On An Ephemeral Identifier and Injective Agreement Authentication for 6G Systems

Geir M. Køien

University of South-Eastern Norway (USN), Campus Vestfold, Norway
geir.koien@usn.no

Abstract. In this paper we propose introducing an ephemeral identifier for providing lightweight and inexpensive identity- and location privacy in 6G. We also propose to revise the current authentication and key agreement (AKA) protocol model. The current model dates back to 2G/3G, and while 4G and 5G have added to it, it is time to revise it.

Keywords: Authentication and Key Agreement · Injective Agreement · Ephemeral Identifier · Identity Privacy · Quantum-safe · 6G

1 Introduction and Problem Statement

1.1 Background

The mobile systems have had a family of AKA protocols that dates back to 2G systems. For 2G, the protocol was staged and unilateral, and one only derived one session key. The 5G-AKA protocol is still staged, but provides mutual authentication and derives a key hierarchy [4]. The 5G-AKA scheme is complex, and crucially depends on the 3G cryptographic core functions. Identity privacy relies on avoiding exposure of the permanent subscriber identifier. In 5G, one finally solved this problem, but unfortunately the solution is not quantum-safe.

1.2 Quantum-Safety

The 6G system is expected be completed in late 2029, and will be the main generation for appox. 10 years. Historically, it will be operational for at least another 10 years after that. It is therefore imperative to take quantum-safety into account. Symmetric-key primitives, like the one used in the 5G-AKA protocol, are considered quantum-safe. One *may* need to extend the key length, and one should prepare for this. The SUCI scheme (see clause 2.3), which provide identity privacy, is the exception (it uses elliptic curve cryptography). It is possible to define quantum-safe SUCI solutions [6, 7]. Still, there is a communications cost associated with this, and alternative solution should be sought.

1.3 Problem Statement

We investigate and propose a new model for a 6G-AKA protocol, and a new ephemeral identifier that provides lightweight identity privacy.

2 Architecture, Actors and Identifiers

2.1 The Principal Parties

We have three principle parties in our model:

- UE: The mobile device ("User Equipment"). The "subscriber".
- HN: Home Network. Where the UE has its subscription for service access.
- VN: Visited Network. The radio access network used by the subscriber.

The VN and HN *may* be controlled by the same administration. However, the roaming procedures are agnostic with respect to who controls the VN.

2.2 Relationships and Security Contexts

There is a subscription relationship between the UE and the HN. The HN has *security jurisdiction* over the UE. Then there are roaming agreements between the HN and the VNs, which permit UEs to use VN services. The outcome of a 6G-AKA protocol run will be the establishment of a UE-HN primary security context, and a UE-VN control plane context. There is also a UE-VN user plane context, subsequently derived from the control plane context. Each context will have its own *anchor* key (a key-deriving key). The security context structure is similar to that of 5G [4].

2.3 Subscriber Identifiers and Identity Privacy

Identifiers in the 3GPP-based systems is defined in TS 23.003 [2].

Subscription Permanent Identifier (SUPI): The primary identifer for the UE is the SUPI. The SUPI is globally unique, and will usually be instantiated as an International Mobile Subscription Identity (IMSI).

Globally Unique Temporary UE Identity (GUTI): The systems have a temporary subscriber identifier for UE-VN use. The identifier, called TMSI in 2G, is assigned after having run the AKA protocol and started encryption. Subsequently, the TMSI is used in clear over-the-air. The use of TMSI avoids using the SUPI for most use-cases, and thus it provides a measure of *identity privacy* for the subscriber. One still has to use the SUPI for *initial registration* cases, and the VN can always request the identification to be by SUPI. In 4G and 5G, the TMSI is part of the compound identifier GUTI. The GUTI includes address information related to the VN access network.

Subscription Concealed Identifier (SUCI): In 5G, one introduced the SUCI-scheme (Annex C in [4]). Here one encrypts the SUPI, using an elliptic curve integrated encryption scheme (ECIES). Unfortunately, ECIES is not quantum-safe. Note that one may define post-quantum cryptography (PQC) compliant profiles for SUCI [7], and this could remedy the problem.

2.4 The Staged AKA Execution Model

The AKA protocol include the concept of an authentication vector (AV). The AV is forwarded from the HN to the VN, and the VN runs the actual challenge-response towards the UE based on the AV. In 5G, one has strengthened the security somewhat, but one still has retained the delegated ("forward AV") aspects. The staged AKA model dates back to 2G/GSM, and is due for retirement.

2.5 Mutual Entity Authentication and Sequence Number Scheme

Since 3G, the AKA protocols provide mutual authentication [1, 3, 4]. That is, the challenge is authenticated so that the UE knows it was issued by the HN. A sequence number provides freshness/timeliness guarantee. The assurance is weak, given the staged AV forwarding and imprecise freshness assurance.

2.6 The SIM History and the 3G Legacy

The subscription credentials are associated with the Subscription Identification Module (SIM). Historically, the SIM has been software hosted on a smartcard. The cost of upgrading the physical SIM is huge, and so one has avoided this (since 3G). Consequently, the SIM still is based on the cryptographic functions and primitives introduced with 3G. However, since 4G one have had downloadable SIM versions (eSIM/iSIM). The downloadable model is assumed to be dominant for 6G. Hence, one is now free to redefine the SIM, and its cryptographic core.

3 An Ephemeral UE Identifier

3.1 Identity Presentation

Identity presentation can today take place with either SUPI, GUTI or SUCI. What is missing is an ephemeral identifier for use between the UE and the HN. Such an identifier should offload the need for SUCI, and be inexpensive to use.

3.2 Introducing the Globally Unique Ephemeral UE Identifier

Today, one cannot avoid presentation by means of SUPI or SUCI for *initial registration*. Also, when the GUTI is not recognized (for whatever reason), the network may explicitly ask for identification by a HN issued identifer. One must avoid exposing the SUPI, and a quantum-safe SUCI will be costly to run. Thus, we propose the GUEI:

$$GUEI = nonce + HN{-}routing{-}info$$

The *HN-routing-info* will be similar to the SUCI routing information. The GUEI is derived by the 6G-AKA protocol, and it is valid for the HN-UE context. The next AKA invocation will regenerate the GUEI. The HN stores the GUEI

in a lookup-table in order to retrieve the associated SUPI. A GUEI is only to be used for initial registration cases (which triggers the AKA protocol). The GUEI scheme cannot entirely prevent the need for SUCI, but one can significant reduce the need. An active intruder can still force the use of the SUCI scheme. Frequent use of SUCI should therefore be monitored. The GUEI may be defined as a new identifier, but it can conceivable also be fitted into a new SUCI profile.

4 A Subscriber Initiated Injective Agreement Protocol

4.1 Combined Identity Presentation and Subscriber Challenge

It is strongly suggested that one combines the *identity presentation* procedure with a *subscriber challenge*. That is, the identification is provided in conjunction with a pseudo-random challenge issued by the subscriber. Identification by GUTI may be with- or without a challenge, depending on the need for re-authentication.

4.2 Injective Agreement

The term *injective agreement* is used when we want to "insist that there is a one-one relationship between the two agents' runs." [8]. We propose a two-way subscriber initiated challenge-response protocol to provide injective agreement.

4.3 The Role of the VN

The VN is not directly part of the UE-HN injective agreement, but adds a nonce for derivation of the UE-VN anchor key and inclusion in the UE-HN context. UE-HN control plane re-keying procedures may be done in conjunction with handovers, as it is today in 5G [4].

4.4 Protocol Outline

We assume that the reader is aware of the common symmetric cipher primitives. Furthermore, we keep the model as an outline, ignoring many important details.

- AUK: The authentication key shared between UE and HN
- RAK: The roaming agreement key shared between VN and HN
- HID, VID: The public HN/VN identifier.
- UID: This may be a SUPI, SUCI, GUTI or GUEI.
- $RAND, RES$ The random challenge/response

The cryptographic functions:

- `Nonces:` $RAND_n = prf(\cdot)$
- `UE-HN anchor key:` $K_{UEHN} = kdf_{AUK}(RAND_{UE}, RAND_{HN})$
- `UE-VN anchor key:` $K_{UEVN} = kdf_{K_{UEHN}}(RAND_{VN})$
- `Response to UE:` $RES_{UE} = mac_{AUK}(RAND_{UE}, RAND_{HN}, RAND_{VN})$
- `Response to HN:` $RES_{HN} = mac_{AUK}(RAND_{HN}, RAND_{UE}, RAND_{VN})$
- `The GUEI:` $GUEI = prf_{AUK}(RAND_{UE}, RAND_{HN})$ + HN-routing-info

A 6G-AKA protocol model outline:

1. $UE \rightarrow VN$: $UID, RAND_{UE}$
2. $VN \rightarrow HN$: $UID, RAND_{UE}, VID, RAND_{VN}$
3. $HN \rightarrow VN$: $RES_{UE}, RAND_{HN}, \{SUPI, K_{UEVN}\}_{RAK}, \{VID, K_{UEVN}\}_{AUK}$
4. $VN \rightarrow UE$: $RES_{UE}, RAND_{HN}, RAND_{VN}, \{VID, K_{UEVN}\}_{AUK}, \{GUTI\}_{K_{UEVN}}$
5. $UE \rightarrow VN$: $\{RES_{HN}, hash(GUTI)\}_{K_{UEVN}}$
6. $VN \rightarrow HN$: RES_{HN}

4.5 Model Checking

A model of the 6G-AKA protocol has been constructed in the AnB notation and verified with the OFMC model checker [9]. See appendix A for the details.

5 Summary and Conclusion

The presented AKA protocol is an outline of a possible 6G-AKA protocol. It demonstrates the model and the derivation of the GUEI. The GUEI provides an ephemeral identifier for the UE-HN context, analogous to the GUTI for the UE-VN context. The GUEI scheme is a lightweight solution compared to SUCI, and it reduces the use and reliance on the SUCI and/or a PQC SUCI scheme.

Acknowledgments. This research was done for the RAKSHA project, funded by the Research Council of Norway under IKTPLUSS-IKT grant agreement No. 312122.

Disclosure of Interests. The author have no competing interests to declare.

References

1. 3GPP: TS 33.102 - 3G security; Security architecture. Technical Specification 33.102 v19.1.0, 3GPP (07 2025)
2. 3GPP: TS 23.003 - Numbering, addressing and identification. Technical Specification 23.003 v20.0.0, 3GPP (06 2026)
3. 3GPP: TS 33.401 - 3GPP System Architecture Evolution (SAE); Security architecture. Technical Specification 33.401 v19.2.0, 3GPP (01 2026)
4. 3GPP: TS 33.501 - Security architecture and procedures for 5G system. Technical Specification 33.501 v20.2.0, 3GPP (06 2026)
5. Gollmann, D.: Analysing security protocols. In: Formal Aspects of Security. pp. 71–80. Springer (2002)
6. Khan, Q., Purification, S., Chang, S.Y.: Post-quantum key exchange and id encryption analyses for 5g mobile networking. In: NOMS 2025-2025 IEEE Network Operations and Management Symposium. pp. 1–9 (2025)
7. Køien, G.M.:
8. Lowe, G.: A hierarchy of authentication specifications. In: Proceedings 10th Computer Security Foundations Workshop. pp. 31–43. IEEE (1997)
9. Mödersheim, S.: Protocol security verification tutorial. Tutorial, DTU (2 2023)

Appendix A. An AnB model of the 6G-AKA protocol

The devised model is intended to provide a sanity check and not a "proof" as such. Some properties are verified for the given model with the given verification context. Still, the validity of the model must also be assured, and the limitations of the proof context must be taken into account. The motivation for devising the model was mainly to aid the design process, in line with Gollmann's advice [5].

A.1 Model outline

The AnB language supported by OFMC has a few peculiarities, shortcomings and omissions. That is, one cannot realistically expect to express all properties that one might want to verify. The reader is referred to the OFMC Tutorial [9] for details concerning the AnB language.

The HN is a trusted entity, and is therefore modelled as a constant agent. The HN and UE are mutually authenticated (injective agreement) on the response values (RES_{HN},RES_{UE}). The secrecy of the anchor keys (K_{UEVN},K_{UEHN}) is verified, as is the secrecy of the $GUTI$ and the $GUEI$ identifiers.

A.2 Number of sessions

When running a model, the OFMC tool will attempt to run the model for an increasing number of sessions. That is, by default, it is run for an unbound number of sessions, and it will then not terminate unless an attack is found. One therefore must run the model with a bounded number of sessions. For proper checking of the injective agreement property, one must run two (or more) parallel sessions. We have opted for a fairly complete model, with quite a few variables. The problem then is that the state-space increases combinatorially with the number of session. This imposes a practical limit on the number of parallel session that feasibly can be run.

The 6G-AKA protocol model was verified for 2 sessions. The given command:

```
ofmc --numSess 2 6G-AKA.AnB
```

A.3 The verification output

```
Open-Source Fixedpoint Model-Checker version 2024
INPUT:
   6G-AKA.AnB
SUMMARY:
  NO_ATTACK_FOUND
GOAL:
  as specified
DETAILS:
  BOUNDED_NUMBER_OF_SESSIONS
BACKEND:
```

```
  Open-Source Fixedpoint Model-Checker version 2024
STATISTICS:
  TIME 1150656 ms
  parseTime 0 ms
```

A.4 The model

```
Protocol: AKA # 6G-AKA protocol example
# Note:
#   The HN is a trusted entity, hence the constant agent definition.
#   auk()/rak() is used for the pre-shared secrets (AnB notation peculiarity)
#   kdf() is key derivation function, res() is the response function.
#   hash() is a hash function.
#   guei() is generating the GUEI, and GUTI assignment is included.
#   GUEI and GUTI is later used in plaintext.


Types:
    Agent UE,VN,hn;
    Number RANDue,RANDvn,RANDhn,GUTI;
    Function auk,rak,kdf,res,guei,hash


Knowledge:
    UE: UE, VN, hn, auk(UE,hn),kdf, res, guei, hash;
    VN: UE, VN, hn, rak(VN,hn), kdf;
    hn: UE, VN, hn, auk(UE,hn), rak(VN,hn), kdf, res, guei, hash;


Actions:
    UE->VN: RANDue
    VN->hn: RANDue, RANDvn

    hn->VN: res(auk(UE,hn),RANDue,RANDhn,RANDvn),
            RANDhn, {| UE, kdf(kdf(auk(UE,hn),RANDue,RANDhn),RANDvn)|}rak(VN,hn),
            {| VN, kdf(kdf(auk(UE,hn),RANDue,RANDhn),RANDvn)|}auk(UE,hn)

    VN->UE: res(auk(UE,hn),RANDue,RANDhn,RANDvn),
            RANDhn, RANDvn, {| VN, kdf(kdf(auk(UE,hn),RANDue,RANDhn),RANDvn)|}auk(UE,hn),
            {| GUTI |}kdf(kdf(auk(UE,hn),RANDue,RANDhn),RANDvn)

    UE->VN: {| res(auk(UE,hn),RANDhn,RANDue,RANDvn), hash(GUTI) |}
            kdf(kdf(auk(UE,hn),RANDue,RANDhn),RANDvn)
    VN->hn: res(auk(UE,hn),RANDhn,RANDue,RANDvn)

Goals:
    UE authenticates hn on res(auk(UE,hn),RANDue,RANDhn,RANDvn)
    hn authenticates UE on res(auk(UE,hn),RANDhn,RANDue,RANDvn)

    kdf(auk(UE,hn),RANDue,RANDhn) secret between UE,hn                  # Anchor key Kuehn
    kdf(kdf(auk(UE,hn),RANDue,RANDhn),RANDvn) secret between UE,VN,hn   # Anchor key Kuevn
    GUTI secret between UE,VN                                           # The GUTI
    guei(auk(UE,hn),RANDue,RANDhn) secret between UE,hn                 # The GUEI
```

Fig. 1. The 6G-AKA AnB model.