Concerns regarding 5G AKMA security

Duparc, Max
Cyber-Defence Campus
armasuisse Science and Technology
Thun, Switzerland
max.duparc@ar.admin.ch
max.duparc@epfl.ch

Barschel, Colin
Cyber-Defence Campus
armasuisse Science and Technology
Thun, Switzerland
colin.barschel@ar.admin.ch

July 25, 2023

Abstract

We would like to share some concerns we have regarding the AKMA mechanism (as described in v18.0 of TS 33.535 [1] and in v18.0 of TR 33.737 [2]) that will likely impact its security with respect to its scalability and roaming capabilities. We indeed detail here several potential attacks & vulnerabilities that are possible due to some security weaknesses that those technical specifications hold and that we list here.

1 Introduction

In this document, we consider necessary that *the security provided by AKMA for a connection between a given UE and AF should not be impacted by other AFs.*

This is especially true regarding AFs that are external to the HPLMN of the UE, meaning external AFs and those that reside inside VPLMN. Indeed, these are not in the trust domain of the HPLMN, and their number is likely to expand drastically with the deployment of 5G SA. This is induced, among other things, in the first case by the introduction of MECs, (standardised by ETSI) and, in the latter, by the introduction of roaming hubs (standardised by GSMA).

Note that both mechanisms act either as an intermediary between PLMNs or can host AFs themselves. A compromised AF could remain unknown to the HPLMN and threaten the security of the HPLMN. This emphasises the necessity of our starting statement.

In this notice, we share some concerns we have regarding the validity of this affirmation. Indeed, assuming one malicious of these AFs exists in either of the previously stated domains enables potentially dangerous vulnerabilities and attacks. Note that, in all the following, apart from the above-mentioned AF, we consider all networks, and especially the VPLMNs, to be honest, and to follow 3GPP guidelines.

This notice is split into two sections. The first details the potential security vulnerabilities and attacks we found, while the second lists all security weaknesses they rely on. Whenever possible, the security risks are graded, and mitigations are proposed.

Contents

2 Potential vulnerabilities & attacks

In this part, we detail all potential vulnerabilities and attacks on AKMA that we found. They are listed in an order that we consider logical, following a gradation in severity.

2.1 Key requests by AF inside a VPLMN are accepted independently of UE position.

Any AF in a VPLMN that has a roaming agreement with the HPLMN of a given UE and gains access to its A-KID can request the HAAnF via the HNEF. This is possible independently of the fact that the UE is actually roaming inside the VPLMN. Indeed, both HNEF and HAAnF do not know the UE's current serving PLMN, i.e. location. This means the UE could be in its HPLMN, and a key request from an AF in the VPLMN would be considered valid and answered positively.

Consequences This increases the potency of attacks using AFs inside VPLMN, as there is no need for the UE to be inside the malicious AF's PLMN to perform some attacks. This makes attacks (2.2 & 2.3) usable as long as there exists a malicious AF in *any* VPLMN that has a roaming agreement with the HPLMN of the UE. This is especially problematic as operators have hundreds of roaming agreements.

Used weaknesses 3.1.3

2.2 Impersonate the AF to the UE using AKMA initiation

This attack is more theoretical than all the others but is interesting because it highlights what problems could occur from the lack of specification of the AKMA initiation (6.5 of [1]).

If a different FQDN is specified in the AKMA initiation message to be used to derive K_{AF}, then the AF shall be authenticated. Otherwise, this would enable the impersonation of the AF.

Used vulnerabilities 3.1.2, 3.2.4, 3.2.5

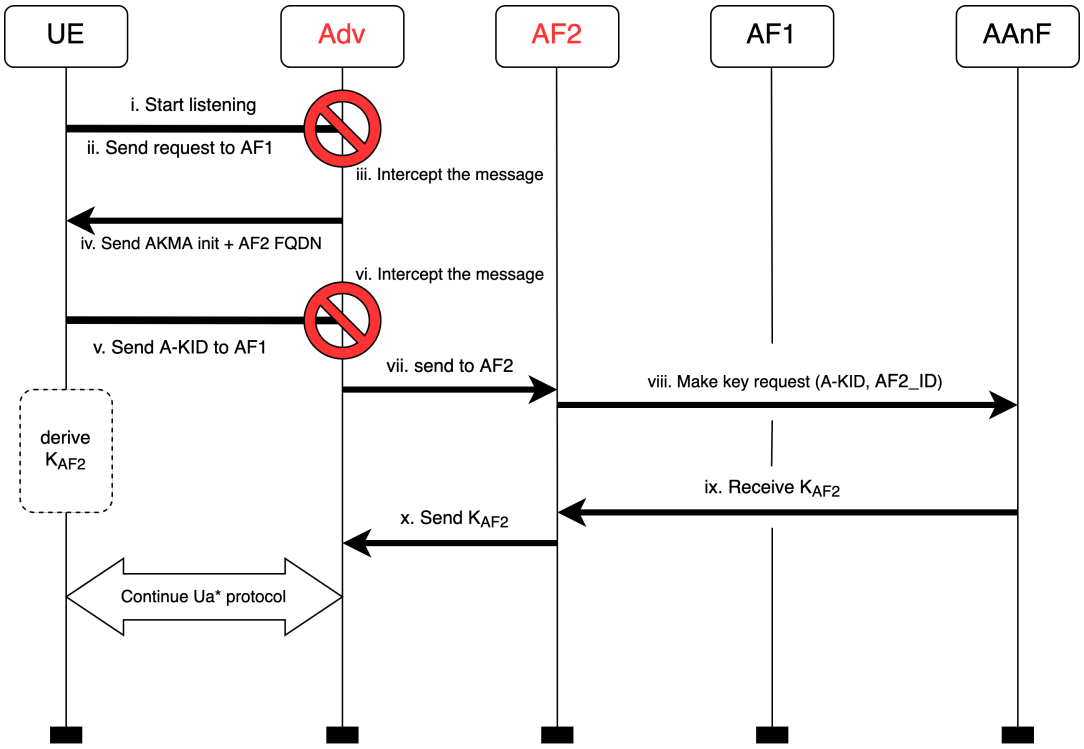

Figure 1: Impersonate attack via AKMA initiation

Needed conditions

- An UE wants to connect to AF1.
- The adversary can *intercept* all the exchanges between UE and AF1.
- The adversary has control of AF2, any kind of AF.
- The UE is *naive*, and believe what it is told.

Modus Operandi

(i) The adversary starts listening to traffic.

(ii) UE sends to the AF1 a request.

(iii) The adversary *intercepts* this request.

(iv) The adversary answers an AKMA initiation message that indicates AF2's FQDN as the FQDN that will be used for performing AKMA. It furthermore asks to use B.1.3 of [1] (TLS with PreShared Keys).

(v) The UE, being naive, derives K_{AF2} using AF2-ID and send its A-KID to AF1 using B.1.3 of [1].

(vi) The adversary *intercepts* this message.

(vii) A-KID is sent to AF2.

(viii) AF2 performs a key request to the home network using A-KID and AF2-ID.

(ix) AF2 receives K_{AF2} and forwards it to the adversary.

(x) AF2 forwards it to the adversary that continue Ua*, thus impersonating AF1.

2.3 Privacy breaking attack via AKMA

We now explain how an adversary can retrieve the GPSI (Generic Public Subscription Identifier) of a UE trying to enter contact with an AF. The adversary listens to an AKMA first message to AF1 and uses the retrieved A-KID and AF1-ID to get the GPSI. AF2 provides this information.

This attack is a GPSI catcher that works outside the core network, provided AF1 is external. This potential attack represents a danger to privacy.

Here, the attack is presented for a fixed AF1. Still, as the AF's identity (AF1-ID) can be found in the first message of the UE, the adversary could listen to traffic and identify Ua* connections that pass through.

The attack is described in figure 2.

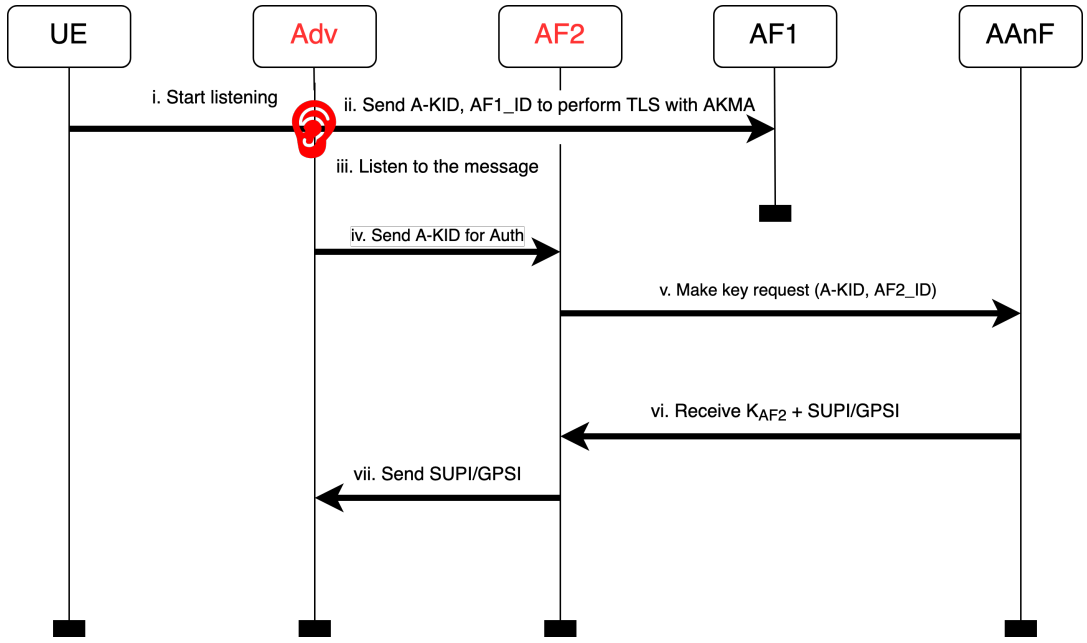

Figure 2: Privacy breaking attack

Needed conditions

- An UE wants to connect to AF1 using B.1.3 of [1].
- The adversary can *listen* at the exchanges between UE and AF1.
- Adversary has access to AF2, an AF authorised to receive GPSI.

Used weaknesses 3.1.4, 3.2.3, 3.2.4

Modus Operandi

(i) Adversary starts listening to traffic.

(ii) UE initiates an Ua* connection to AF1 using B.1.3 of [1].

(iii) The adversary *listen* to their first message.

(iv) The adversary sends the A-KID to AF2.

(v) AF2 sends a key request to the HPLMN (using A-KID and AF2-ID).

(vi) AF2 receives the desired GPSI from the home network.

(vii) AF2 sends back the GPSI to the adversary.

Remarks:

- This attack is totally independent of the capabilities of AF1, meaning that it only depends on what AF2 is allowed to ask the HPLMN.
- There exist AFs like MECs that have the additional property that UEs connect them only if they are in a very specific location. This attack on those AFs can be seen as a GPSI catcher.

2.4 Lacks of roaming LI specifications enables AF inside the VPLMN to make AKMA key request via VAAnF

Although AKMA LI (Legal Interception) architecture and targets are fully defined in section 7.15.3 of [3], its application in case of roaming, available at the end of [2], concerns us. We are especially worried about its lack of specifications. This will most likely result in different protocols being used. They could be incompatible with each other and also hold dangerous vulnerabilities.

For example, we now detail why, for LI reasons, sharing the $\mathsf{K}_{\mathsf{AKMA}}$ with the VPLMN where the UE is roaming enables AFs inside this VPLMN to bypass the HPLMN NEF for any key request. As specified in 4.3 of [2], any AF must access the AAnF via the HNEF. However, during roaming, the $\mathsf{K}_{\mathsf{AKMA}}$ is stored in the VPLMN, possibly inside the VAAnF. The presence of thoses master keys could be easily misused. While we suppose an honest VPLMN, a malicious AF could retrieve any K_{AF} keys by knowing the A-KID and AF-ID.

Used weaknesses 3.1.3, 3.2.1, 3.2.2

Modus Operandi

If, as proposed in some LI roaming solutions [1], we send the $\mathsf{K}_{\mathsf{AKMA}}$, SUPI and A-KID to the VPLMN and they are stored in the VAAnF, we enable AFs inside the VPLMN to ask for K_{AF} not only via the HNEF but also via the VAAnF. Indeed, for the VAAnF, a $\mathsf{K}_{\mathsf{AKMA}}$ is identified with the received A-KID, meaning that AKMA is enabled. It would therefore derive K_{AF} and provide it to the AF. This also works because the VAAnF does not check the HNI in the A-KID.

The malicious AF may not know in which AAnF the $\mathsf{K}_{\mathsf{AKMA}}$ is stored, but it can try all AAnFs.

Remarks

- In some very specific cases (if using the RID inside the A-KID, the VNEF can find in which VAAnF the LI information are stored), an external AF could also obtain K_{AF} by making a key request to the VNEF. This enables external AFs trusted by the VPLMN to use AKMA with the UE. Those external AF need not be trusted by the HPLMN, which is a problem.
- For this vulnerability to be active, we need $\mathsf{K}_{\mathsf{AKMA}}$ to be stored in a VAAnF, but this is logical as AAnFs are designed to store $\mathsf{K}_{\mathsf{AKMA}}$.
- We think that the SA3 group should state unambiguously if VPLMNs can ask for $\mathsf{K}_{\mathsf{AKMA}}$ for LI purpose. Furthermore, the LI roaming architecture should be specified, particularly regarding key management.

2.5 Wiretap attack on AKMA

This attack enables an adversary to break the confidentiality of AKMA by retrieving the master key of the TLS tunnel. It is described in figure 3.

[1] #5, #8, #10, #11, and #12 of [2]

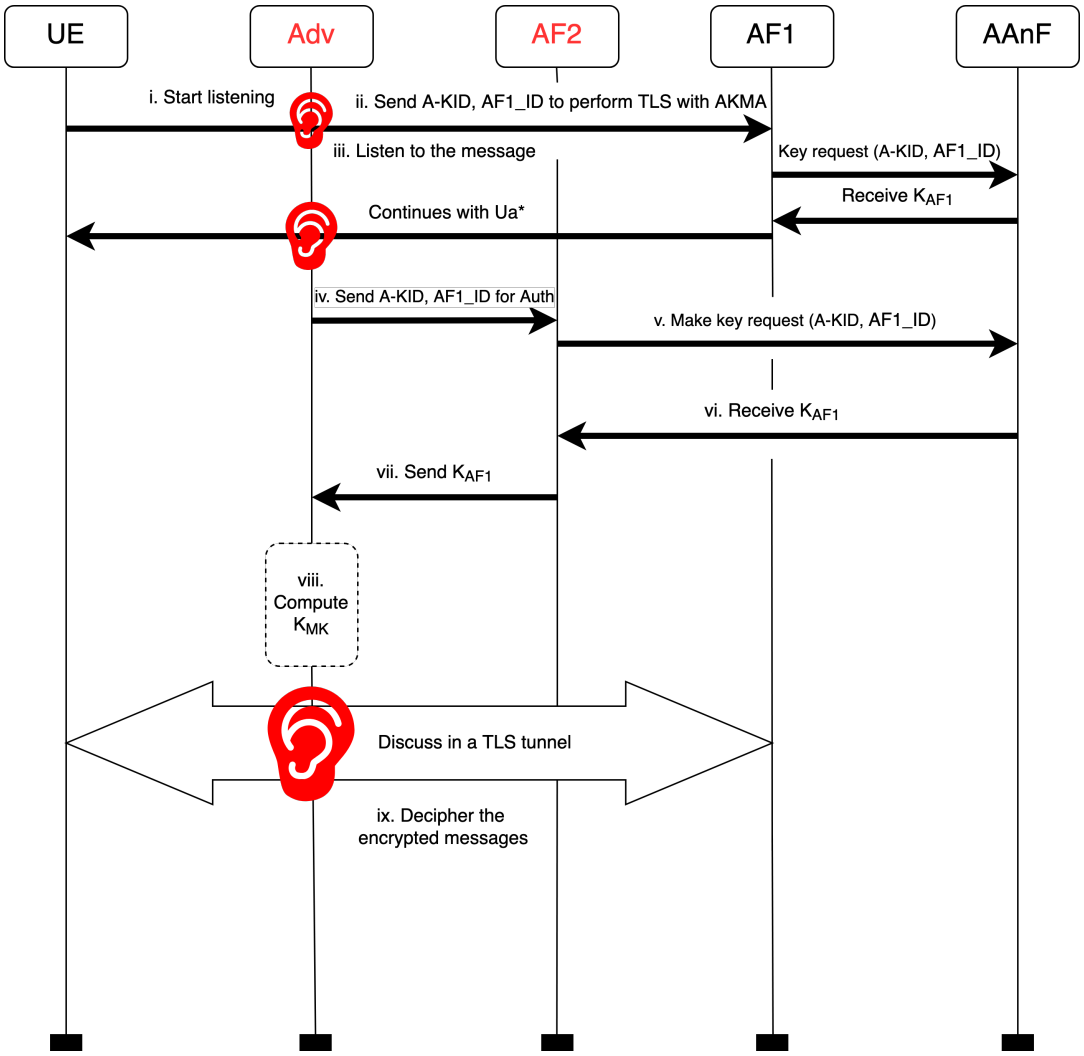

Figure 3: Wiretap attack

Needed conditions

- An UE wants to connect to AF1 using B.1.3 of [1] with a cipher-suite based only on PSK.
- The adversary can *listen* at the exchanges between UE and AF1.
- The adversary has control of AF2, an AF inside the VPLMN where the UE roams.
- The adversary is able to perform 2.4 above or has direct access to the AAnF.

Used weaknesses 3.1.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5

Modus Operandi

(i) The adversary starts listening to traffic.

(ii) The UE initiates a Ua* connection to AF1 using TLS with only PSK derived from AKMA.

(iii) The adversary *listen* to the first message (in clear text by definition), with the A-KID and AF1-ID.

(iv) The adversary sends the A-KID and AF1-ID to AF2.

(v) AF2 sends a key request to the network (using A-KID and AF1-ID).

(vi) AF2 receives the K_{AF1} from the network.

(vii) AF2 sends back the K_{AF1} information to the adversary.

(viii) The adversary derives the TLS master key K_{MK} following rule in [4].

(ix) The adversary uses this key to decipher all messages exchanged between the UE and the AF using Ua*.

Remarks

- The query from AF2 to the AAnF must be done before the A-KID is no longer valid, i.e. before the next primary authentication or AKMA context removal.

2.6 MitM Attack on AKMA

We now detail how an adversary can perform a man-in-the-middle attack between the AF and the UE. It is described in figure 4. [2]

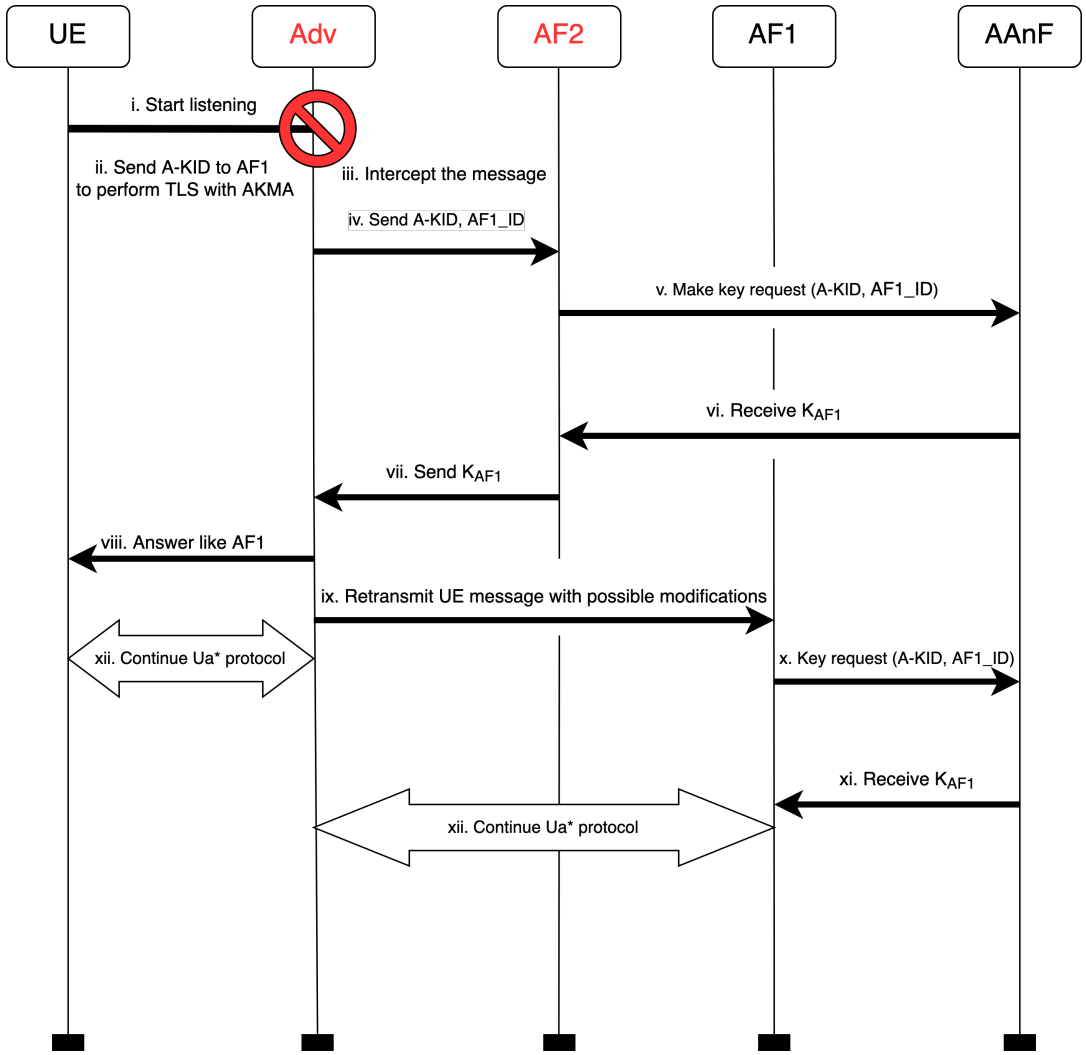

Figure 4: Man-in-the-Middle attack

[2]This attack is based on the idea found in [5], which depicted how an adversary could impersonate the AF. We have expended it in the form of a full MitM attack.

Necessary conditions

- An UE want to connect to AF1 using B.1.3 of [1].
- The adversary is able to *intercept* the exchanges between UE and AF1.
- Adversary has the control of AF2, an AF inside the VPLMN where the UE roams.
- The adversary is able to perform 2.4 above or has direct access to the AAnF.

Used weaknesses 3.1.1, 3.2.2, 3.2.3, 3.2.4

Modus Operandi

(i) The adversary starts listening to traffic.

(ii) UE initiates an Ua* connection to AF1 using B.1.3 of [1].

(iii) The adversary *intercepts* the first message (in clear text by definition), with the A-KID and AF1-ID.

(iv) The adversary sends the A-KID and AF1-ID to AF2.

(v) AF2 sends a key request to the network (using A-KID and AF1-ID).

(vi) AF2 receives the $\mathsf{K}_{\mathsf{AF1}}$ from the network.

(vii) AF2 sends back the $\mathsf{K}_{\mathsf{AF1}}$ to the adversary.

(viii) The adversary answer like AF1 would using $\mathsf{K}_{\mathsf{AF1}}$ and continue the Ua* connection.

(ix) The adversary then sends the initial request of the UE to AF1 and modify the secret part of the Diffie-Hellman in case it is used.

(x) AF1 performs the key request to the AAnF/NEF.

(xi) AF1 receives $\mathsf{K}_{\mathsf{AF1}}$ from the AAnF/NEF.

(xii) $\mathsf{K}_{\mathsf{AF1}}$ is then used to continue the Ua* connection to finish the MitM attack.

Remarks

- All this protocol must be performed before the timeout of the UE that waits for an answer.
- We can of course perform only half of this attack and impersonate the AF to the UE or the UE to the AF, depending on the situation.

	Used weakn.
2.1	3.1.3
2.4	3.1.3 3.2.2 3.2.1

Figure 5: Summary table of potential vulnerability

	Used weakn.	External AFs	AFs in UE's VPLMN	AFs in other VPLMNs
2.2	3.1.2 3.2.2 3.2.4	✓	✓	using 2.1
2.3	3.1.4 3.2.3 3.2.4	✓[3]	✓	using 2.1
2.5	3.1.1 3.2.2 3.2.3 3.2.4 3.2.5	not doable	using 2.4	not doable
2.6	3.1.1 3.2.2 3.2.3 3.2.4	not doable	using 2.4	not doable

Figure 6: Summary table of potential attacks assuming an AF under control

[3]Depending on the network local policy.

3 Security weaknesses

In this section, we list all security weaknesses that we identified during our analysis. We grade the security risk they represent and propose mitigation whenever possible. We split them into two categories. The first corresponds to security weaknesses that necessitate, in our eyes, strong consideration, as they are the cornerstone of the previously stated vulnerabilities. The second is security weaknesses that do not lead by themselves to vulnerabilities (although they can contribute). It is, therefore, good to know their existence to monitor them.

3.1 Primary security weaknesses

3.1.1 The AAnF does not check that the send AF-ID correspond to the sending AF.

Description: We consider two AFs (AF1 and AF2), with AF2 having direct access to the AAnF and with a valid A-KID and AF1-ID. Then AF2 can send an Application-Key_Get_Request(A-KID, AF1-ID) to the AAnF and will receive a valid key. Indeed, the AAnF does not verify that AF1-ID correspond to AF2 and considers the request valid.
This vulnerability was, up until v17.7 of [1], possible for any AF but was patched in the NEF but not in the AAnF, therefore solving only half of the problem, as not providing security in case AFs can connect directly to AAnF.

Security risks: High (it enables 2.5 and 2.6)

Mitigations: The AAnF should check that the send AF-ID corresponds to the sending AF too. As specified in [6], there are three different mechanisms for authorisation for 5G SBA:

- Using OAuth, where a token must be acquired in order to request services from other NFs. In this case, the AAnF should check that the FQDN in the AF-ID corresponds to one of the tokens.
- Using TLS certificates. Similarly to before, we can check that the FQDN of the certificate is in fact the one inside AF-ID.
- Using "trusted network", meaning that the NFs accept anything from inside the network. In order to be secure, this type of authorisation often relies on a secure environment, meaning that all internal AFs should be known. It may therefore be possible to check that the IP address of the asking AF and FQDN in the AF-ID matches, using a whitelist.

  At the very least, a cautionary note should be stated.

Additionally, we recommend clarifying the wording of the NEF patch in 6.2 of [1] which is rather unclear. It states that: *"If the AF is authorised by the NEF to request* $\mathsf{K_{AF}}$*, including the authorisation after verification of the AF-ID, the NEF discovers and selects an AAnF."* Kept as it is, this may lead to implementation errors.

3.1.2 The AKMA initiation protocol is underspecified.

Description: The specification of the AKMA initiation protocol (6.5 in [1]) is unclear on its limitations and thus on what it allows and what it does not. In its current state, it enables the AKMA initiation message to contain a different FQDN from the requested AF. The UE will use this information to derive the K_{AF} key on its side.
For example, this scenario could be set up by a VPLMN that does not want other PLMNs to know the FQDN of its AFs. This could indeed reveal its internal architecture to competitors. In this case, It would use a specific AF to handle all roaming AKMA demands.

Security risks: Medium (as 2.2 also depend on the UE).

Mitigations: We think 3GPP should provide detailed specifications like it did for Ua*. A crucial point to consider is to know whether or not AFs can indicate inside their AKMA initiation message a FQDN used do derived K_{AF} and what are the limitations. (We recommend that the AF be authenticated by the UE).

3.1.3 The AAnF and NEF do not know the UE's serving PLMN.

Description: The AAnFs and NEFs are ignorant of the serving PLMN ID in which the UE is currently. This means that key requests are handled independently of UE position.

Security risks: High (It enables 2.1)

Mitigations: The UE-Serving PLMN IDentifier (UE SN-ID) used during the latest primary authentication should be sent to the HAAnF by the AUSF and should be checked in case of a key request. This means that the HAAnF should ensure that the only VPLMN able to use AKMA is the UE-Serving PLMN. This could be done by the HNEF. When receiving a key request from an AF that is internal in a VPLMN, the HNEF forwards the AF's VPLMN ID (noted AF SN-ID) to the AAnF which would then check if it agrees with UE SN-ID.
This is an easy fix as all connections between NEF and AFs are authenticated with TLS certificates.

3.1.4 The privacy of the UE is only dependent on the AF and the 5G network.

Description: An UE has no say whether or not an AF is authorised to query its SUPI/GPSI, as it only depends on the 5G network policy regarding the AF. Furthermore, the UE is not informed when it occurs.
Security risks: High (as it enables 2.3)

Mitigations: This weakness is very hard to solve without changing the design of the AKMA mechanism. Our best idea is to make use of the fact that AKMA requires that we previously finished a primary authentication, meaning that there exists a way to create a secure tunnel between the UE and the HPLMN (this can be done by using the shared secret between UE and AAnF that is K_{AKMA}). Therefore, we propose that before sending the A-KID to an AF, UE send *securely* to the AAnF the AF's FQDN and waits for the acknowledgement. Note that the UE must know the AF's FQDN as it is necessary to compute K_{AF}. We then follow the AKMA key request up until the AAnF has to derive K_{AF}. At that time, the AAnF checks the AF-ID and that it agrees with the FQDN sent by the UE. Our solution can be criticised because it increases both the Round-Trip Time (RTT) and the complexity of the implementation on the UE and network side. However, it guarantees that only AF selected by the UE can use AKMA.

In any case, this security weakness requires great attention. Additionally, we think that consideration should be put on which AFs are allowed to receive SUPI/GPSI via AKMA.

3.2 Secondary security weaknesses

3.2.1 The HNI inside the A-KID is not checked by the AAnF and the NEF.

Description: The NEF and AAnF do not check during a key request that the HNI inside the A-KID corresponds to their respective PLMN. This becomes problematic when considering that AAnFs, when receiving an A-KID, will just check that they hold a $\mathsf{K_{AAnF}}$ identified by this A-KID to know whether or not AKMA is enabled.

Security risks: Low (This only starts getting problematic if $\mathsf{K_{AAnF}}$ is distributed in several VPLMN, as in 2.4.)

Mitigations: The HNI inside the A-KID should be checked by both the AAnF and NEF in order for them to refuse all A-KIDs that are not from the AAnF's or NEF's network.

3.2.2 $\mathsf{K_{AF}}$ is deterministically derived.

Description: If we make two key request with the same $\mathsf{K_{AKMA}}$, A-KID and AF-ID, then we will receive two time the same $\mathsf{K_{AF}}$.

Security risks: Low

Mitigations: This weakness is impossible to mitigate as it comes from the deliberate decision to make AKMA an explicit bootstrapping protocol, meaning that no handshake between the AAnF and the UE is performed.

3.2.3 $\mathsf{K_{AKMA}}$ and A-KID are AF-independent and are rarely renewed.

Description: A-KID and $\mathsf{K_{AKMA}}$ are only renewed by running the primary authentication or by using the context removal procedure. If the latter depends on the network policy, the former can be considered a rare event to limit resource usage. Therefore, both A-KID and $\mathsf{K_{AKMA}}$ can be considered as fixed in the order of one hour. An intercepted A-KID could be misused during this time frame

Security risks: Low

Mitigations: This is hardly mitigable as having $\mathsf{K_{AKMA}}$ and A-KID independent from AFs is core to AKMA, as it was one of its design requirements.

3.2.4 B.1.3 of [1] send the A-KID and AF-ID in clear.

Description: By the design of TLS (both 1.2 and 1.3), the cipher-suite, the A-KID and the FQDN of the AF are available in cleartext inside in the clientHello message of the UE to the AF.

Security risks: Low

Mitigations: This is hardly mitigable because that information is necessary for authentication and sometimes confidentiality. They can not be sent in an encrypted extension. This is an issue that B.1.2 of [1] does not have, as A-KIDs are sent inside a preexisting TLS tunnel. This latter one should therefore be preferred.

3.2.5 Using B.1.3 of [1] with cipher-suites using only PSK does not provide forward security.

Description: Detailed in 2.2 of [7].

Security risk: Low (although it enables 2.5)

Mitigations: This is an old and widely known security weakness of TLS using only PSK. However, those cipher-suites must be kept in order to enable secure connection for extremely low-capacity systems, which are one of AKMA's targets. We would advise to prefer other cipher-suites, whenever possible.

We represent in figure 7 all our proposed mitigations to AKMA key request protocol.

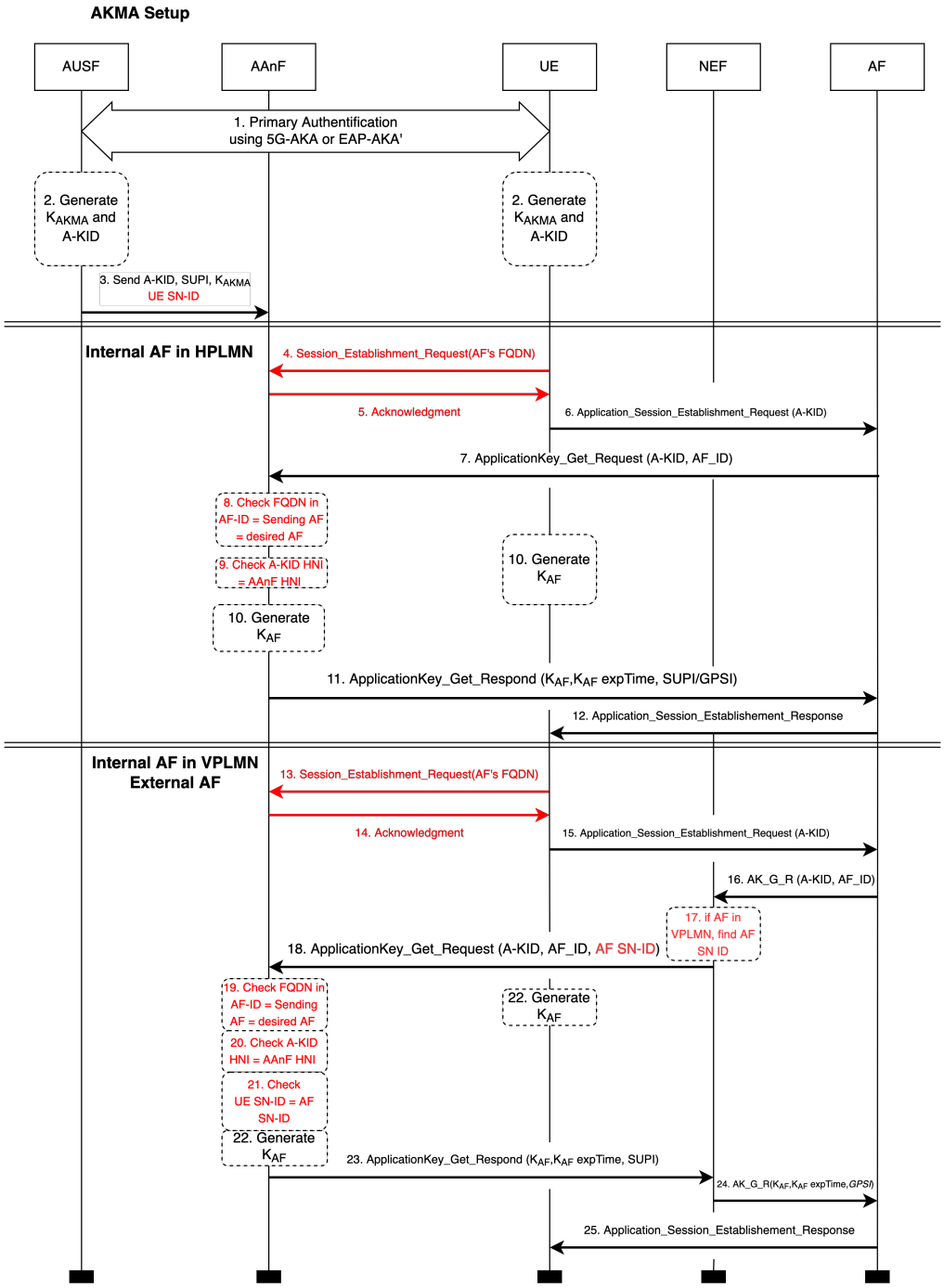

Figure 7: AKMA key request protocol with mitigations (simplified version)

References

[1] 3GPP, "Authentication and key management for applications," Tech. Rep. 33.535 v18, 3rd Generation Partnership Project (3GPP), June 2023.

[2] 3GPP, "Study on authentication and key management for applications phase 2," Tech. Rep. 33.737 v1.0, 3rd Generation Partnership Project (3GPP), June 2023.

[3] 3GPP, "Lawful interception (li) architecture and functions," Tech. Rep. 33.127 v18.3, 3rd Generation Partnership Project (3GPP), Mar. 2023.

[4] Y. Li, S. Schäge, Z. Yang, F. Kohlar, and J. Schwenk, "On the security of the pre-shared key ciphersuites of tls," in *Public-Key Cryptography–PKC 2014: 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings 17*, pp. 669–684, Springer, 2014.

[5] G. Akman, P. Ginzboorg, M. T. Damir, and V. Niemi, "Privacy-enhanced akma for multi-access edge computing mobility," *Computers*, vol. 12, no. 1, p. 2, 2022.

[6] 3GPP, "Security architecture and procedures for 5g system," Tech. Rep. 33.501 v18.0, 3rd Generation Partnership Project (3GPP), Dec. 2022.

[7] IETF, "The transport layer security (tls) protocol version 1.3," Tech. Rep. 8446, Internet Engineering Task Force, Aug. 2018.