3GPP SA3 - 5G SECURITY

Major changes in 5G security architecture and procedures | Sander de Kievit

THIS TALK

- Short introduction about me and some words on 3GPP SA3.
- Major changes since 4G, what do we really get?
  - Unified authentication framework for both 3GPP and non-3GPP access
    - Increased home control
  - Extended key hierarchy for later security services
    - E.g. steering of roaming under discussion and protection of UE to home traffic
  - Improved subscriber identity confidentiality
    - Encryption at initial registration
  - Security of the interconnect network between operators
    - Work in progress…

ABOUT ME

- Sander de Kievit
- Security researcher at TNO
- Representing KPN in 3GPP SA3

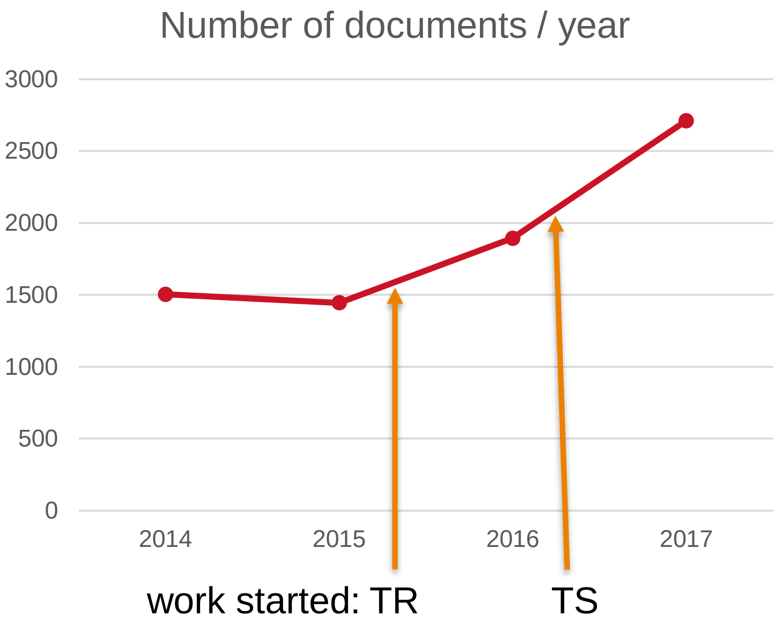
- My interests include:
  - Security as enabler of 5G Mobile Networks
  - Security consultancy and assessments for IT systems.
  - In the past: Monitoring and Detection of Advanced Persistent Threats

3GPP SA3 SECURITY WORKING GROUP

- SA3 is the working group tasked with security and privacy within the scope of 3GPP.

- Study started at #83 with TR 33.899
  - Overall topics identified
  - Priorities set

- Specification work started at #86-BIS
  - New spec: TS 33.501
  - First approved version (15.0.0) available soon



MAJOR CHANGES IN 5G – AUTHENTICATION

- **Design Goals:**
  - Unified authentication framework for both 3GPP and non-3GPP access
  - Improved control by home network

- **Design Questions:**
  - How to deal with potentially different transport of NAS and EAP?
  - How to add home control to EPS AKA?
  - Authentication algorithm under control of 3GPP SA3?

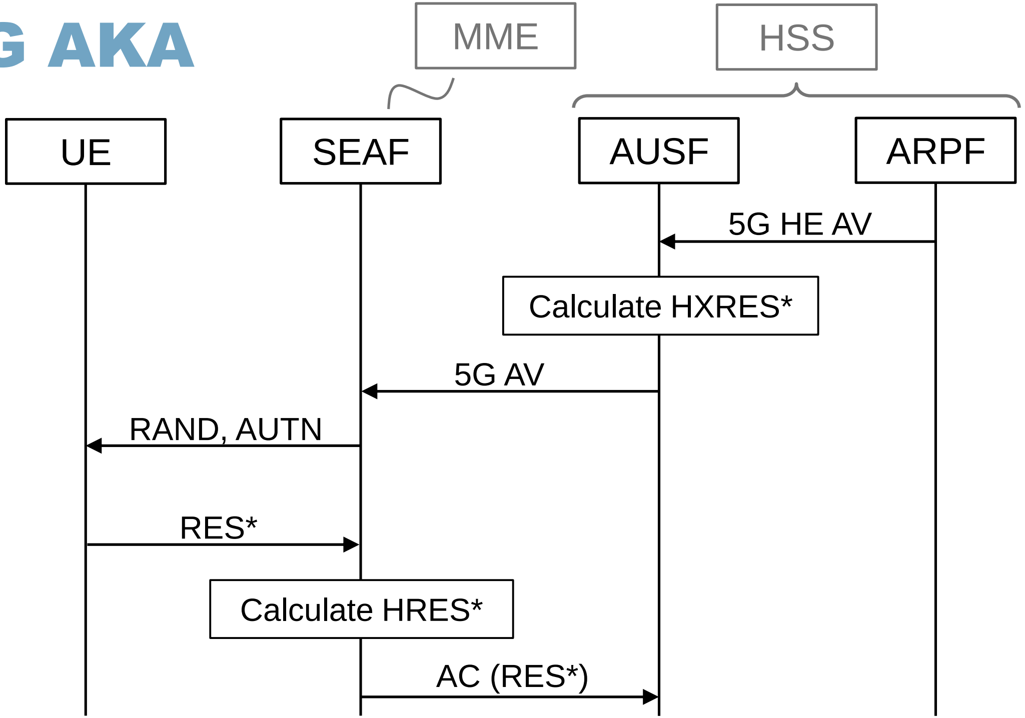
- **Final design decisions:**
  - Both EAP AKA’ and newly developed 5G AKA supported
  - Continued compatibility with Rel-8 USIM

MAJOR CHANGES IN 5G – AUTHENTICATION HOME CONTROL IN 5G AKA

- Based on EPS AKA
  - New authentication confirmation
  - New RES* and H(X)RES*

- Calculation of RES*:
  - KDF(CK, IK, SN name, RAND, RES)
  - Calculated in ARPF and UE

- Calculation of HRES*:
  - HASH(RAND, RES*)
  - Calculated in SEAF and AUSF
  - Used for authentication by the SEAF



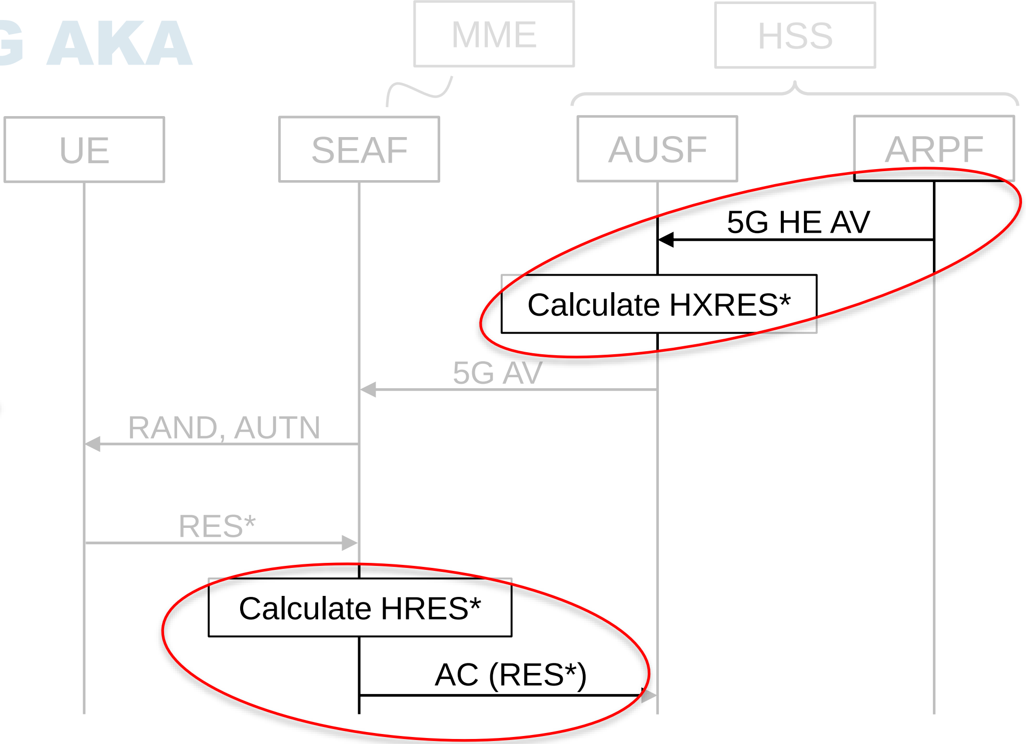
MAJOR CHANGES IN 5G – AUTHENTICATION

HOME CONTROL IN 5G AKA

- Based on EPS AKA
  - New authentication confirmation
  - New RES* and H(X)RES*

- Calculation of RES*:
  - KDF(CK, IK, SN name, RAND, RES)
  - Calculated in ARPF and UE

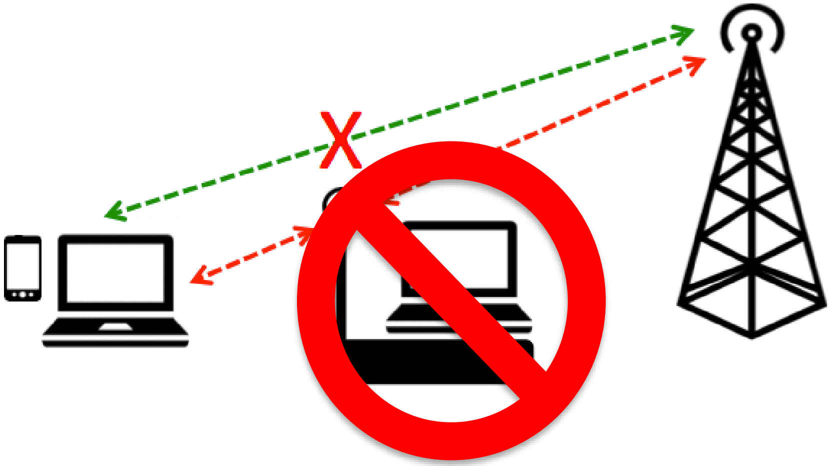
- Calculation of HRES*:
  - HASH(RAND, RES*)
  - Calculated in SEAF and AUSF
  - Used for authentication by the SEAF



MAJOR CHANGES IN 5G – SUBSCRIBER PRIVACY

- **Design Goal:**
  - Defeating the IMSI catcher

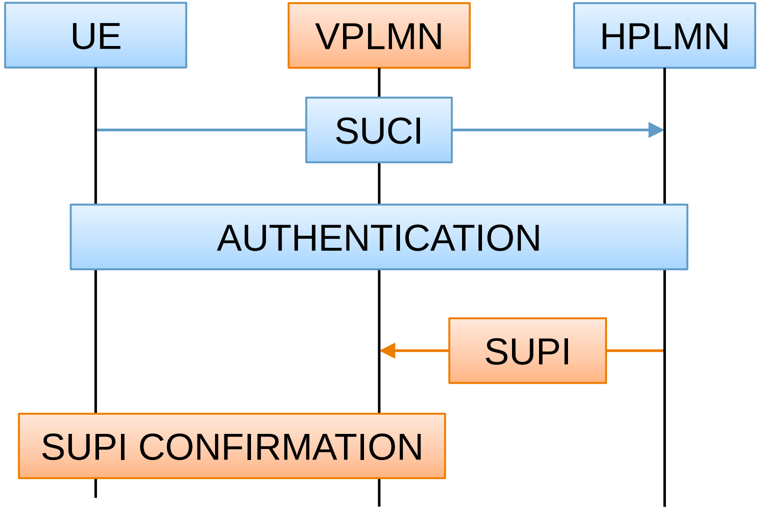
- **Design Challenges:**
  - Scalable solution under control of operator
  - Comply with regulations



MAJOR CHANGES IN 5G – SUBSCRIBER PRIVACY

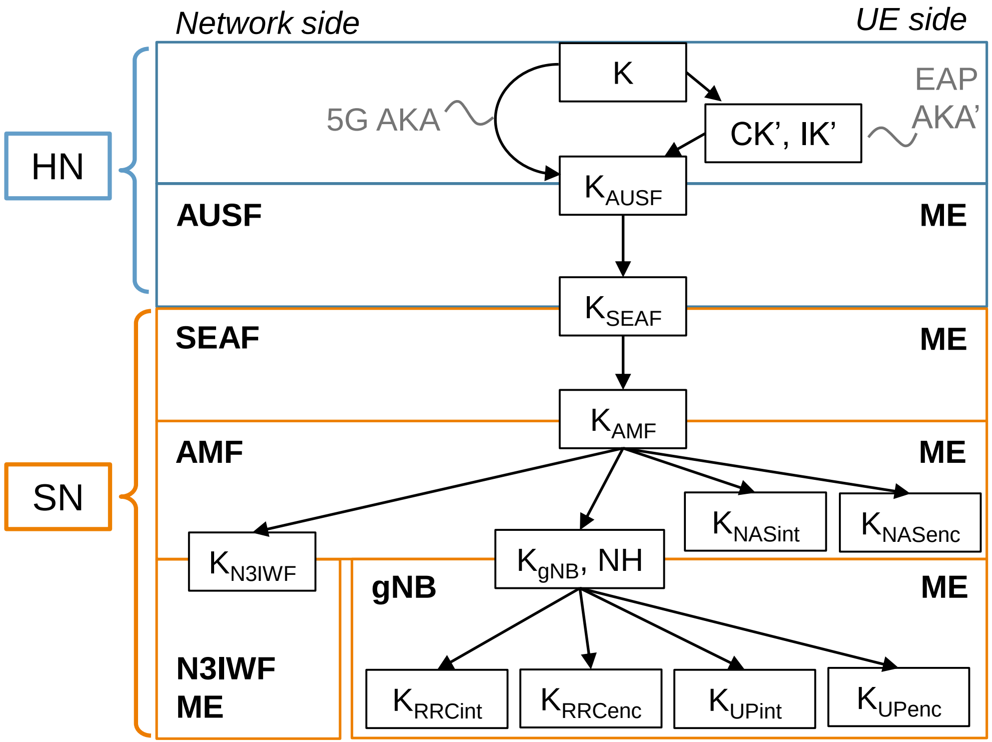
- **Solution:**
  - SUPI encrypted with home network public key on initial attach (SUCI)
  - Complete authentication
  - Then, send SUPI from HPLMN to VPLMN
  - Finally, confirm SUPI by binding into a key

- **Further details:**
  - Encryption can done on UE or USIM
  - Two algorithms standardized on UE side
  - Algorithms on the USIM can be controlled by operators



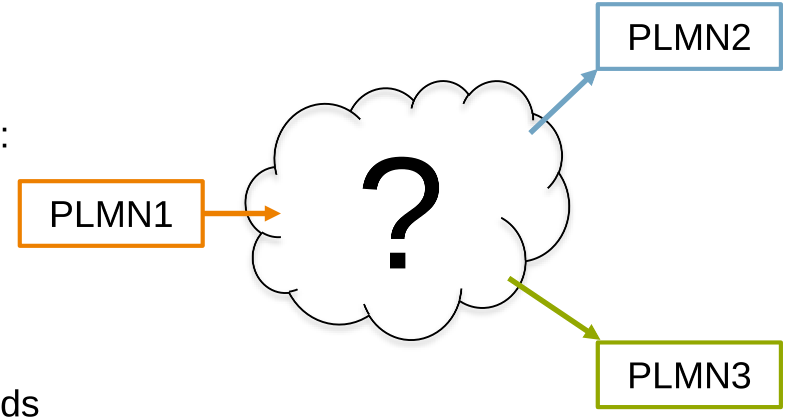
MAJOR CHANGES IN 5G – KEY HIERARCHY

- Key hierarchy extended to also include:
  - K_{AUSF} at home network
  - K_{SEAF} at visited network
- Reasons for K_{AUSF}
  - Quick reauthentication
  - Protecting home to UE traffic, e.g. steering of roaming under discussion
- Reasons for K_{SEAF}:
  - Separate security anchor from mobility anchor
  - Pre-empts AMF at insecure locations



MAJOR CHANGES IN 5G – INTERCONNECT SEC.

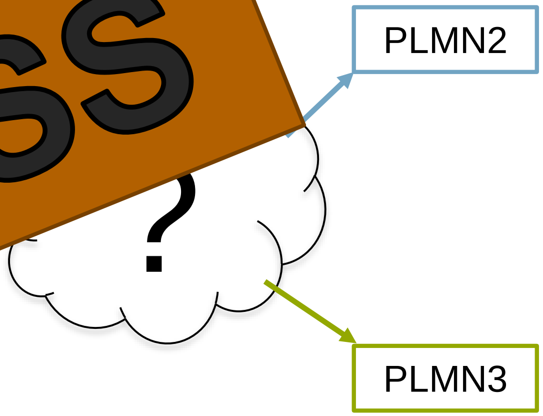
- **Design Goal:**
  - Protecting messages exchanged between operators via the IPX network
- **Design Challenge:**
  - Deal with the complex services of IPX providers:
    - Rerouting of messages
    - Mediation of messages
    - Roaming hubs
  - Providing PLMN to PLMN security
  - Being compliant with JSON and HTTP2 standards



MAJOR CHANGES IN 5G – INTER ECT SEC.

WORK IN PROGRESS

- **Design Goal:**
  - Protecting messages exc
- **Design Chal**
  - D
    -
  - Provi
  - Being 2 standards



THANK YOU FOR YOUR ATTENTION

Take a look:
TIME.TNO.NL