ERICSSON

S3-020400

SA handling

SA3#24 Helsinki

9th – 12th July, 2002

Vesa Torvinen

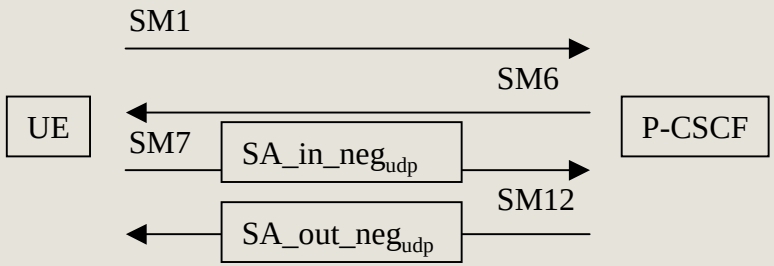
Ericsson

ERICSSON

Conclusions

- Problems in SA handling:
  - Quite many SAs
  - Becoming complex and hard to analyse
  - SA handling operations outside REGISTER messages
  - Must store the old SAs in case they are used later
- Solution:
  - P-CSCF: delete old SAs after SM10
  - UE: delete old SAs after SM12
- Problem with the solution:
  - Attacker may ‘delete’ old SAs with unprotected registrations
  - Attack not possible if the old SAs are mandatory for SM1 & SM6
  - If the old SAs can not be used, they can be removed anyway

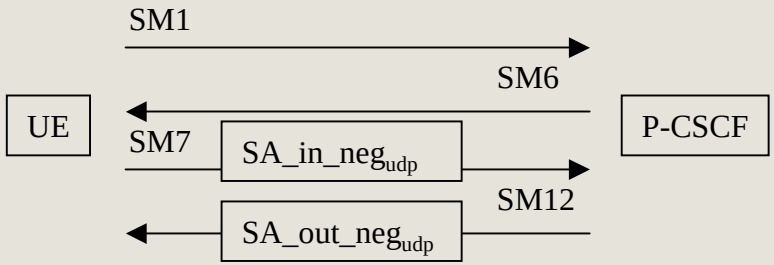
P-CSCF: Unprotected registration, old SAs exist



- When the new SAs are known to be OK (i.e. no attacker)?
  - Inbound: After SM7
  - Outbound: After the next incoming message after SM12
- When the old SAs can be removed?
  - Inbound: After the next incoming message after SM12 (because UE may still use the old SA until it has received SM12)
  - Outbound: After the next incoming message after SM12

ERICSSON

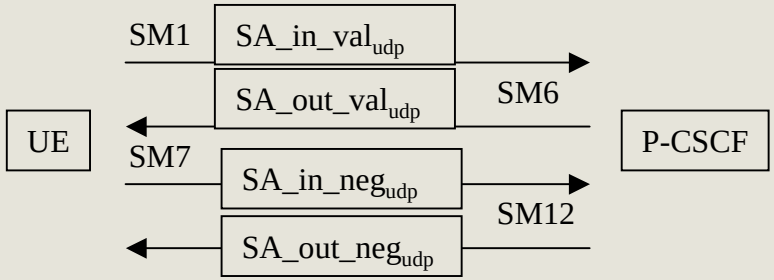
UE: Unprotected registration, old SAs exist



- When the new SAs are known to be OK?
  - Inbound: After SM12
  - Outbound: After SM12
- When the old SAs can be removed?
  - Inbound: After the next incoming message after SM12 (because P-CSCF does not know if SM12 was ever received, and may use the old SA)
  - Outbound: After SM12

ERICSSON

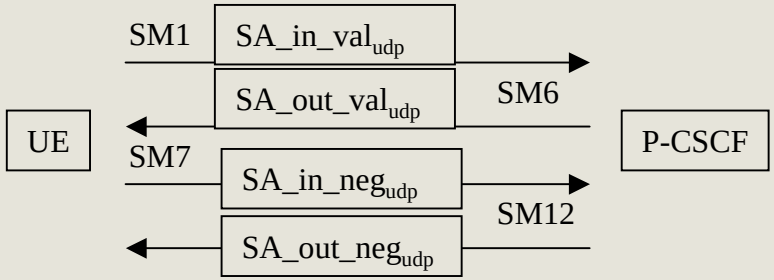
P-CSCF: Protected registration



- When the new SAs are known to be OK?
  - Inbound & Outbound: After SM7 (because SM1 & SM6 were protected)
- When the old SAs can be removed?
  - Inbound & Outbound: After SM10 (because 1: UE and P-CSCF know the same key IK, 2: the home network was able to authenticate the user, and 3: messages SM1 and SM6 were protected and consequently no attacker could have modified the SA parameters)

ERICSSON

UE: Protected registration



- Q1: When the new SAs are known to be OK?
  - Inbound & Outbound: After SM6
- Q2: When the old SAs can be removed?
  - Inbound: After SM12 (because P-CSCF does not know if SM6 was ever received, and may use the old SA for INVITEs)
  - Outbound: After SM6