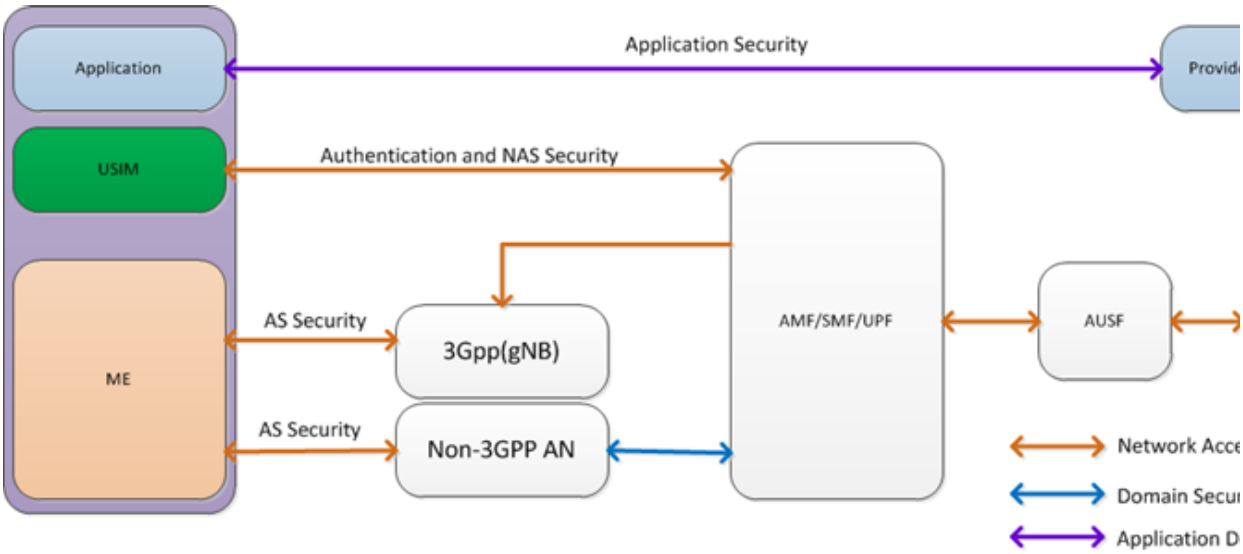
5G Security (5G AKA Authentication)

Jan 20, 2020 (http://5gblogs.com/2020/01/)

5G Security (5G AKA Authentication)

By **prasanna (http://5gblogs.com/author/prasanna/)** in **(http://5gblogs.com/5g-security-5g-aka-authe**
5GSecurity (http://5gblogs.com/category/5gsecurity/)

5G Security Procedure between UE and Network



Security Types in 5G Network

1. Security required for UE to access network services comes under Network access security. This sec mainly cover Authentication, Integrity and ciphering of Signalling and data.
2. Domain Security mainly covers secure communication between different Network nodes.
3. Application domain security covers security mechanism between peer applications.
4. There are two different kind of authentication

Different Authentication, Ciphering and Integri Algorithms

- In most cases for Authentication Key Agreement(AKA), operators use Milenage/TUAK algorithm. Bu cases proprietary algorithm.
- For Cyphering and Integrity Protection following Algorithms are used.

Ciphering Algorithms

value	Identifier	name
0000	NEA0	Null
0001	128-NEA1	Snow 3G
0010	128-NEA2	AES
0011	128-NEA3	ZUC

Integrity Algorithms

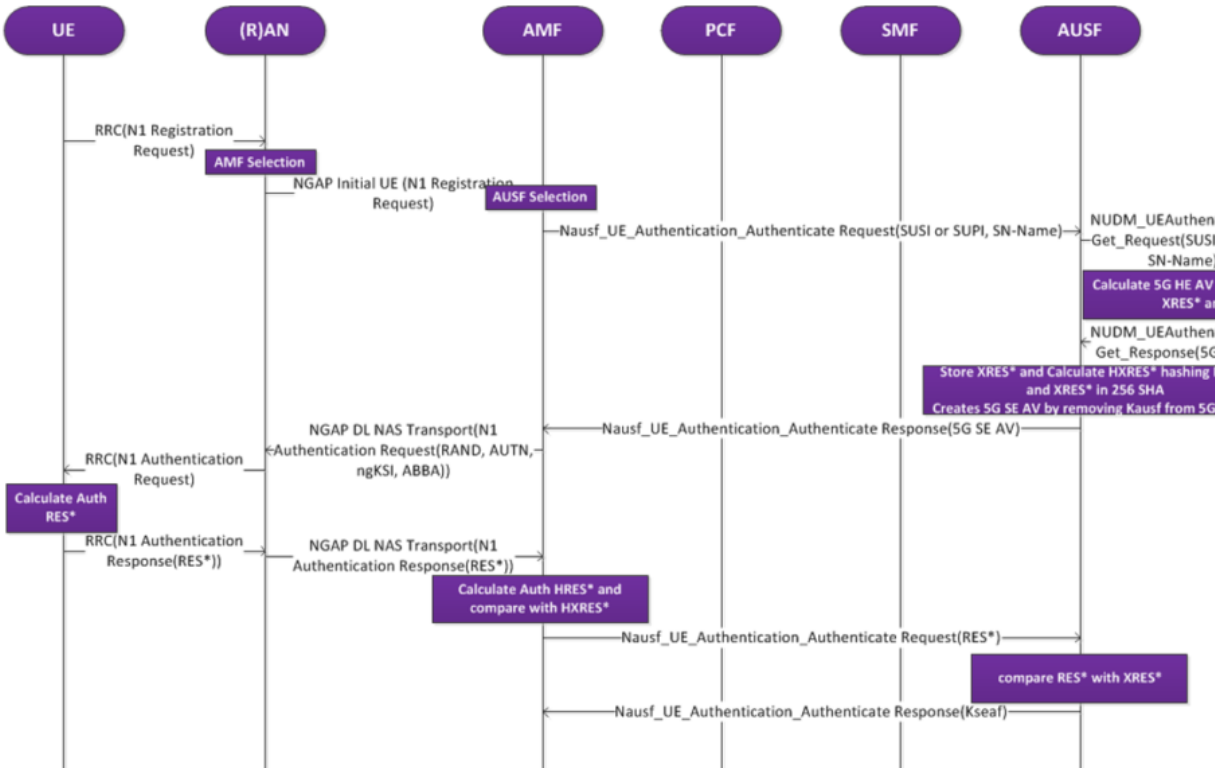
value	Identifier	name
0000	NEA0	Null
0001	128-NIA1	Snow 3G
0010	128-NIA2	AES
0011	128-NIA3	ZUC

Key Distribution

	UE	gNB	AMF	AUSF	UDM
Pre-Shared Keys	K				K
	OP				OP
Generated parameters	SQN				SQN, R
Derived keys for 5G AV for authentication	IK				IK
	CK				CK
	RES				XRES

	MAC				XMAC
	RES*				AUTN
				Kseaf	Kausf
				HXRES*	XRES*
			HRES*		

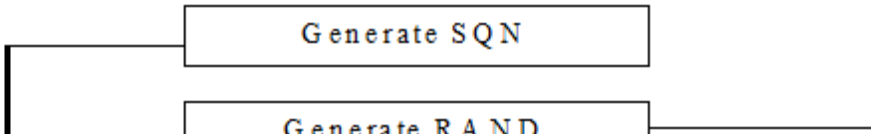
5G AKA Authentication Procedure

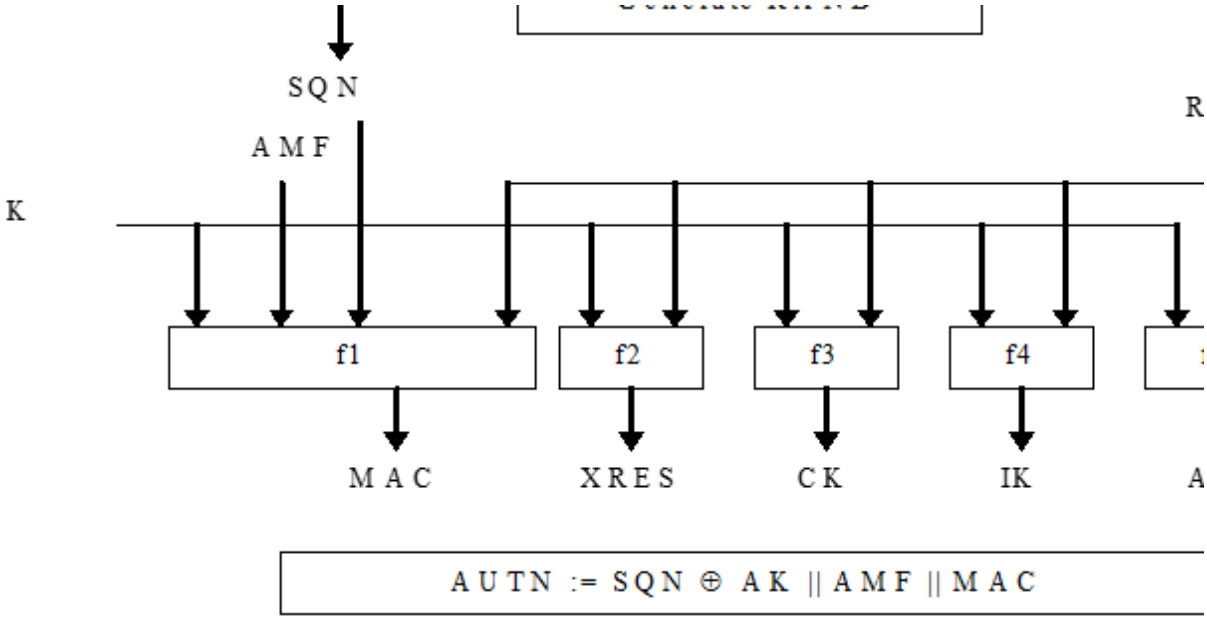


(http://5gblogs.com/wp-content/uploads/2020/01/image-11.png)

Authentication Flow Steps

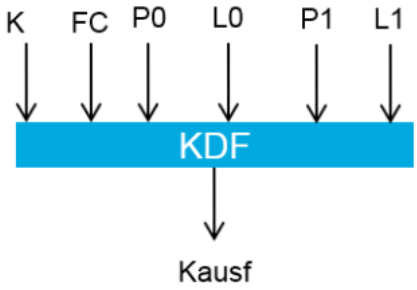
1. After receiving Registration Request, AMF initiates authentication procedure with UE, if UE security not existing with AMF.
2. AMF sends Nausf_UEAuthentications Request with SUCI or SUPI and Serving network name.
3. AUSF based on the Serving Network name, determine if AMF is authorised to send this message.
4. Then AUSF, sends Nudm_UEAuthentication_Get Request with SUPI/SUCI to UDM.
5. UDM Calculates the 5G HE AV as below. UDM Uses Milenage functions to derive MAC, XRES, CK, IK





(http://5gblogs.com/wp-content/uploads/2020/01/image-13.png)

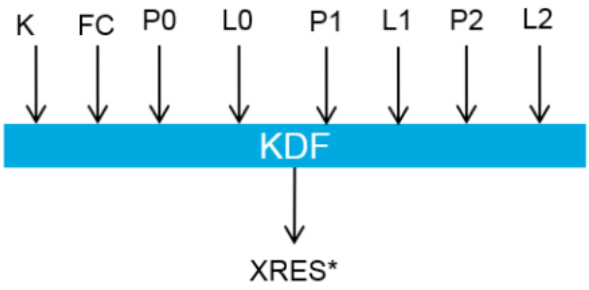
- UDM derives Kausf is as follows using HMAC-SHA-256(K, S) KDF(Key Derivation Function) function a



K = CK || IK
FC = 0x6A
P0 = SN Name
L0 = Length of SN Nam
P1 = SQN XOR AK
L1 = Length of SQN XO

(http://5gblogs.com/wp-content/uploads/2020/01/image-14-1024x271.png)

- UDM derives XRES* as follows using HMAC-SHA-256(K, S) KDF function.



K = CK || IK
FC = 0x6B
P0 = SN Name
L0 = Length of SN
P1 = RAND
L1 = Length of RAN
P2 = XRES
L2 = Length of XRE

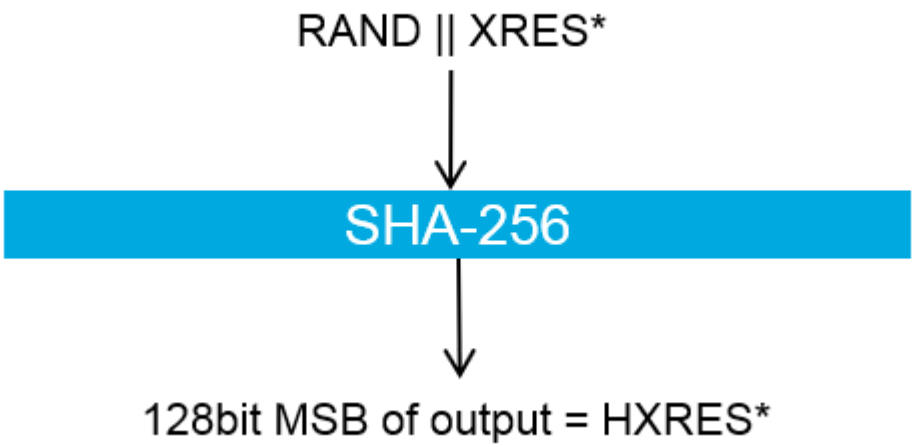
(http://5gblogs.com/wp-content/uploads/2020/01/image-15.png)

- UDM derives 5G HE AV from above derived keys as below and send it to AUSF with message

"Nudm_Authentication get Response" **5G HE AV = RAND || XRES* || Kausf || AUTN**

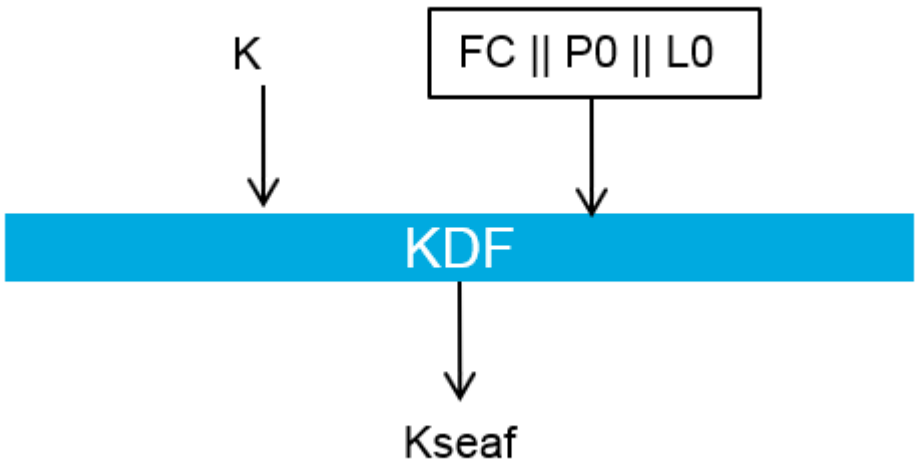
6. Derivation of 5G SE AV at AUSF

- HXRES* Calculation at AUSF: HXRES* is 128 bit MSB of the output of SHA-256 hash, calculated by p RAND || XRES* as input to SHA-256 algorithm.



(http://5gblogs.com/wp-content/uploads/2020/01/image-16.png)

- AUSF derives Kseaf from Kausf by passing K= Kausf and S = 0x6C || Serving Network Name || Ler Serving Network Name to KDF function.

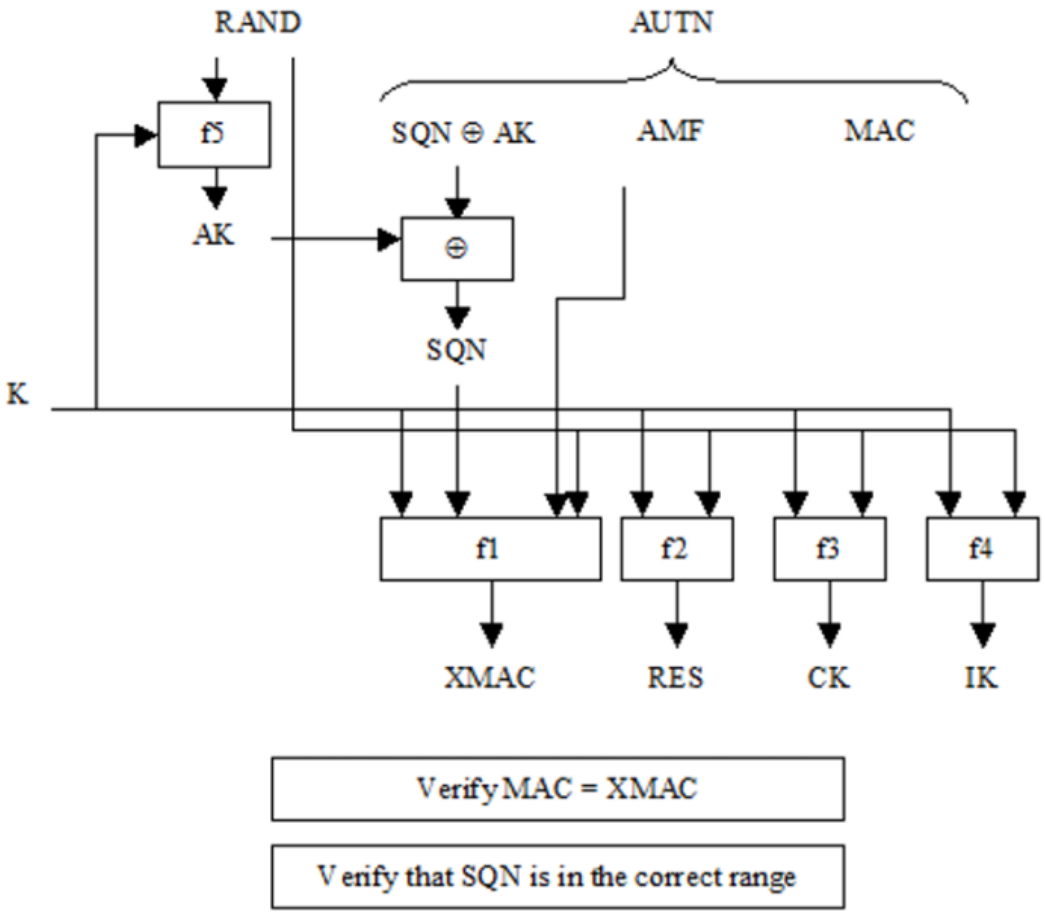


(http://5gblogs.com/wp-content/uploads/2020/01/image-17.png)

- AUSF calculates 5G AV and 5G SE AV as below and send 5G SE AV to AMF. **5G AV = RAND || HXRES AUTN 5G SE AV = RAND || HXRES* || AUTN**

7. AMF Sends NAS Authentication Request to UE with RAND and AUTN from 5G SE AV.

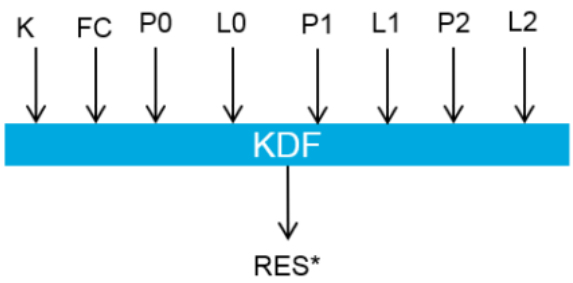
8. UE Uses Milenage functions to derive XMAC, RES, CK, IK as below.



(http://5gblogs.com/wp-content/uploads/2020/01/image-18.png)

9. UE Verify the MAC received in AUTN with XMAC calculated above to authenticate the network and freshness of AUTN. Here if the comparison fails then it will send authentication failure with AUTS.

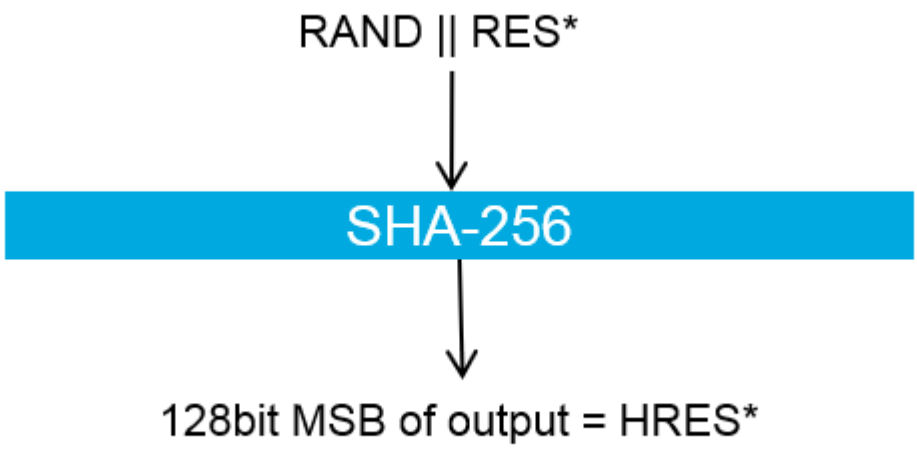
10. UE derives RES* as follows using HMAC-SHA-256(K, S) KDF function. using keys calculated above, a sends RES* to AMF.



K = CK || IK
FC = 0x6B
P0 = SN Name
L0 = Length of SN
P1 = RAND
L1 = Length of RAN
P2 = RES
L2 = Length of RES

(http://5gblogs.com/wp-content/uploads/2020/01/image-19.png)

11. AMF Calculates HRES* from RES* : HRES* is 128 bit MSB of the output of SHA-256 hash, calculated RAND || RES* as input to SHA-256 algorithm.



(http://5gblogs.com/wp-content/uploads/2020/01/image-20.png)

12. AMF compares HRES*(Calculated above) with HXRES* received from AUSF to check for successful authentication.

13. AMF sends RES* received from UE to AUSF with “Authenticate Request” message.

14. AUSF compares RES* with the XRES*(part of 5G HE AV) received from UDM in step 5.

15. If Comparison is successful, AUSF sends Authentication Event notification to UDM with “Success”.

About Latest Posts

(http://in.linkedin.com/pub/prasanna-sahu/29/257/91a)

Prasanna (Http://in.linkedin.com/pub/prasanna-sahu/29/257/91a)

I am Prasanna Sahu. I live in Dublin Ireland. I work in 3gpp wireless technology UMTS and LTE and 5G. I love Photography, painting. Know more about me: http://in.linkedin.com/pub/prasanna-sahu/29/257/91a
See my photographs: http://www.flickr.com/photos/24986299@N05/

Search

Search here

Search

Recent Posts

- Emergency Services(E911) FallBack procedures in 5G (http://5gblogs.com/emergency-servicese911-fallback-procedures-in-5g/)
- EPS Fallback Voice in 5G (http://5gblogs.com/eps-fallback-voice-in-5g/)
- 5G Security (5G AKA Authentication) (http://5gblogs.com/5g-security-5g-aka-authentication/)
- 5G Quality Of Services (QoS)

(http://5gblogs.com/5g-quality-of-services-qos/)

- 5G Network Identity SUPI/SUCI (http://5gblogs.com/concealing-of-supi-into-suci/)

Archives

- May 2020 (http://5gblogs.com/2020/05/)
- April 2020 (http://5gblogs.com/2020/04/)
- January 2020 (http://5gblogs.com/2020/01/)
- May 2019 (http://5gblogs.com/2019/05/)
- April 2019 (http://5gblogs.com/2019/04/)
- November 2018 (http://5gblogs.com/2018/11/)
- October 2018 (http://5gblogs.com/2018/10/)