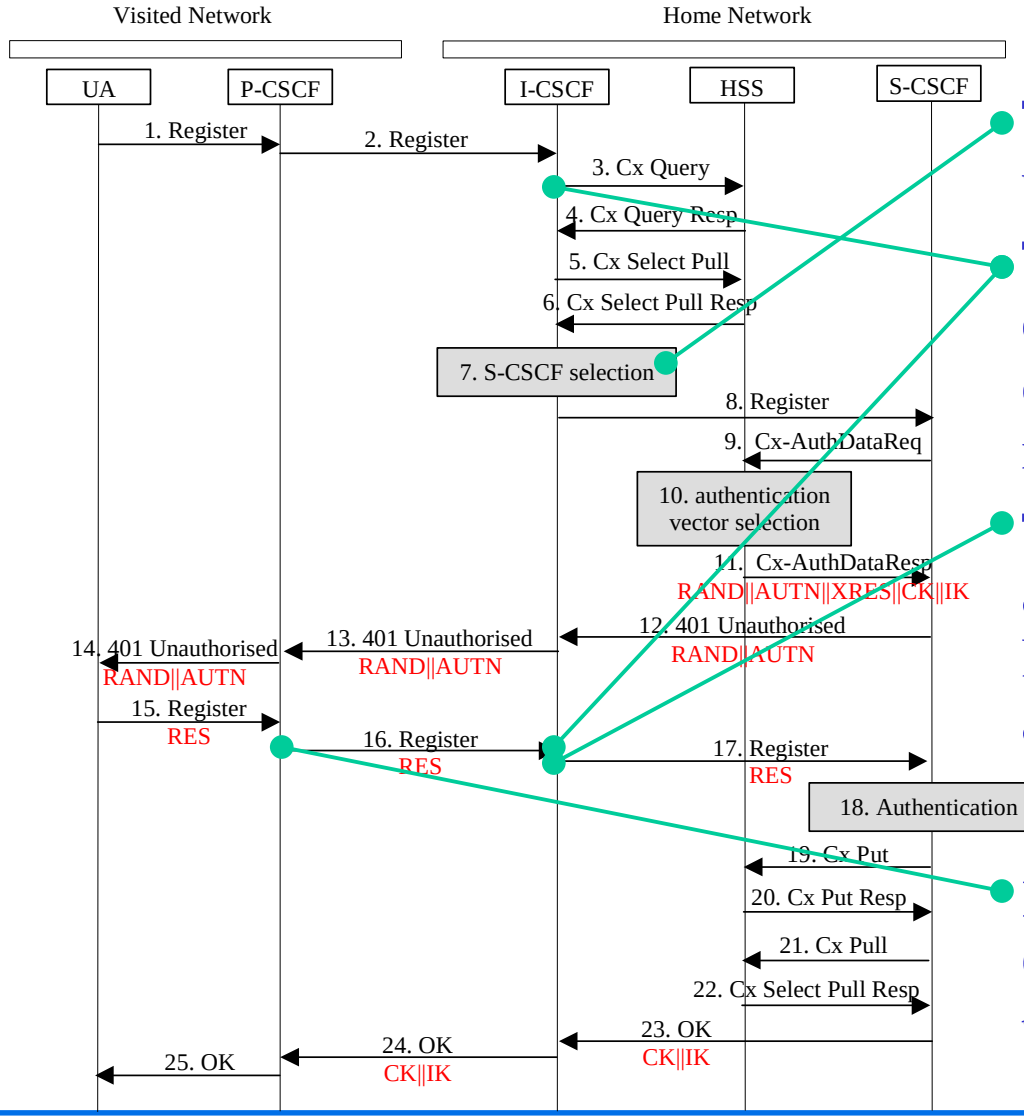
- After a registration transaction the I-CSCF shall not store any state information
- The HSS shall, after receiving a Cx-Put store the S-CSCF name/address
- The P-CSCF shall store the network entry point
- The P-CSCF shall not take into account previous registrations when routing SIP-registration messages

Successful Authentication in the HSS (Non-registered User):



- HSS checks if the user is allowed to register & generates a challenge and stores the XRES
- The dialogue is closed
- No states in the I-CSCF.
  The I-CSCF always behaves in the same way for SIP Register i.e. sends a Cx message towards the HSS
- The user is authenticated before a S-CSCF is selected

Successful Authentication in the S-CSCF (Non-registered User):



- The S-CSCF is selected before the user has been authenticated
- The I-CSCF treats the SIP Register differently depending on which state of the authentication process. This is not compliant with 23.228.
- The I-CSCF does not store the address of the S-CSCF and can not know where to send the response according to 23.228.
- It can not be guaranteed that the P-CSCF will send the SIP Register to the same I-CSCF.

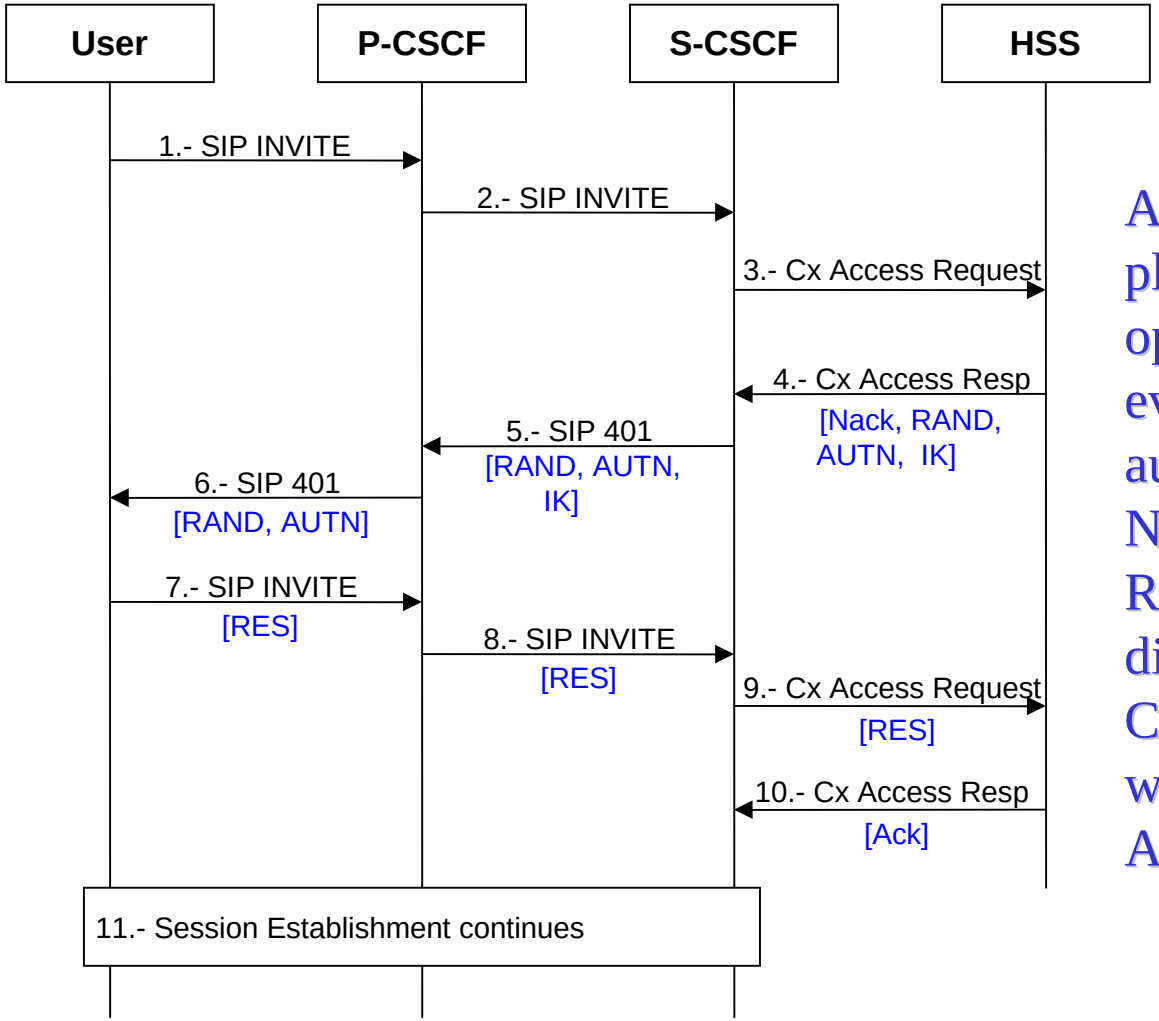
Authentication & Synchronization Failure:

The table shows the number of messages needed to make the HSS aware of the indicated type failure

	Network auth. Failure	UE auth. Failure	Synchronization Failure
HSS	9	9	16
S-CSCF	*16* +S-CSCF selection	*16* +S-CSCF selection	*23* +S-CSCF selection

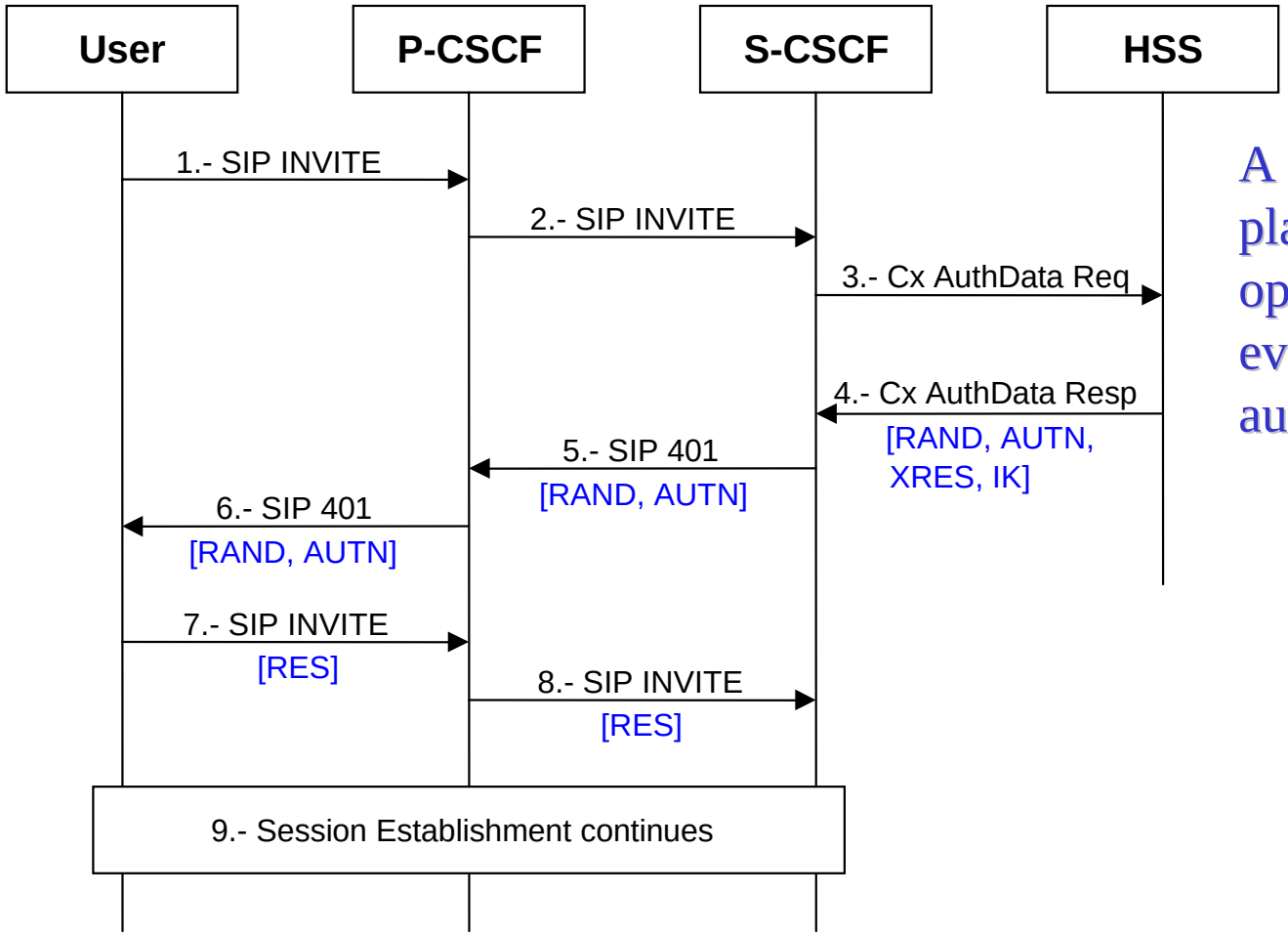
Note: *For the S-CSCF case it has been assumed that the signalling flow in S3z01003 is used. However as shown in this analysis this flow has to be revisited and hence the figures above for the S-CSCF case seems to be increased then. Therefore the number of messages for the S-CSCF case is in Italic. The process for S-CSCF selection always has to be performed.*

Authenticating the Session Establishments (HSS alternative):



A parameter should be in place such that the operator can decide that every *n* establishment is authenticated.
Note that as in the Registration case the dialouge towards the S-CSCF is always closed when HSS sends the Cx-Access-Response.

Authenticating the Session Establishments (S-CSCF alternative):



A parameter should be in place such that the operator can decide that every *n* establishement is authenticated.

Conclusions (HSS alternative):

- The most efficient solution in terms of signalling overhead and use of network resources.
- The solution is fully compliant with [3G TR 23.228] and no changes in the TS are needed
- No states are introduced to the P-CSCF and the I-CSCF.
- The corresponding XRES have to be stored in the HSS. This however has a limited impact since there will be no penalty in real time performance but some penalty on the amount of memory needed in the HSS
- It should be noted that the S-CSCF should have a similar XRES mechanism.
- The signalling towards the HSS increases when authenticating the session establishments

Conclusions (S-CSCF alternative as in S3z010003):

- Introduces a lots of extra signalling for a bogus user compared to the HSS alternative. This is significant both for the registrations and the different types of failures
- S-CSCF is assigned before the user has been authenticated which means unnecessary access to network resources for bogus users
- The non optimised use of resources creates unnecessary sensitivity to DoS attacks and a security breach
- The flow described in S3z010003 is not compliant with 3G TR 23.228. The flow could work if e.g. the P-CSCF and the I-CSCF becomes stateful
- A new mechanism is needed since the I-CSCF would behave differently for SIP Register messages. Sometimes the I-CSCF should route REGISTER towards the S-CSCF and sometimes send a Cx message to the HSS.

Conclusions:

• Only one node either the HSS or the S-CSCF should be responsible for authenticating a subscriber (at registrations and session establishments)

• The disadvantages and the security concerns with the S-CSCF alternative i.e. non optimised of network resources and sensitivity to DoS attacks make Ericsson to conclude that the HSS node shall perform the authentication of the user

• It is not clear whether authentication at session establishments is needed since the integrity protection is provided hop-by-hop. This feature could also be established by an optimised use of re-registrations.