3GPP SA3 6G Study Conference Call

Qualcomm Incorporated

Agenda

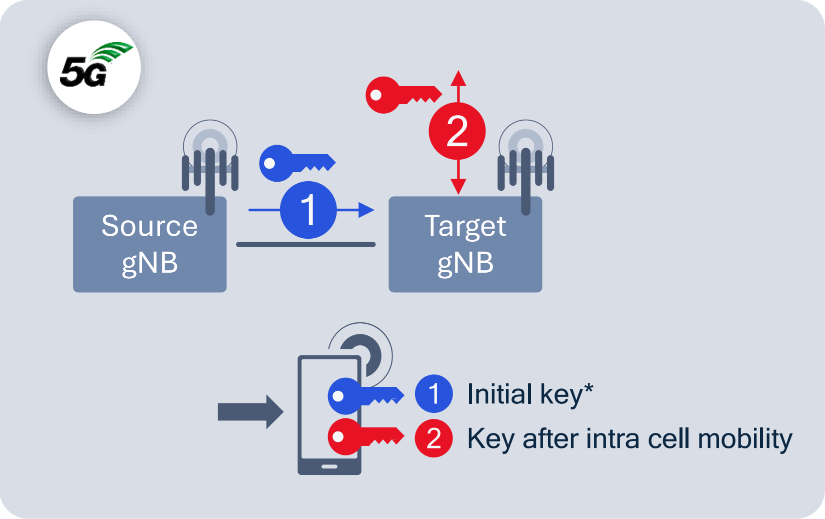
- Security for RAN Mobility
- Enhanced AS key handling
- Robust security setup
- Isolation of UE security contexts
- Security evaluation and dynamic policy

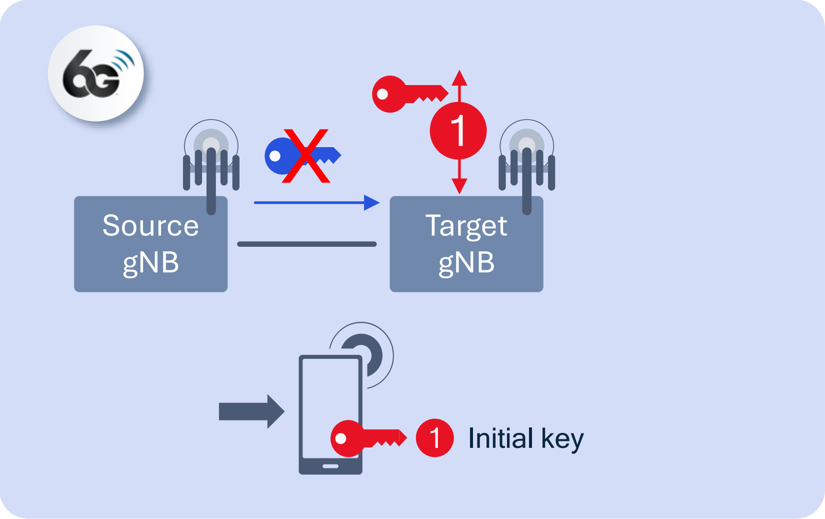
Security for RAN Mobility

Key hierarchy for enhanced security in mobility

- 5G Key change during mobility
  - RRC signaling for key change is always required
  - Source gNB knows the key at the target gNB for Xn-based mobility
  - Intra-cell HO is required to support forward security
- Limitations
  - Key separation between gNBs is not immediate for Xn-based mobility
  - K_{gNB} cannot be prepared at multiple gNBs to support flexible mobility, e.g., subsequent LTM
  - Deployment is inflexible due to potential impacts of RAN procedures on AMF or vice versa
- Potential 6G enhancements
  - Support *immediate* forward/backward security by design with vertical key derivation for 6gNB change (or 6G-CU change)
  - Support multiple *concurrent* key preparation at different RAN nodes

→ Horizontal key derivation
→ Vertical key derivation



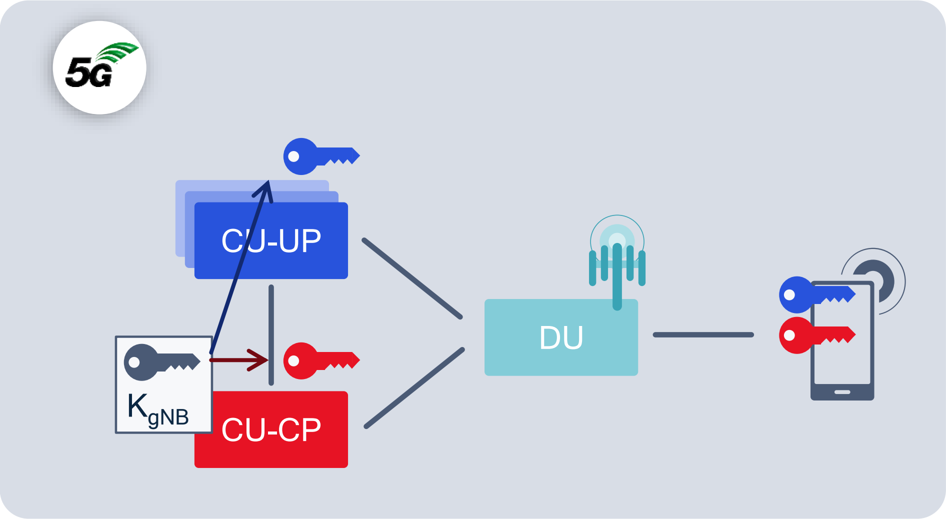


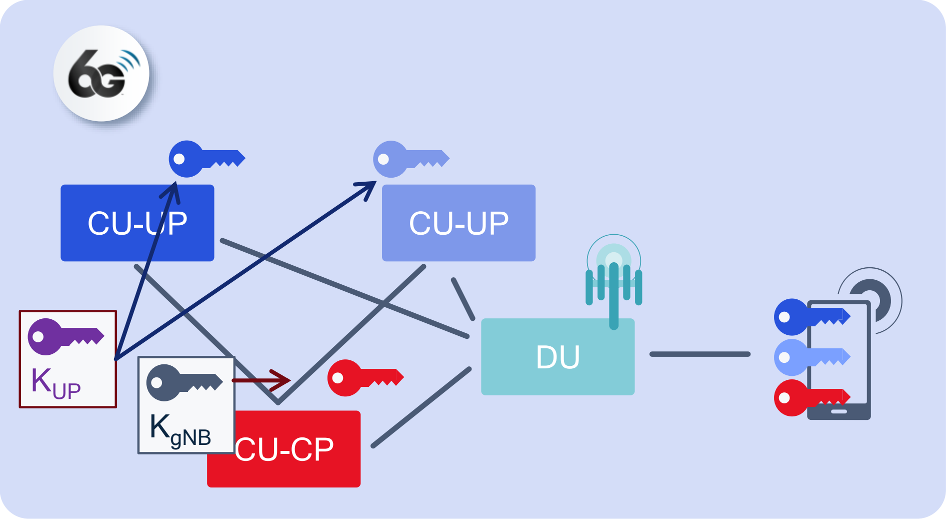
*Initial key refers to the key used at the target gNB after inter-gNB mobility

Enhanced AS key handling

User-plane security anchor to support of different UP termination points per application/service needs

- 5G User plane security
  - A UE may be connected to multiple CU-UPs (1 per PDU session)
  - KgNB change also requires UP key change
- Limitations
  - No key separation when multiple CU-UPs are configured for a UE
  - No key separation for different PDU sessions/slices
  - Frequent UP key changes required for highly mobile UEs
  - UP security processing overhead while CU-UP may stay same in gNB change, e.g., CU-UP shared by multiple gNB-CUs
- Potential User plane security enhancements
  - Support of different UP termination points per application/service needs, e.g., location(s) of CU-UP is determined by network using UE mobility pattern, UE capability, service security requirements
  - Service specific configuration which enables security isolation of services as desired
  - UP key separation from KgNB

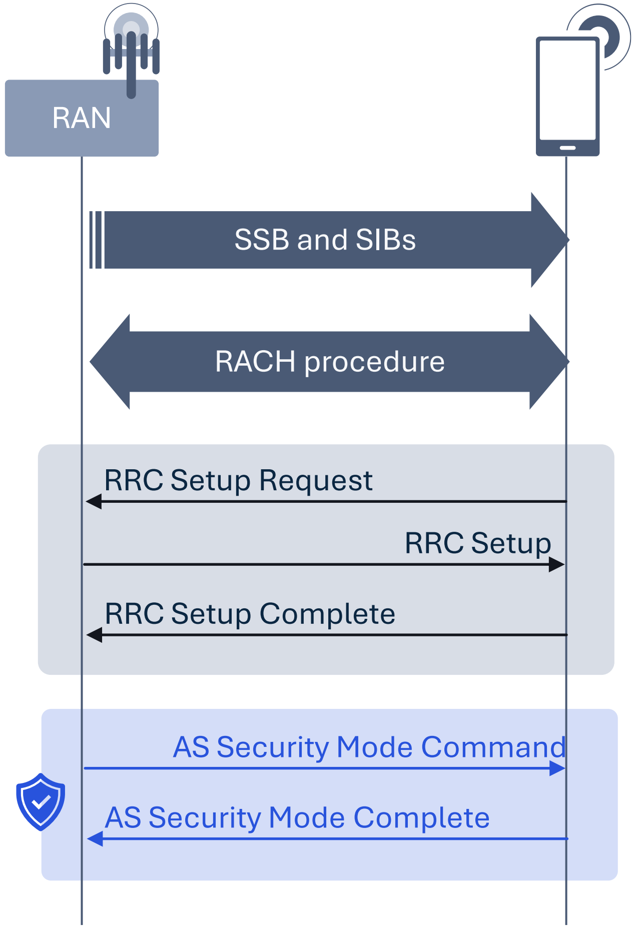




Robust security setup

Ensure integrity of the messages exchanged before the Security Mode Command activates AS security

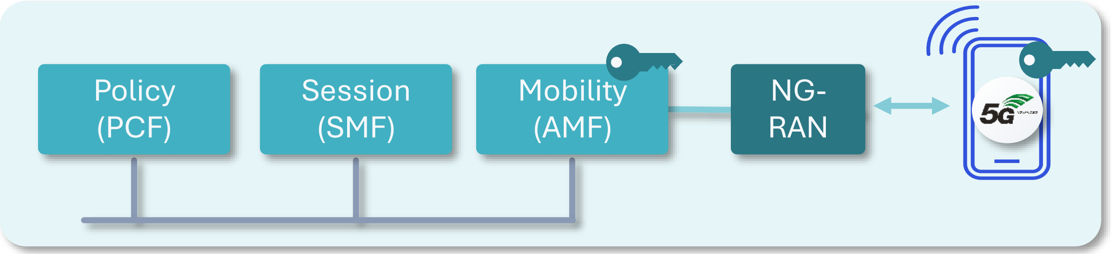
- 5G AS security setup
  - Messages exchanged prior to the Security Mode Command are sent unprotected, e.g., RACH, RRC setup messages,
- Potential threats
  - Manipulation of messages before the SMC can lead to UE being misconfigured
- Potential 6G AS SMC enhancements
  - ***Verification*** of messages exchanged prior to AS Security Mode Command procedure
    - This is similar to initial NAS protection
  - Upon detecting an error/mismatch, 6G-NB either provisions correct parameters or releases connection

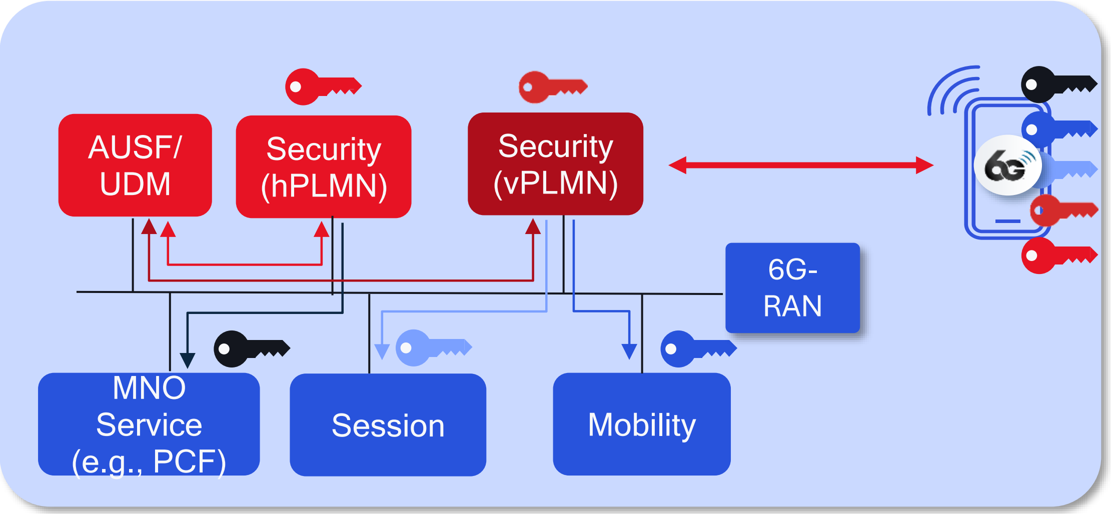


Isolation of UE security contexts

Independent security contexts at each network functions/services

- 5G NAS security
  - NAS messages are securely exchanged between UE and AMF
  - Single security termination point at AMF
  - Initial AMF is the trust anchor for 5G security until the next authentication
- Limitations
  - No generic secure communication channel between HPLMN and UE (e.g., HPLMN relies on VPLMN to deliver UE policies)
  - No forward security in AMF relocation, i.e., source AMF knows the NAS key at the target AMF and henceforth
    - 5G SEAF is collocated with AMF and only used for initial AMF key derivation
  - Secure access to **new** control plane services may require changes to the existing network function (e.g., AMF)
- Potential 6G NAS security enhancements
  - Independent 6G SEcurity Anchor Function (SEAF)
  - Separate security anchors at HPLMN and VPLMN
  - Independent and secure access to control plane services, e.g., for easier service deployment

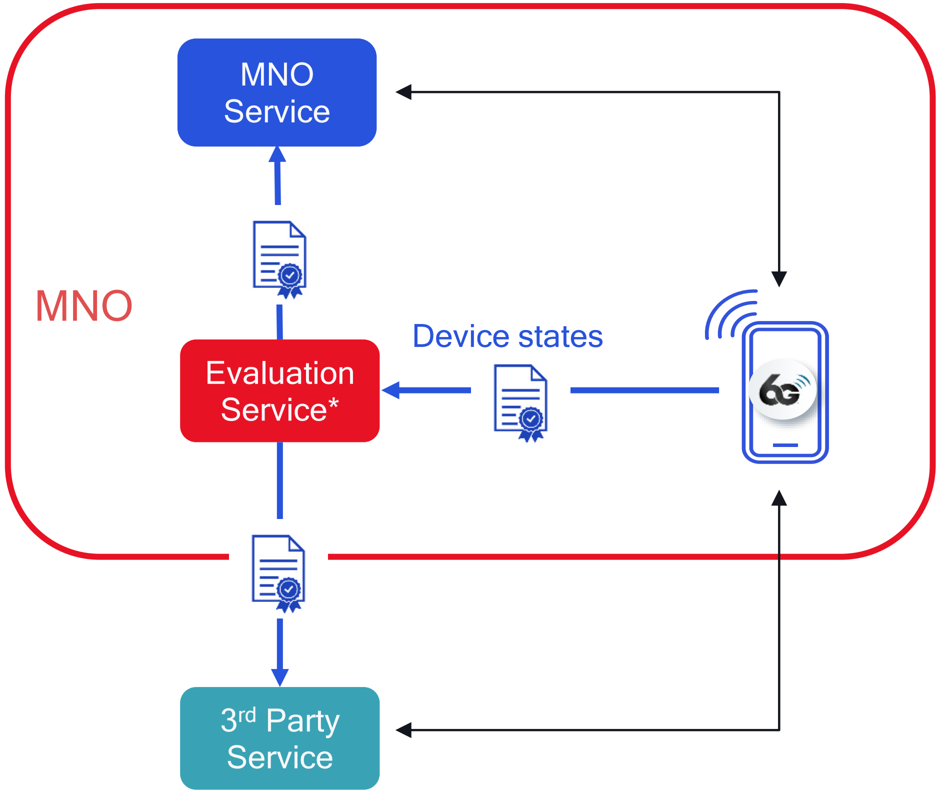




Security evaluation and dynamic policy

Help evaluate and strengthen overall security of the cellular system

- 5G security
  - Authentication and authorization only based on the subscription credentials
  - Secure connection and/or service access only based on primary authentication and subscription (authorization) information
- Potential threats
  - Compromised or unpatched devices/NFs (including UE) may waste operator's network resource
- Potential 6G security enhancements
  - Support collection of 6G device (security) state information periodically or on-demand
  - Define/collect 6G device (security) appraisal policy for service access
    - Appraisal policy defined for each service, e.g., HW model, HW version, SW version, …
  - Make 6G device (security) evaluation results available to NF service producer/consumer to help enforce respective security policy
  - Additional use cases include device authentication, data provenance,…



*Evaluation Service may obtain device state information from 3rd parties

Thank you

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

Qualcomm and Snapdragon are trademarks or registered trademarks of Qualcomm Incorporated.
Other products and brand names may be trademarks or registered trademarks of their respective owners.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.

Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.
Qualcomm patented technologies are licensed by Qualcomm Incorporated.

Follow us on:

For more information, visit us at qualcomm.com & qualcomm.com/blog