# aSIP-Access Security for IP-Based Services

Krister Boman

Ericsson

ERICSSON

## Description of IMS security architecture

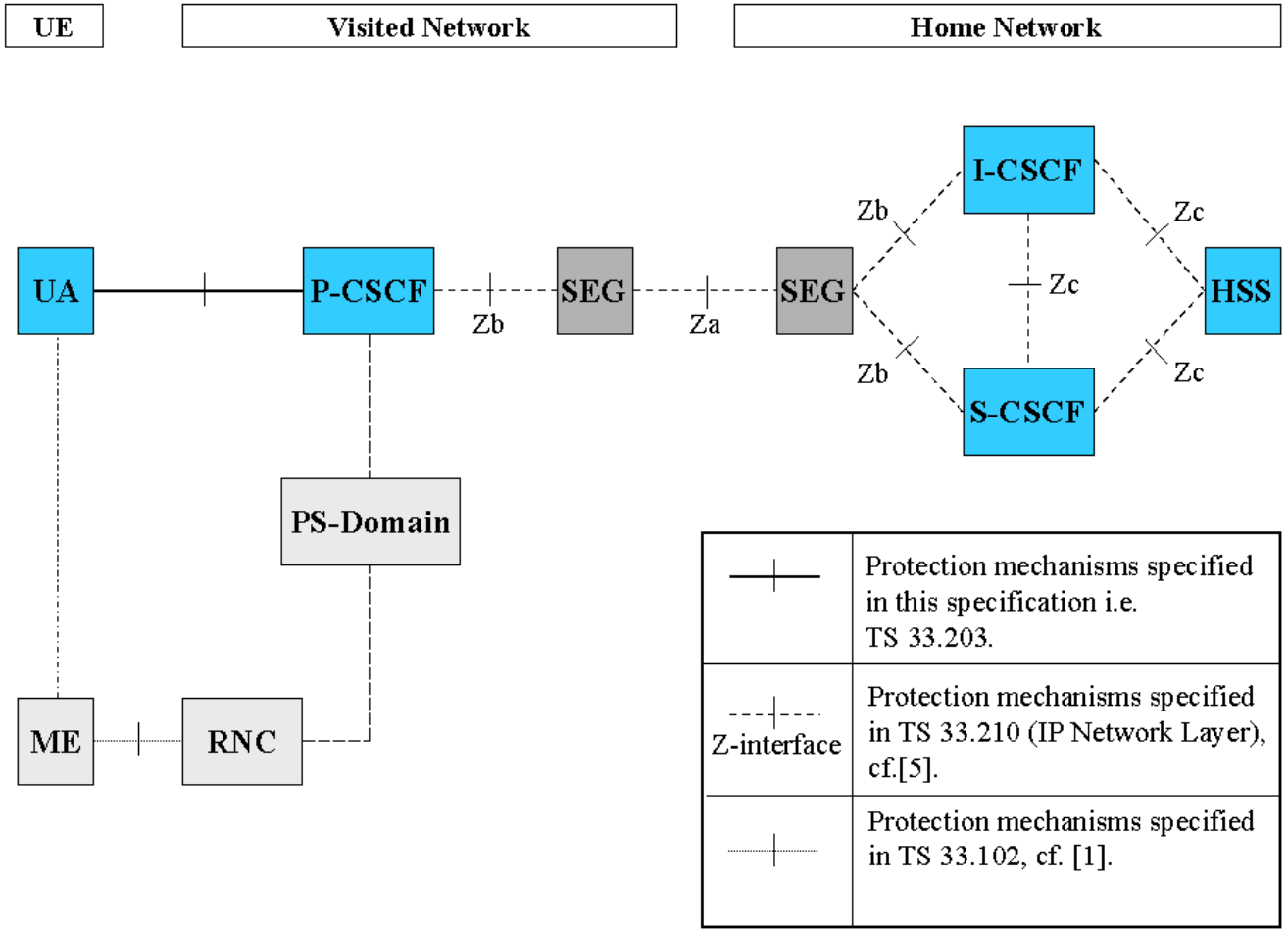
- Overview:
  - ❖ IMPI (IM Private Identity) is the identity which is authenticated
  - ❖ Signaling protection in a hop-by-hop fashion
  - ❖ Signaling protection dependent on Network Domain Security
  - ❖ Re-use of AKA defined in for UMTS here called IMS AKA
  - ❖ Authentication  takes place via SIP REGISTER messages
  - ❖ Authentication is performed by the S-CSCF in the HN

ERICSSON

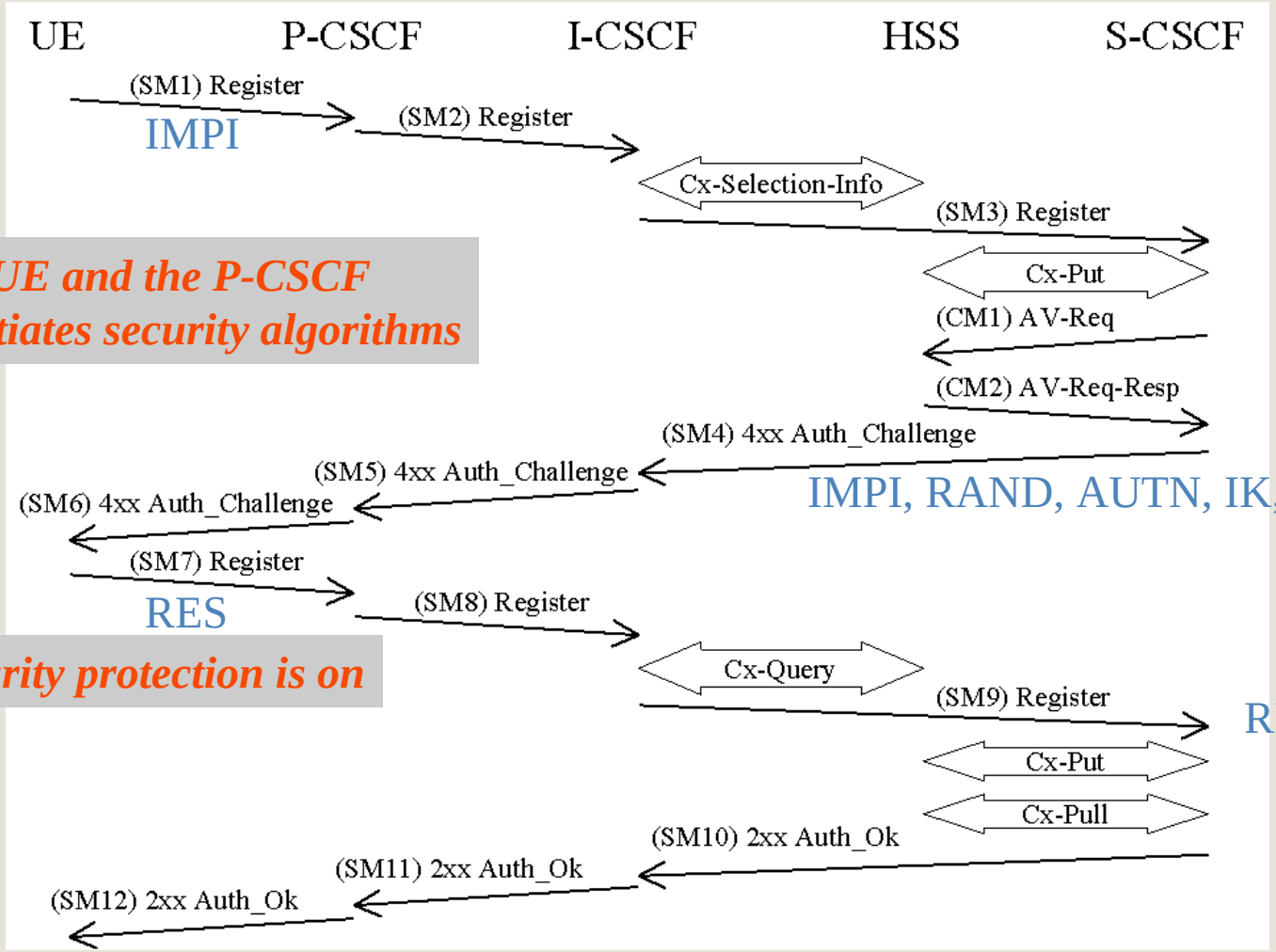
## Description of IMS security architecture

- Overview:
  - ❖ The HN is able to request a re-authentication of an IMS subscriber at any time
  - ❖ TS33.203 is dependent on IETF specifications. Work is in progress
  - ❖ It is still open if SIP-signaling will be protected by IPSec or SIP mechanisms at SIP level
  - ❖ The latest version of TS33.203v070 presented at SA3#21
  - ❖ TS33.203 will go to the SA-plenary in December as version 1.0.0 for information

# Description of IMS security architecture



# Description of IMS security architecture




***The UE and the P-CSCF negotiates security algorithms***

***Integrity protection is on***

ERICSSON

# The ISIM concept

Requirements that formed the ISIM concept:

- TS23.228v510
  - The IMPI (IM Private Identity)
    - ❖ The IMPI is securely stored on the USIM
    - ❖ The UE shall not be able to modify the IMPI
    - ❖ The IMPI is not dynamic and shall be permanently allocated to the IM subscriber
    - ❖ *The IMPI shall take the form of a NAI*
    - ❖ *It is possible to re-use the IMSI within the NAI*
    - ❖ The Home Domain Name of the subscriber shall be securely stored on the USIM
    - ❖ The UE shall not be able to modify the Home Domain Name

ERICSSON

# The ISIM concept

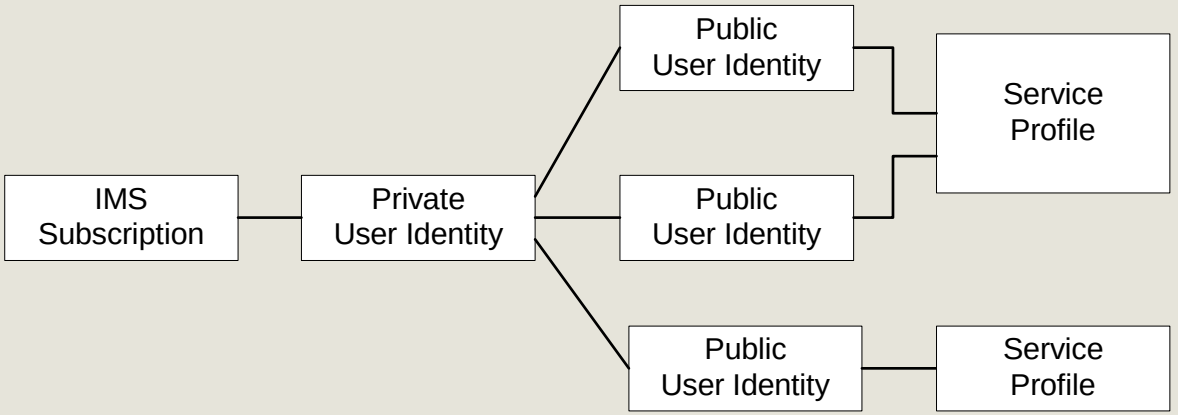
Requirements that formed the ISIM concept:

- TS23.228v510
  - The IMPU (IM Public Identity)
    - *The IMPU shall take the form of SIP URL or E.164 Number*
    - At least one IMPU shall be stored on the USIM
    - The UE shall not be able to modify the IMPUs stored on the USIM
    - *The IMPUs are not authenticated*
- TS22.228v510
  - Access independence
    - Access independence shall be supported
    - It is desirable that an operator should be able to offer services to their subscribers regardless of how they obtain an IP connection (e.g. GPRS, fixed lines, LAN).

# The ISIM concept

## Requirements that formed the ISIM concept

- The relationship between the IMPI and the IMPUs



ERICSSON

# The ISIM concept

## The ISIM as currently defined by SA3:

- The ISIM and the USIM are logically independent
  - The following cases are possible for implementation:
    - ISIM and USIM are implemented as a single application inside one UICC
    - ISIM and USIM are implemented as two distinct applications inside one UICC
    - ISIM and USIM are implemented inside two distinct UICCs
- The IMPI and IMPU(s) are stored in the ISIM
- More parameters shall be stored in the ISIM e.g. Authentication key K, Sequence numbers etc but this is open for the joint meeting with T3