Aspects of 5G’s authentication security and ways to mitigate threats

Stepan Davydov

JSRPC “Kryptonite”

КРИПТОНИТ

Authentication in 5G

КРИПТОНИТ

Authentication steps in 5G:

- $[ECIES]_{optional}$
- GUTI or SUCI transmission
- 5G-AKA or EAP-AKA’

Authentication security requirements:

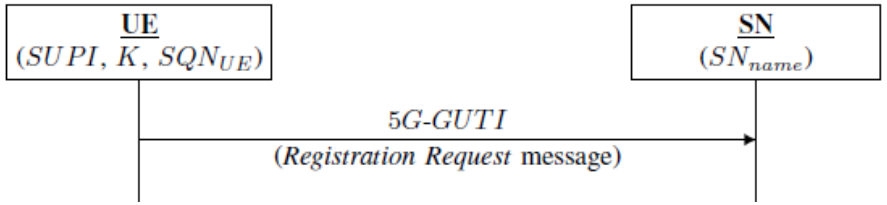
- Authentication between Subscriber (User), Serving Network and Home Network
- User identity confidentiality
- User location confidentiality
- User untraceability

Authentication between a user and its service provider is based on a shared symmetric key, thus can only take place after an initial user identification.

Initialization of Authentication

КРИПТОНИТ

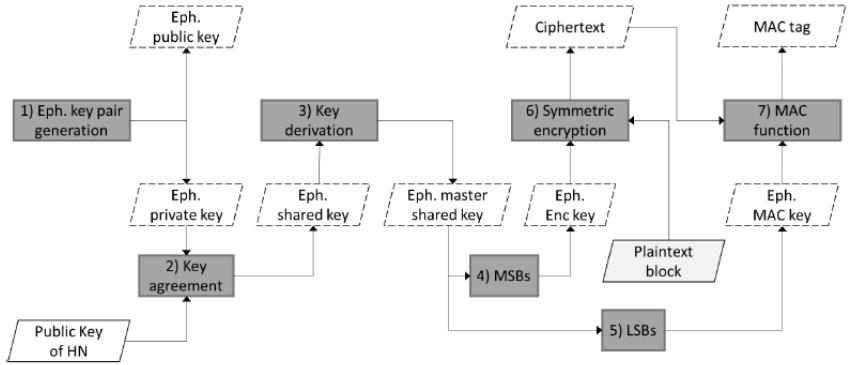
A GUTI (Globally Unique Temporary User Equipment Identity) is a frequently-changing temporary identifier, which is used for identification purposes over the wireless link before the establishment of a secure channel.



GUTI reuse is prohibited, so, if user has no fresh GUTI, SUPI (Subscription Permanent Identifier) transmission is needed.

ECIES scheme is used to protect identifier SUPI from intruder.

If ECIES is not used, IMSI-catching (SUPI-catching) attack is possible and “user identity confidentiality” is violated [3].



(a) Encryption at the UE side

5G-AKA

КРИПТОНИТ

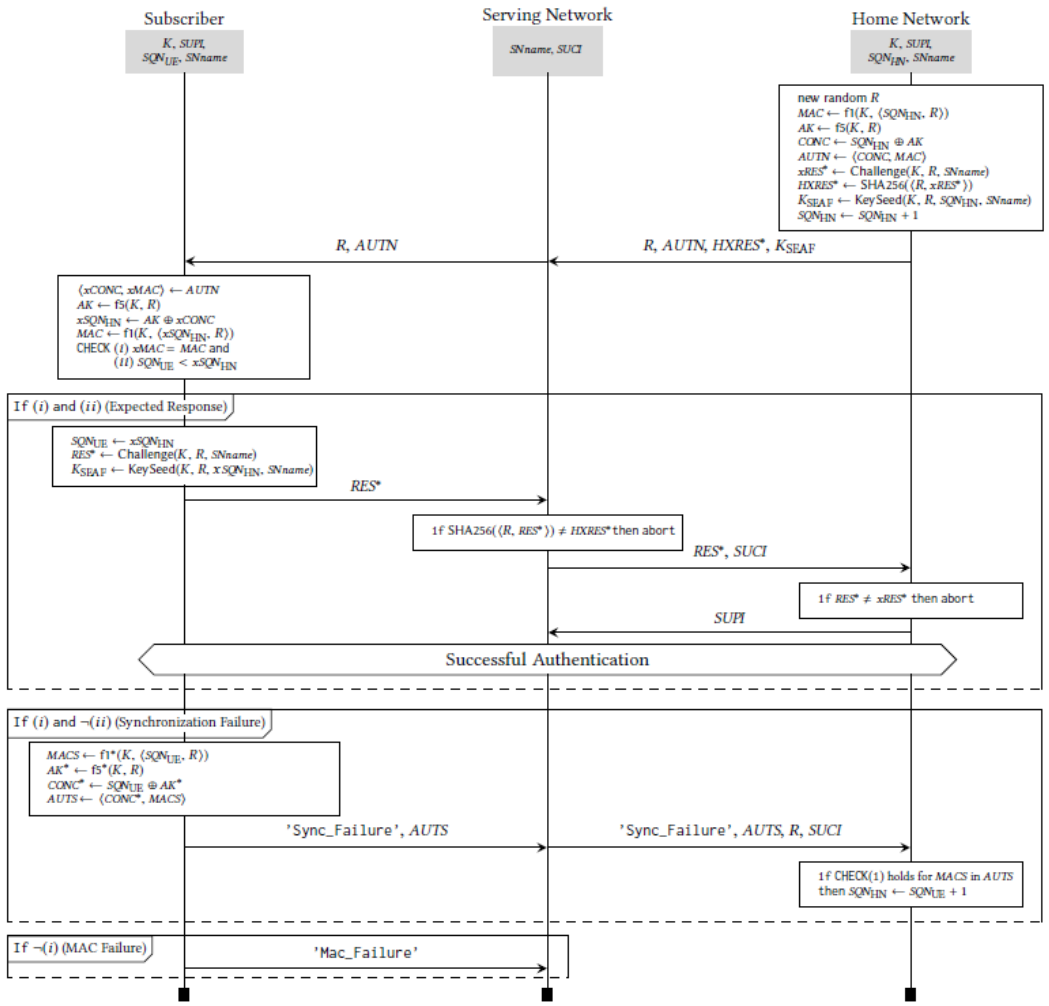


Figure 3: The 5G AKA protocol (continuing Figure 2)

Known vulnerabilities:

1. Linkability of Failure Message attack, (LFM-attack) Arapinis et al. 2012 [4]
2. SUCI replay attack, Fouque et al. 2016 [5]
3. Activity Monitoring Attack (AMA-attack), Borgaonkar et al. 2019 [6]

and other's

3GPP TR 33.846

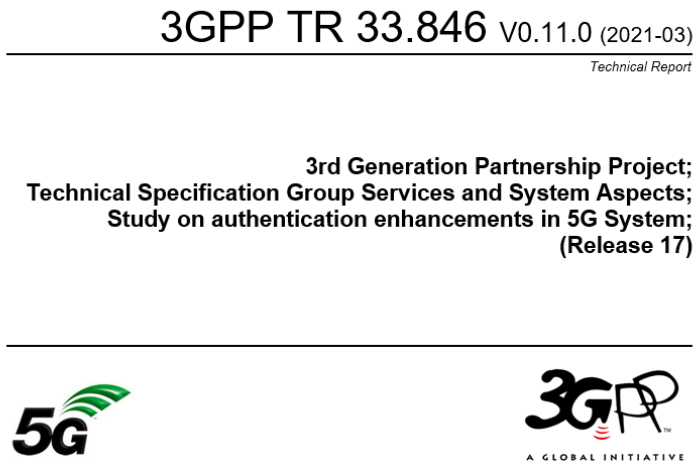
КРИПТОНИТ

In 2019 3GPP TR 33.846 “Study on authentication enhancements in 5G system” had been created.

There were six Key Issues corresponding known vulnerabilities in this document.

It had been concluded to have no normative work for two of them (KI #1.1, KI #3.1).

There were twenty-two solutions to mitigate another Key Issues.



3GPP TR 33.846 V0.11.0 (2021-03)

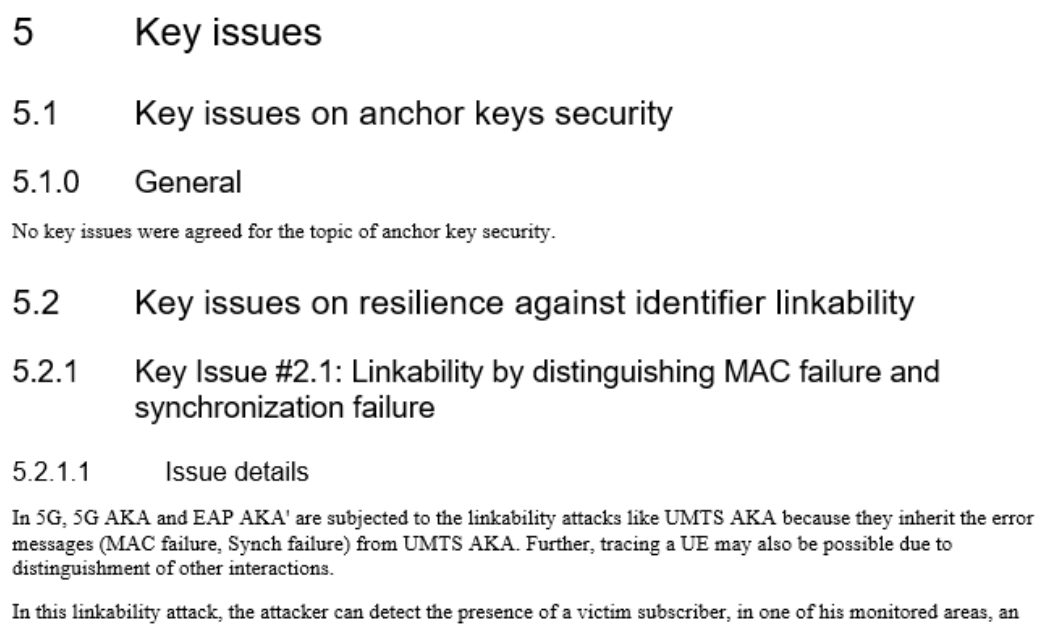
Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on authentication enhancements in 5G System;
(Release 17)

5G

3GPP

A GLOBAL INITIATIVE



5 Key issues

5.1 Key issues on anchor keys security

5.1.0 General

No key issues were agreed for the topic of anchor key security.

5.2 Key issues on resilience against identifier linkability

5.2.1 Key Issue #2.1: Linkability by distinguishing MAC failure and synchronization failure

5.2.1.1 Issue details

In 5G, 5G AKA and EAP AKA' are subjected to the linkability attacks like UMTS AKA because they inherit the error messages (MAC failure, Synch failure) from UMTS AKA. Further, tracing a UE may also be possible due to distinguishment of other interactions.

In this linkability attack, the attacker can detect the presence of a victim subscriber, in one of his monitored areas, an

3GPP TR 33.846

КРИПТОНИТ

In December 2021 the work on the document was concluded.

Only one solution (sol. #4.1) was chosen as an optional to deploy.

Solution #4.1 address only one(!) Key Issue (KI #4.1).

Another Key Issues and corresponding attacks are still possible in 5G-AKA.

Table 6.0-1: Mapping of solutions to key issues

	Key Issues							
Solutions	#1.X	#2.1	#2.2	#3.1 *)	#3.2	#4.1		
Solutions for anchor keys security								
No solution so far								
Solutions for resilience against identifier linkability								
#2.1: Handling of Sync failure by AUTS encryption						x		
#2.2: Encryption of authentication failure message types by UE with new keys derived from K_AUSF		x				x		
#2.3: Unified authentication response message by UE		x						
...	...		...		...			
Solutions on re-synchronisation in AKA								
#4.1: Using MACS as freshness in the calculation of AK						x		

One way to mitigate all vulnerabilities

КРИПТОНИТ

In August 2021 we proposed Solution #2.12 “Adding randomness on both sides to mitigate all replay-attacks and assuring SUCI generation by legitimate entity using MAC calculation on secret key”.

It was proposed:

- to add $RAND_{MS}$ to mitigate LFM attack and AMA attack;
- to add MAC calculation to mitigate SUCI replay attack, SUPI check and SUPI guessing attacks.

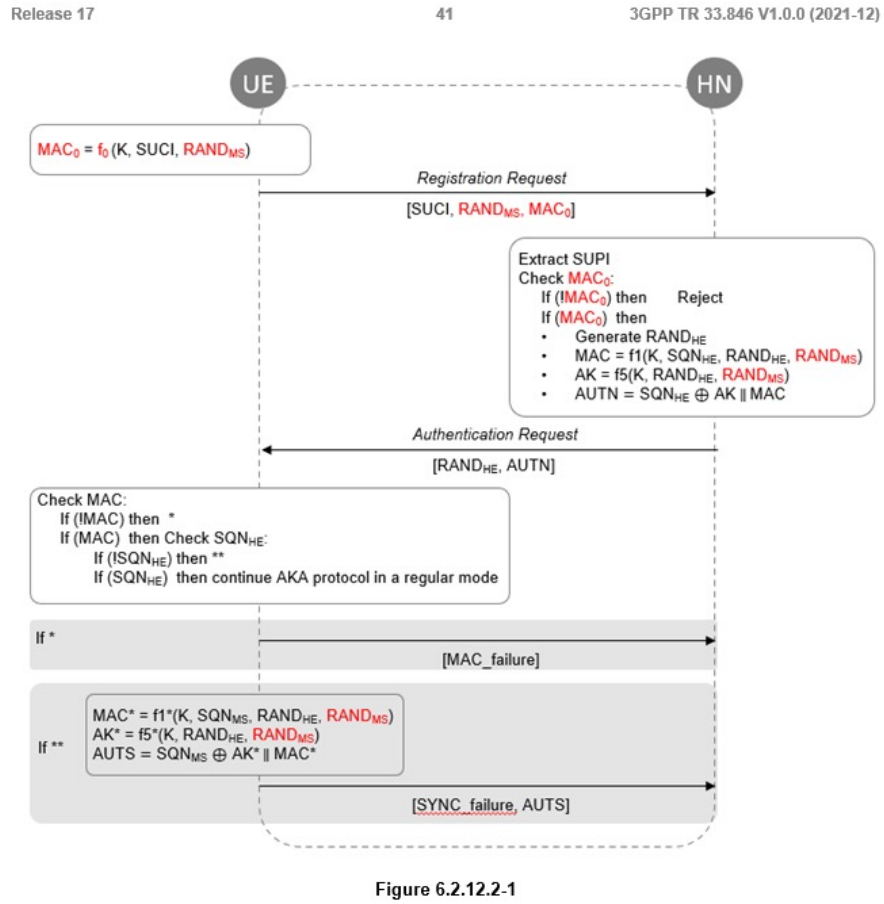


Figure 6.2.12.2-1

One way to mitigate all vulnerabilities

КРИПТОНИТ

Our Solution proposes changes in the protocol follows the accepted paradigm of constructing SigMa-like protocols [8], on which many modern protocols (e.g., TLS and IPSec) are based.

We strictly demand binding to the random numbers of both parties.

Our Solution mitigates all Key Issues (except KI #1.1, KI #3.1, which was concluded to have no normative work).

Table 6.0-1: Mapping of solutions to key issues

Solutions	Key Issues							
	#1.X	#2.1	#2.2	#3.1 *)	#3.2	#4.1		
Solutions for anchor keys security								
No solution so far								
Solutions for resilience against identifier linkability								
#2.1: Handling of Sync failure by AUTS encryption						x		
#2.2: Encryption of authentication failure message types by UE with new keys derived from K_AUSF		x				x		
#2.3: Unified authentication response message by UE		x						
#2.4: MAC-S based solution		x				x		
#2.5: Encryption of authentication failure message with SUCI method		x				x		
#2.6: Certificate based encryption of unicast NAS message		x				x		
#2.7: Mitigation against the SUCI replay attack			x					
#2.8: Assuring SUCI generation by Legitimate SUPI owner using K_{SUCI}			x					
#2.9: MAC, SYNCH failure cause concealment		x						
Solution to Key Issue #2.2: SUCI replay			x					
Solution #2.11: Mitigate the SUCI replay based on UE's public key			x					
Solution #2.12: Adding randomness and MAC calculation on the UE side		x	x		x	x		

Conclusion and our suggestions

КРИПТОНИТ

Since some replay attacks are still possible in 5G-AKA, we consider the work on the authentication enhancement must be continued.

It might be a good thing to follow the accepted paradigm of constructing SigMa-like protocols, which are cryptographically strong.

Among proposed the only way to mitigate all vulnerabilities is to implement changes from Solution #2.12 3GPP TR 33.846 to the ECIES scheme and 5G-AKA protocol.

References

КРИПТОНИТ

[1] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[2] 3GPP TS 33.102: "Security architecture".

[3] Khan, Haibat & Martin, Keith. (2020). A survey of subscription privacy on the 5G radio interface - The past, present and future. Journal of Information Security and Applications. 53. 102537. 10.1016/j.jisa.2020.102537.

[4] Arapinis, M., Mancini, L.I., Ritter, E., Ryan, M.D., Golde, N., Redon, K., & Borgaonkar, R. (2012). New privacy issues in mobile telephony: fix and verification. Proceedings of the 2012 ACM conference on Computer and communications security.

[5] Fouque, Pierre-Alain & Onete, Cristina & Richard, Benjamin. (2016). Achieving Better Privacy for the 3GPP AKA Protocol. Proceedings on Privacy Enhancing Technologies. 2016. 10.1515/popets-2016-0039.

[6] Borgaonkar, Ravishankar & Hirschi, Lucca & Park, Shinjo & Shaik, Altaf. (2019). New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. Proceedings on Privacy Enhancing Technologies. 2019. 108-127. 10.2478/popets-2019-0039.

[7] 3GPP TR 33.846: “Study on authentication enhancements in 5G system”.

[8] Krawczyk, Hugo. (2003). SIGMA: The 'SIGn-and-MAc'approach to authenticated Diffie-Hellman and its use in the IKE protocols. Proceedings of Crypto'03. 2729. 400-425. 10.1007/978-3-540-45146-4_24.

КРИПТОНИТ

Thank for your attention!

Stepan Davydov, cryptanalyst

s.davydov@kryptonite.ru

JSRPC “Kryptonite”

2022