Security in 3GPP

Bengt Sahlin
3GPP TSG SA WG3 Chairman

Ericsson Research NomadicLab

Outline

- 3GPP Security in General
- Recent specification work
- Ongoing specification work

3GPP TSG SA WG3 (Security)

- 3GPP TSG SA WG3 (SA3) has the overall responsibility for security in 3GPP
  - performing analysis of potential threats to the system
  - specifying the security architecture and protocols
  - setting security requirements and specifications

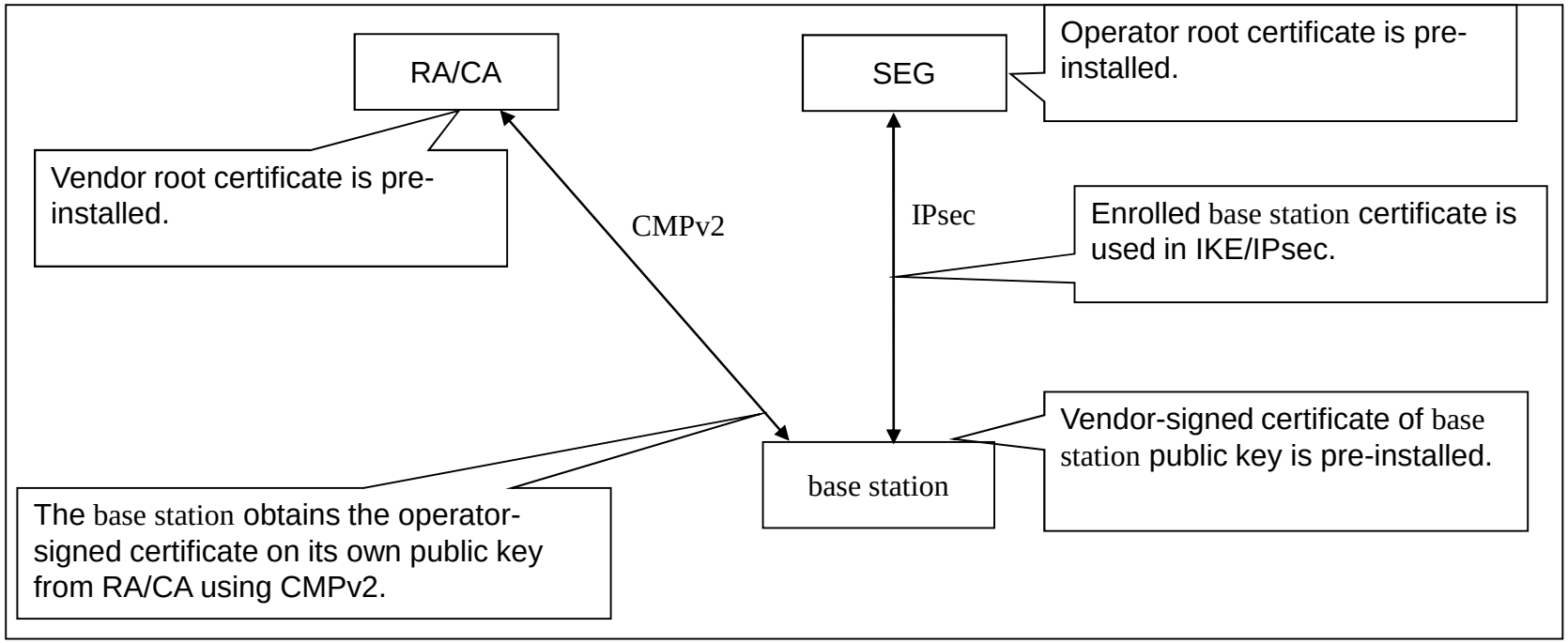
Security Features (I)

- Security for 3GPP Radio Access Networks
  - GERAN (GSM, GPRS, EDGE)
  - UTRAN (UMTS, HSPA)
  - E-UTRAN (LTE)
  - includes the needed security features for different types of base stations
    - eNBs, Home (e)NBs, relay nodes
- Security interworking of Wireless Local Area Network (WLAN) and other non-3GPP access technologies with 3GPP networks
- Security for the communication between the user equipment and the 3GPP network (core network)
  - authentication, integrity protection, confidentiality, etc.
- Network Domain Security
  - how to protect communications between network elements

Security Features (II)

- IMS Security
  - security for the IMS signalling
  - security for real-time media and messaging
  - work ongoing on specifying security for other use cases like conferencing
  - presence and list management
  - protection against unsolicited communication in IMS
    - A TR with recommendations produced in Rel-9 (3GPP TR 33.937)
    - work currently continuing
- Security of Multimedia Broadcast/Multicast Service (MBMS)
- Generic Bootstrapping Architecture
  - re-using the UICC-based authentication protocol for network access for securing access to network applications and services
- Technical Reports describing interworking with
  - Liberty Alliance features
  - OpenID features
- Key establishment features
  - between a UICC and a terminal
  - between a UICC hosting device and a remote device
- Security for system improvement for machine-type communications

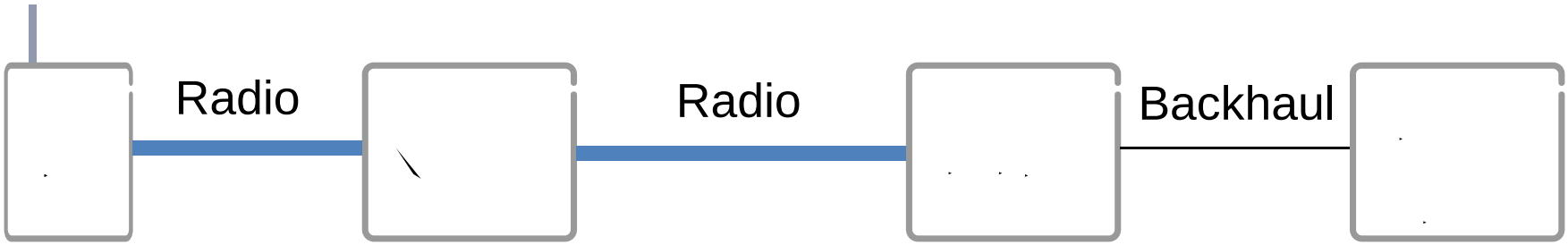
Certificate Enrollment for Base Stations



Picture from 3GPP TS 33.310

Relay Nodes

- A new base station type in E-UTRAN (LTE)
- Motivation
  - improve coverage of high data rates
  - improve cell edge throughput
- Challenge:
  - Relay node “invisible” to the UE
  - Relay Node looks like a UE to the network in some aspects
- Basic Architecture:



Relay Node Security

- Authentication
  - Mutual authentication between the relay node and the network
    - using AKA, credentials stored on a UICC
  - Relay node device authentication is mandatory
  - A binding between these two authentication procedures is needed
- The relay node is assumed to have a secure environment for storing and processing sensitive data
- It should be possible to perform a device integrity check
- Control plane traffic shall be integrity protected
- Optional integrity protection of user plane traffic
- The connection between the relay node and the network should be confidentiality protected
- Work ongoing, several solutions still under consideration

Security for System Improvement for Machine-type communications

- Work ongoing in 3GPP on system improvements for machine-type communications
- Analysis of security aspects ongoing in SA3
  - identification and analysis of threats
  - identification of potential security impacts of the system improvements
  - identification of potential new security features needed

EEA3 and EIA3 Work Item

- 3GPP has a work item on EEA3 and EIA3 algorithms for LTE
- Work was started during 2009
- The agreed work item is found in 3GPP document:
  - http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_44/Docs/SP-090445.zip
- The EEA3/EIA3 design is based on ZUC
- 3GPP is responsible for the changes needed in 3GPP specifications
- ETSI SAGE is providing the draft EEA3/EIA3 specifications and is handling the evaluation process
- The evaluation is a three-stage process
  1) evaluation by ETSI SAGE
  2) evaluation by selected teams of cryptanalysts
  3) public evaluation
- The public evaluation of EEA3/EIA3 is currently ongoing

Work Related to SSO Frameworks (I)

- Existing TRs
  - 3GPP TR 33.980 (Rel-7)
    - interworking of GBA and Liberty Alliance
  - 3GPP TR 33.924 (Rel-9)
    - interworking of GBA and OpenID

Work Related to SSO Frameworks (II)

- Study ongoing on SSO Application Security for IMS - based on SIP Digest (draft 3GPP TR 33.914)

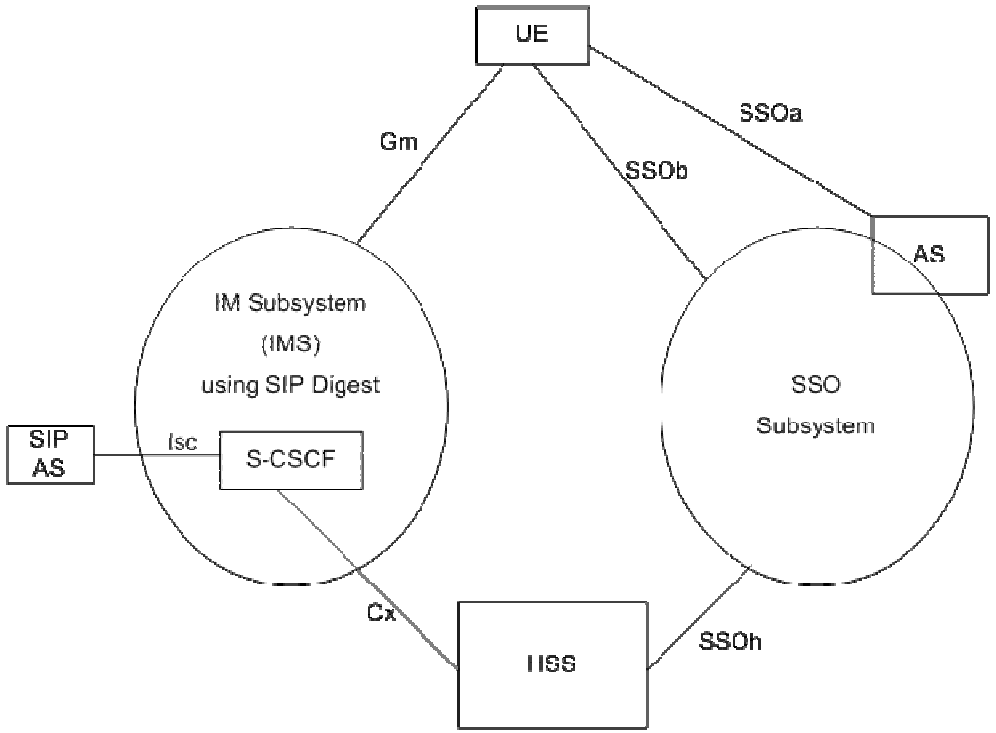


figure from draft 3GPP TR 33.914

Work Related to SSO Frameworks (III)

- New Work Item
  - Study on Security aspects of Integration of Single Sign-On (SSO) frameworks with 3GPP networks
  - Main Objective
    - investigate the security aspects of the use cases and service requirements currently being identified by SA1 in their study on the integration of SSO frameworks with 3GPP networks for various operator authentication configurations.

Questions?