5G Authentication

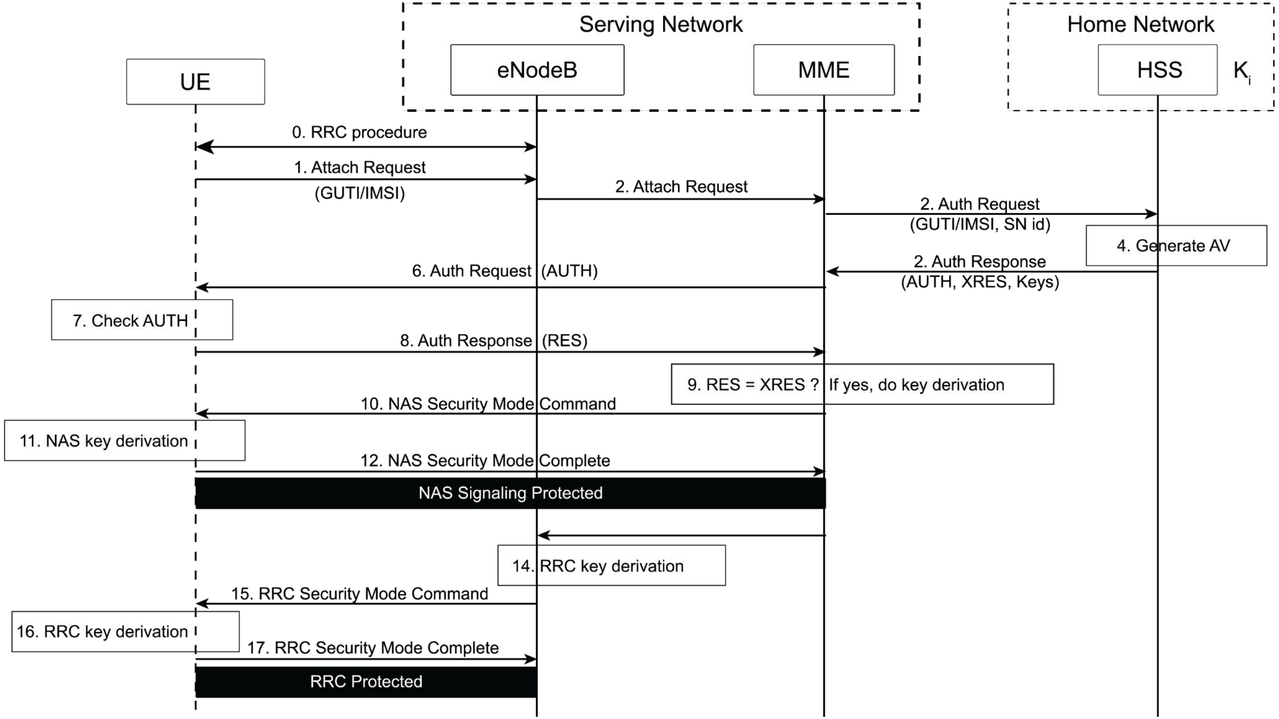
NETWORK SECURITY (2021-2022)

Abbreviations

- AKA = Authentication and Key Agreement
- UE = User Equipment
- eNodeB = Evolved NodeB
- MME = Mobility Management Entities
- HSS = Home Subscriber Server
- RRC = Radio Resource Control
- IMSI = International Mobile Subscriber Identity
- GUTI = Globally Unique Temporary Identity
- AV = Authentication Vector
- SEAF = Security Anchor Function
- AUSF = Authentication Server Function
- UDM = Unified Data Management
- ARPF = Authentication Credential Repository and Processing Function
- SIDF = Subscription Identifier De-concealing Function
- SUPI = Subscription Permanent Identifier
- SUCI = Subscription Concealed Identifier

4G Authentication -Recap-

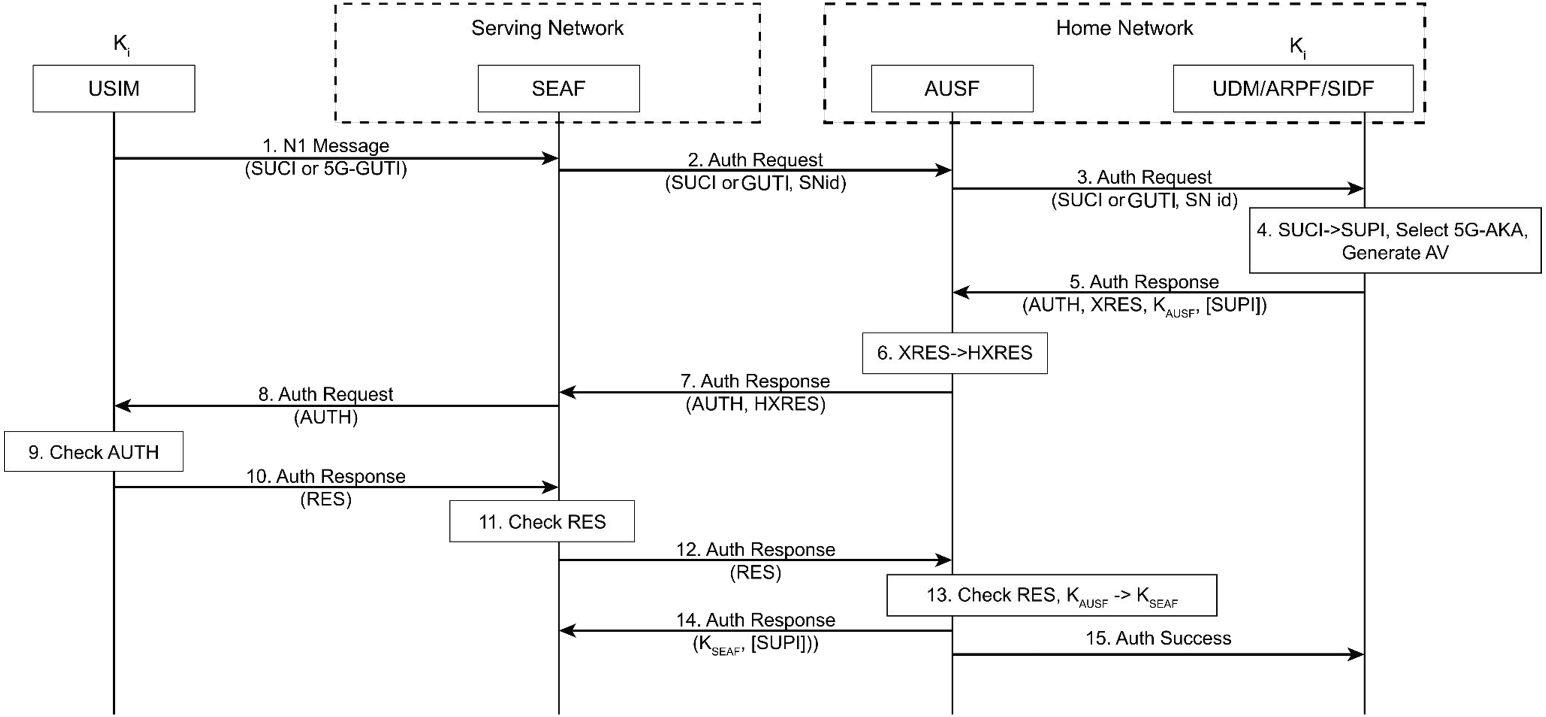
4G EPS-AKA



[Source: https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication]

5G Authentication

5G-AKA



Serving Network

Home Network

K_i

USIM

SEAF

AUSF

K_i

UDM/ARPF/SIDF

1. N1 Message (SUCI or 5G-GUTI)

2. Auth Request (SUCI or GUTI, SNid)

3. Auth Request (SUCI or GUTI, SN id)

4. SUCI->SUPI, Select 5G-AKA, Generate AV

5. Auth Response (AUTH, XRES, K_{AUSF}, [SUPI])

6. XRES->HXRES

7. Auth Response (AUTH, HXRES)

8. Auth Request (AUTH)

9. Check AUTH

10. Auth Response (RES)

11. Check RES

12. Auth Response (RES)

13. Check RES, K_{AUSF} -> K_{SEAF}

14. Auth Response (K_{SEAF}, [SUPI]))

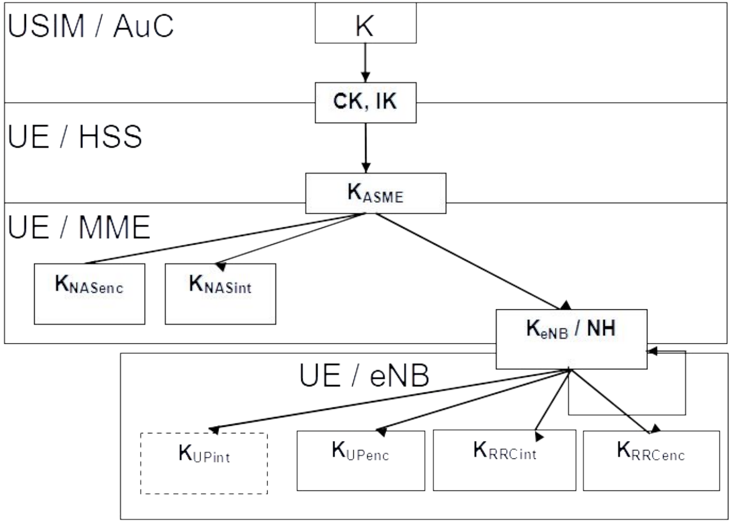
15. Auth Success

[Source: https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication]

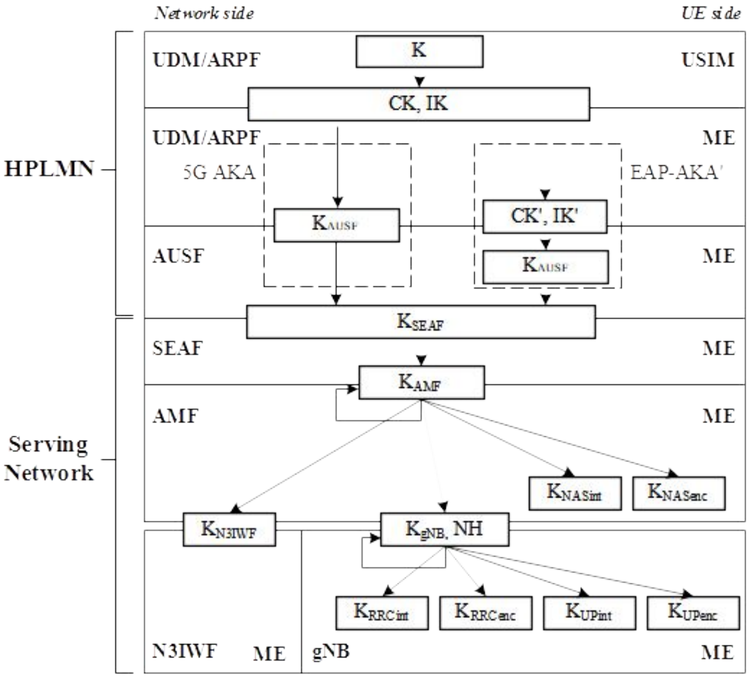
5G-AKA vs. 4G EPS-AKA

- ➔ Different entities involved in the authentication process
- ➔ The permanent identity of the UE is always encrypted in 5G
- ➔ The home network makes the final decision on UE authentication in 5G
- ➔ Key hierarchy is longer in 5G than in 4G: two intermediate keys, K_{AUSF} and K_{AMF}

Key Hierarchy in 4G vs. 5G



[Source: 3GPP TS 33.401 V17.0.0 (2021-12)]



[Source: 3GPP TS 33.501 V17.4.0 (2021-12)]

Resources

- 3GPP TS 33.501 V17.4.0 (2021-12): https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h40.zip

- 3GPP TS 33.401 V17.0.0 (2021-12): https://www.3gpp.org/ftp/Specs/archive/33_series/33.401/33401-h00.zip

- A Comparative Introduction to 4G and 5G Authentication - CableLabs