ERICSSON

S3-010358

aSIP-Access Security for IP-Based Services

Activities and the new timeplan

Krister Boman

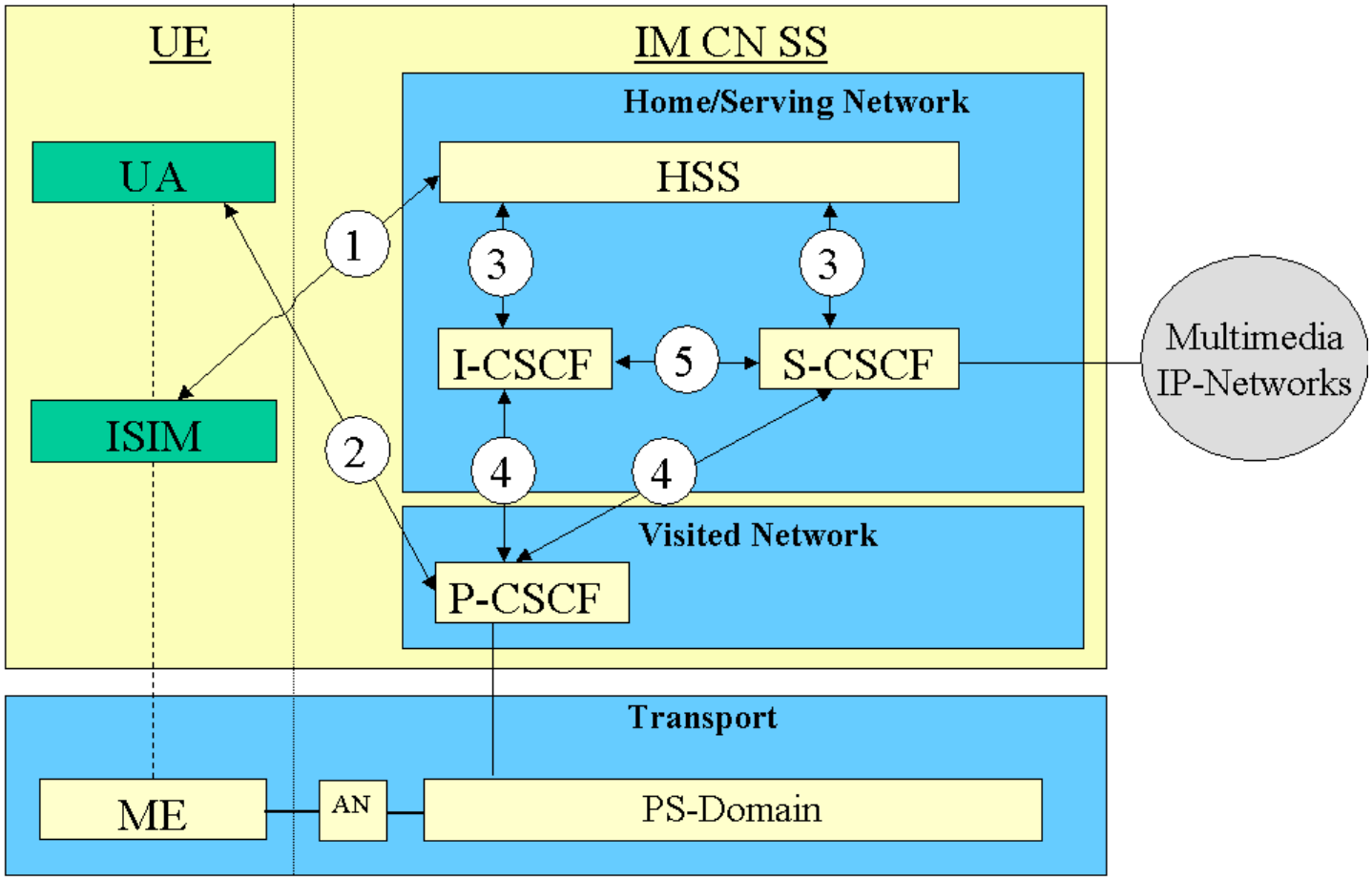
Ericsson

• The TS 33.203 v0.4.0 will be presented to SA3 this week (SA3#19) and it has not yet been approved. The material presented here is based on TS33.203 v0.4.0 and should therefore be understood as being the views of the rapporteur.

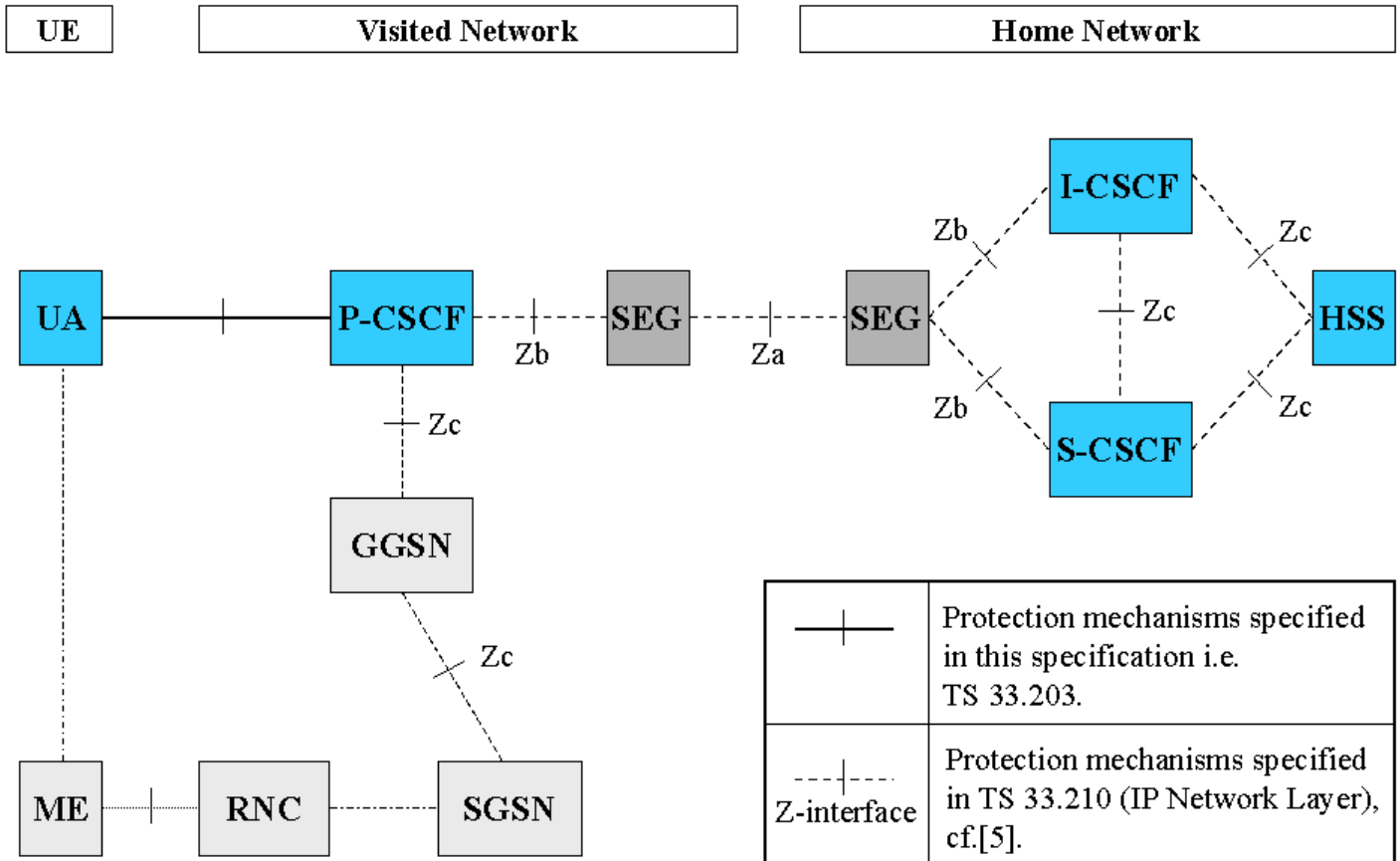
• It should be stressed that the TS33.203 v0.4.0 is a draft and hence changes may and will take place. Some important issues have not been resolved yet.

• It is for R5 and Stage 2 shall be approved at the SA plenary in March 2002 and Stage 3 specifications in June 2002.

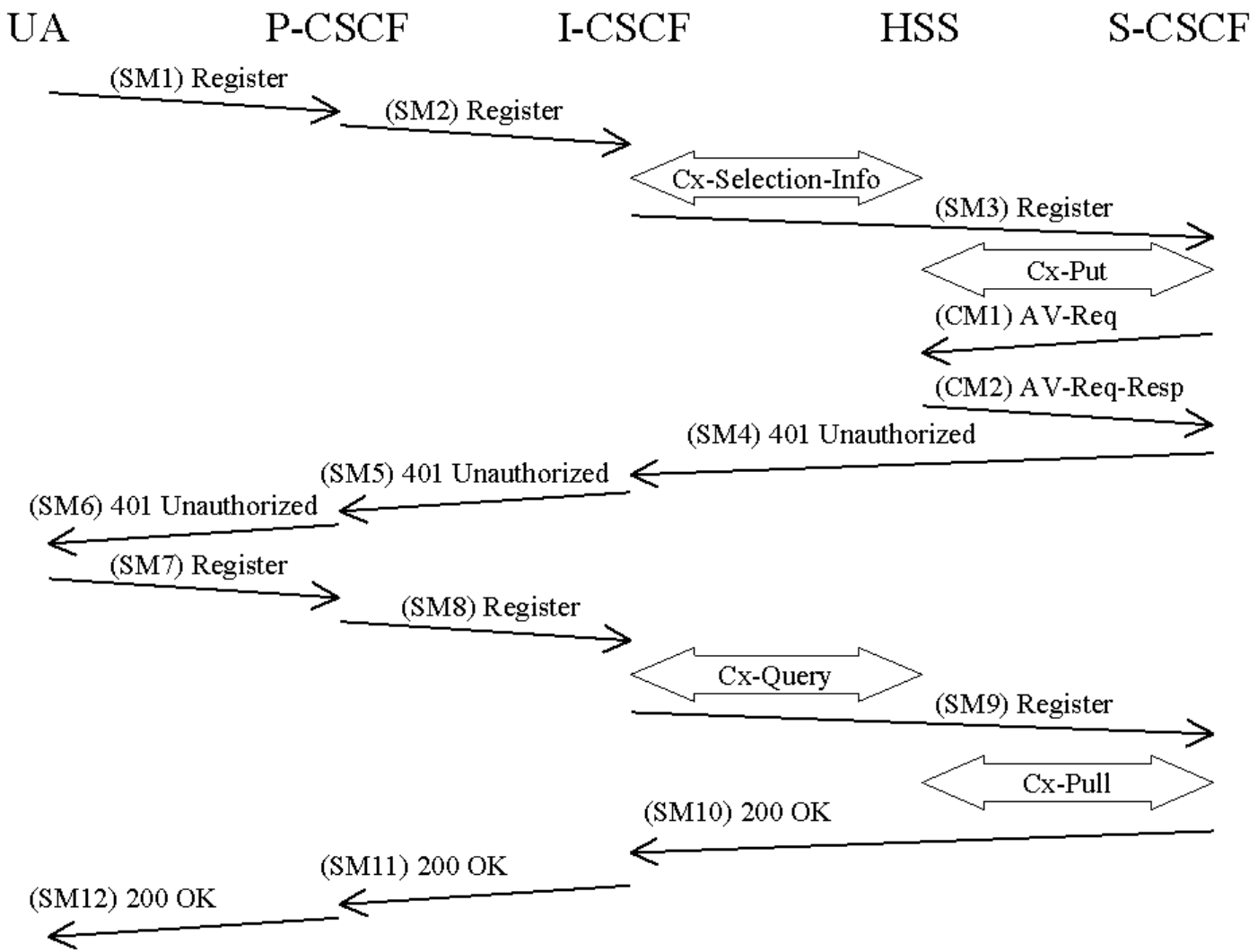
Overview of the security architecture



Overview of the security architecture



	Protection mechanisms specified in this specification i.e. TS 33.203.
Z-interface	Protection mechanisms specified in TS 33.210 (IP Network Layer), cf.[5].
	Protection mechanisms specified in TS 33.102, cf. [1].


UA
P-CSCF
I-CSCF
HSS
S-CSCF
(SM1) Register
(SM2) Register
Cx-Selection-Info
(SM3) Register
Cx-Put
(CM1) AV-Req
(CM2) AV-Req-Resp
(SM4) 401 Unauthorized
(SM5) 401 Unauthorized
(SM6) 401 Unauthorized
(SM7) Register
(SM8) Register
Cx-Query
(SM9) Register
Cx-Pull
(SM10) 200 OK
(SM11) 200 OK
(SM12) 200 OK

Status on aSIP in SA3:

- Authentication is terminated in the S-CSCF.
- EAP is used for transporting the authentication parameters in SIP.
- Confidentiality protection is optional for implementation
- Security protection in a hop-by-hop fashion.
- Authenticating session establishments is not needed. (However this working assumption was challenged at SA3#18)

Open issues for aSIP:

- Security mode setup i.e. how shall the UE and the P-CSCF in a secure manner decide on which algorithm(s) to use. Will be discussed at SA3#19.

- At what level shall protection take place? SIP or IPLevel protection is currently both open alternatives. Will be discussed at SA3#19.

- Authentication flows including failure scenarios

- The principles for the handling of SAs between the UE and the P-CSCF. The relation between IMPIs and IMPUs has to be clarifed.

- Authentication during long calls.