A Subscriber Identity Module for the IMT-2030 System

Geir M. Køien

Department of Microsystems, University of South-Eastern Norway, Norway
E-mail: geir.koien@usn.no

Received 02 September 2025; Accepted 28 January 2026

Abstract

In this paper we argue that the upcoming 6G mobile system should have a new subscriber identity module (SIM). The SIM application used today, the USIM, is functionally the same as the 3G SIM (which dates back to 1999). The SIM holds the subscriber security credentials and algorithms,and these are used during the authentication and key agreement (AKA) procedures. That makes the 4G EPS-AKA and the 5G-AKA protocols, in important ways, restricted by the USIM functionality. This situation should be rectified, and our proposal is for a new 6G-SIM application and a new 6G baseline AKA (6G-BAKA) protocol.

Keywords: IMT-2030, 6G access security, authentication and key agreement, subscriber identity module.

1 Introduction and Background

This paper investigates possible concepts for security improvements to the 6G system architecture. We confine our scope to issues and aspects of subscription credentials hosted on the SIM and the associated AKA protocol.

Journal of Mobile Multimedia, Vol. 22_1, 121–150.
doi: 10.13052/jmm1550-4646.2215

1.1 Design and Development of IMT-2030 (aka 6G)

The International Telecommunication Union (ITU) is a United Nations agency, and it is responsible for a host of information and communication technologies recommendations, etc. The ITU-R arm, which is responsible for radiocommunications aspects, has a "working party" known as WP 5D. This working party is responsible for defining the high-level system aspects (visions) of International Mobile Telecommunications (IMT) systems, comprising the IMT-2000, IMT-Advanced, IMT-2020 and IMT-2030 systems. These IMT visions correspond to 3G, 4G, 5G and 6G respectively. We shall elaborate further on this in Section 3.1.

1.2 State of the SIM

The SIM concept was introduced with 2G/GSM.[1] The GSM SIM contained the subscription identifier, a 128-bit pre-shared secret known as Ki, and two security algorithm interfaces (A3 and A8). The SIM is the user end-point for the GSM-AKA protocol. The basic scheme in GSM-AKA, and subsequent AKA protocols, are a MAC-based challenge–response scheme. The home environment (HE) is the corresponding party. However, GSM was specified during the late 1980s and at that time cryptography was severely restricted through national regulations and laws. The result was that one was only permitted to generate a 64-bit key (K_C).

When 3G was designed and specified, it was clear that 64-bit security was inadequate. This meant that one had to upgrade to a SIM with 128-bit algorithms. The new design featured the UICC (Universal Integrated Circuit Card) and the USIM (UMTS[2] subscription identity module) application. The associated UMTS-AKA protocol could then be based on 128-bit cipher primitives. This worked out very well, even though the cost of switching SIM platform was high.

There never was a new SIM for 4G or 5G. The 128-bit basis of the USIM was deemed adequate and thus the USIM could be retained. One then avoided the overhead involved in switching SIM platform yet again. This had repercussions for so-called long-term evolution (LTE), and in particular it meant that the EPS-AKA protocol would have to be based on the USIM. The names evolved packet system (EPS) and long-term evolution (LTE) are both 4G specific. The 128-bit basis of the USIM was also seen as adequate

[1] Global System for Mobile Communications.
[2] Universal Mobile Telecommunications System.

for 5G, and so the USIM was also retained for 5G. Again, there was a design/functionality cost to this. After all, the new 5G-AKA protocol is still based on the UMTS-AKA protocol machine and its cryptographic basis.

1.3 State of the 3GPP AKA Protocols

As was alluded to in the previous section, the AKA protocols have become more complex with each generation. The GSM-AKA protocol was a very simple challenge–response protocol that only authenticated the SIM and provide a 64-bit session key.

The UMTS-AKA protocol is also a challenge–response protocol, and one now wanted mutual entity authentication. However, the UMTS-AKA protocol inherited the message exchange schematics from its 2G predecessor. This was not inevitable, but rather a convenient way to avoid extra changes (and delays) in the design process.[3] Since the GSM-AKA protocol only provides *unilateral* entity authentication, it was necessary to come up with a scheme to provide *mutual* entity authentication for the same message exchange scheme. The solution was to add an *authentication token* to the challenge, which included an integrity check value to prove that the challenge was issued by the HE.

The UMTS-AKA protocol provides mutual entity authentication, but there are a few problems with this. The two principal entities involved in the UMTS-AKA are the USIM and HE. However, it is the serving network (SN) that initiates the UMTS-AKA protocol sequence, and it may be associated with a separate network from the HE (in which case the subscriber is said to *roam*). The SN handles active subscribers and provide radio access for the subscribers. The SN will therefore request authentication vectors (AV[4]) from the HE, which permits it to conduct the UMTS-AKA protocol on behalf of the HE. Thus, what is achieved is that the HE is authenticated as having produced the AV at some point in time. One may assume that the HE trusted the SN, but since the AV may be forwarded without any security protection, this assumption cannot be substantiated. In summary, this is not satisfactory, and even if there is additional functionality in 4G and 5G to try to remedy this, it is still only a patched-up scheme.

Since the USIM is retained for both 4G and 5G, we then have that the limitations of the UMTS-AKA protocol are present in both 4G and 5G. That

[3]The author participated in the 3GPP security working group (SA3) at the time and recalls the deliberations well.

[4]Which contain the full set of challenge–response data and the derived keys.

is, the EPS-AKA (4G) protocol partially circumvents the limitations and includes some new functionality (e.g. provisioning of a key hierarchy and key binding that include the SN). The 5G-AKA protocol builds on the EPS-AKA protocol, and provides even more SN bindings. However, the improvements adds a significant amount of complexity, and while some of that complexity may be inherent, it cannot be ignored that the design could have been much cleaner had one avoided the UMTS-AKA legacy. We shall return to the 3GPP AKA protocols in Section 2.3.

1.4 Expected Trend for IMT-2030: Terminal Diversity

The official IMT-2030 "future technology trends" report [1] elaborates on many technology aspects. We here choose to highlight section "4.1.2 Diversification of terminals", which (amongst others) state that [1]:

> While smartphones remain, non-portable terminals such as cars, Unmanned Aircraft Systems (UASs), vessels and robots equipped with multisensory integration and intelligent capabilities, are expected to play an increasingly significant role in every field of the future society.

Then we have section 3 "Usage scenarios of IMT-2030" in the IMT-2030 framework recommendation [2]. Figure 1 in this section, the so-called *wheel diagram*, shows the IMT-2030 equivalent of the 5G usage scenario triangle. The *wheel* has six main usage categories, with different characteristics. This is made even clearer in section 4 "Capabilities of IMT-2030". The capabilities are visualized in the so-called *palette diagram* (figure 2 in ITU-R M.2160-0 [2]). The new and enhanced capabilities include[5]:

- Mobility of up to 1000 km/h
- Connection density of up to 10^8 devices/km^2
- Latency in the range 0.1–1.0 ms
- Positioning accuracy in the range 1–10 cm.

There are several noteworthy aspects to the wheel/palette diagrams. One of those is the many quite different characteristics and usages. Thus, it would seem prudent to prepare for terminals with vastly different characteristics.

[5] Enhanced versions of the Wheel- and Palette diagrams can be found on the ITU-R IMT-2030 pages. See https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx.

These terminals will likely also have different needs for security. We return to IMT-2030 and the diagrams in Section 3.

1.5 Related Research and Paper Outline

Related research, standards and reference documents are mentioned, discussed and referenced throughout the paper.

This section provides the background and motivation for the paper. Section 2 provides more information about the SIM applications and the 3GPP AKA protocols. Section 3 provides an overview over the technological trends assumed to be important for IMT-2030 and the IMT-203 framework recommendation. Section 4 outlines some aspects that must be taken into account for a new 6G SIM. Section 5 provides some deliberations on terminal diversity and profiles for access security, which is aligned with the IMT-2030 usage scenarios. Section 6 outlines a possible 6G baseline AKA (6G-BAKA) protocol. The protocol is meant to illustrate the opportunities with new design freedom, and it should not be taken as a concrete proposal per se. Section 7 provides a brief summary and discussion. Finally, Section 8 contains the conclusion.

1.6 Problem Statement

The problem that is investigated in this paper is how to improve on the SIM-basis and the associated AKA protocol(s) for the IMT-2030 systems. That is, to investigate how a 6G SIM could be made without incurring prohibitive logistical complications and costs, and to define the outline of an AKA scheme that clearly improves on the USIM-dependent 5G-AKA and that provides a cost-effective and sound basis for the 6G (with a lifetime assumed to be extending well into the 2040s).

2 State of the SIM and the AKA Protocols

2.1 State of the SIM Platform

The original 2G SIM was removable and independent on the mobile phone/device. It featured an integrated circuit card (ICC) and had a credit card sized form factor (FF). Over the years there have been many form factors (mico-SIM, nano-SIM, etc.), all retaining the "removable" aspect of the SIM. The subscription credentials and the associated cryptographic functions reside on the SIM. The subscription credentials include the permanent

subscriber identifier (the IMSI[6]) and a pre-shared secret, as well as the before mentioned A3 and A8 cryptographic algorithm interfaces.[7] In GSM, the pre-shared secret was the 128-bit key Ki (later only called K). The SIM is the user end-point for the GSM AKA protocol. Correspondingly, the authentication center (AuC) was the 2G home network end-point.

As mentioned, during the late 1980s cryptography was severely restricted through national regulations and laws, and through the COCOM/Wassenaar arrangement for export control.[8] In effect this meant that the "key agreement" part of GSM was limited to 64-bit cryptography. In practice, it was even more restricted since the early COMP128 algorithms only produced 54 bit keys [3].

When 3G was designed, just prior to 2000, it was clear that 64-bit security was inadequate. The restrictions on cryptography was about to be relaxed, and 128-bit end-user cryptography was possible. The 3G access security could therefore by designed with 128-bit cryptography. This meant that one would have to replace the SIM card. The new design would feature a separation of the UICC (physical ICC) and the software-based UMTS subscription identity module (USIM). The associated UMTS-AKA protocol was based on 128-bit cipher primitives and 128-bit keys. The cryptographic functions in the USIM is specified in TS 35.205 and TS 35.206 [4,5]. These specification defines the MILENAGE algorithms set, which provides the cryptographic functions (f1, f1*, f2, f3, f4,f5, f5*) used to execute the UMTS-AKA protocol. MILENAGE is a framework, and has a block cipher at its core (with 128-bit blocks and 128-bit keys). An operator could in principle define its own version of MILENAGE. The suggested block cipher is Rijndael,[9] and there are additional specifications (TS 35.207 [7] and TS 35.208 [8]) that provide Rijndael-based "implementor's test data" and "conformance test data".

There was never a new SIM for 4G. There would have been tangible benefits to upgrade to a 4G SIM, but the costs involved were considered unwarranted. The costs and logistics involved in the procurement and production of a new ICC/SIM and its distribution to a large number of subscribers would have been substantial. However, the USIM was deemed sufficient and it was therefore retained for 4G. That meant the ÈPS-AKA protocol is basically an extension to the UMTS-AKA protocol. Still, one managed to

[6] IMSI: International Mobile Subscriber Identity.

[7] A3 defines the *response* function and A8 the *key derivation* function, commonly realized by the COMP128 family of algorithm.

[8] See the "Origins" tab in www.wassenaar.org/about-us/ for more information.

[9] Rijndael was chosen as the MILENAGE core primitive *before* Rijndael was selected as the Advanced Encryption Standard (AES) algorithm [6] in 2001.

improve on the UMTS-AKA protocol and it was possible to move away from a design using session keys (CK and IK) to a design using key-deriving keys and an associated key hierarchy. Since the USIM is effectively oblivious to the 4G enhancements, the key hierarchy had to be derived at the mobile equipment (ME). The 4G key-deriving key (anchor key) is called K_{ASME} and it was derived with $CK||IK$ as the input key.[10] We note that ME is the entity that will use the keys in the key hierarchy.

The 128-bit basis of the USIM was also seen as adequate for 5G, and so the USIM was retained for 5G too. The 5G-AKA protocol is still based on using a USIM and the basic UMTS-AKA protocol scheme, but it has been further refined and enhanced. The 5G key hierarchy had to be derived by the mobile device and none of the extensions/improvements involve the USIM. So, the 5G-AKA protocol is still restricted by the inherited USIM dependency.

However, while the derivation of the key hierarchy can safely be left to the ME, the UMTS-AKA protocol machinery shortcomings have become more evident over time. It is hard, cumbersome and complex to fix this while still being confined by the USIM functionality. For the 4G-AKA protocol one had modestly complex additions to UMTS-AKA, but the 5G-AKA protocol is significantly more complex than the UMTS-AKA. The added security functionality is useful, but the USIM platform (from 1999) is not a good basis for subscriber security for the IMT-2030 systems (which will have a lifetime that will extend well into 2040).

Finally, when it comes to the state of the SIM platform, it is worth noting that there has been developments to make the SIM downloadable. We elaborate on this in the upcoming section.

2.2 Downloadable SIM

2.2.1 Form factors and the eUICC

Support for Internet-of-Things (IoT) and machine-to-machine (m2m) communications has gradually been improved in 3GPP-based systems. Amongst the developments has been the changes to the SIM and UICC ecosystem. It started out with a need to make IoT devices withstand tough environmental exposure (temperature/humidity, etc.). Furthermore, many of these devices (sensors, etc.) would be unattended for almost all of their lifetime, and this meant that there was a need to solder the ICC to the mobile device (to

[10]The "||" symbol denotes concatenation. This notation is also used in the 3GPP standards.

avoid unreliable physical connections). This was specified by the European Telecommunications Standards Institute (ETSI). The "MFF" form factors are now dedicated to soldered versions of the UICC. This kind of UICC, which is "embedded", is called eUICC. See the ETSI specifications [9,10] for more on the smart card interfaces, form factors and the associated characteristics. The soldered UICC introduced a bit of dilemma in that the device would now be locked to USIM(s) preloaded on the eUICC. The problem might be mitigated by preloading several different USIMs, but even this is somewhat inflexible. Thus was born the need for a downloadable USIM.

2.2.2 Remote SIM provisioning (RSP)

The downloadable SIM concept is defined and specified by the GSM Association (GSMA) in its "SIM Group Permanent (SGP)" activities. The new type of SIM is known as an eSIM. We have different versions and associated "remote SIM provisioning architecture" definitions. These cater to the "consumer" and "IoT" segments, and differ largely by the fact that the IoT version necessarily needs to be fully automated. The consumer version includes user interactions to approve the downloading/activation of the new SIM. See [11, 12] for the general outline, but note that there are several other relevant GSM SGP specifications.

2.2.3 The eSIM and the iSIM

While the eUICC/eSIM provides for a downloadable USIM concept, it was noted that it seemed unnecessary and redundant to have a separate ICC for providing a SIM platform. A dedicated system-on-a-chip (SoC) would be cheaper and would require less energy to run, something which is very desirable for resource constrained devices that must run on batteries for years on end. The most recent GSMA SGP standards therefore defines a tamper resistant element (TRE) and an "integrated" SIM (iSIM). The remote SIM provisioning procedures and the required security assurance is similar for eSIM/eUICC and iSIM/TRE.

2.2.4 Predictions and implications

We shall not go further into these standards and protocols, but we note that eSIM/iSIM based solutions are poised to become the preferred solution for future subscriber provisioning.[11] This implies that the cost associated with changing the SIM application is now substantially reduced. The roll-out could

[11] Strong growth is expected towards 2030. See https://www.counterpointresearch.com/en/insights/over-9-billion-esim-capable-devices-to-be-shipped-by-2030.

be by means of the remote SIM provisioning infrastructure. The eUICC (MFF2) may be somewhat inflexible with respect to supporting new cipher algorithms, but this should not be the case for the TRE. It is also noted that new MFFs may be devised should the need arise.[12] Thus, for IMT-2030 one will essentially be free to update the SIM application to a new native 6G version, without incurring the platform switching costs.

2.3 State of the AKA Protocols

As mentioned earlier, the AKA protocols have become more complex with each generation. This wasn't much of an issue with the GSM-AKA and UMTS-AKA protocols. The UMTS-AKA protocol is a challenge–response protocol, built upon the message exchange defined for the GSM-AKA protocol. That is, UMTS-AKA has an (extended) authenticated challenge. This provides mutual entity authentication, but there are a few problems with this. One of these is that there are really three parties. For instance, the UMTS-AKA protocol doesn't include the SN in the cryptographic binding of the protocol, yet it is the SN that actually initiates the protocol towards the ME/USIM.

We mentioned the AV was forwarded from the HE to the SN. The HE–SN communications may in principle be authenticated and protected, but this is only an option. Thus, in effect, there are no assurances for AV forwarding. The HE and the SN may belong to the same public land mobile network (PLMN), but this is not a given. Thus, AV forwarding may be without protection. The SN is furthermore permitted to request multiple AVs from the HE and then to store them for future use. We then have a situation where the HE may be offline during a challenge–response exchange. Thus, the only thing that is authenticated is that the HE produced the AV at some point in time, and that it forwarded it to the SN. This is not satisfactory. Both the EPS-AKA/5G-AKA protocols contains additional security functionality, but they cannot easily extend beyond the limitations imposed by the UMTS-AKA protocol designs.

Another issue to be noted is that the CK and IK keys (from UMTS-AKA) are really derived from the basis of a single 128-bit secret (called K). One then derives 256-bit anchor keys (K_{ASME} in 4G and K_{AUSF} in 5G) from this. This isn't the best of designs. It really would have benefited from a true 256-bit basis.[13] It is noted that there is a 256-bit version of MILENAGE

[12] We not referring to physical dimensions, etc., but to the ability to support a new 6G SIM.

[13] In 5G, the K *may* be 256-bit, but the "UMTS-AKA" part is still 128-bit.

and an alternative framework based on the KECCAK cryptographic hash function available. These are both 256-bit frameworks (depending on a 256-bit K).

The 5G system also includes functionality for a "subscription concealed identifier (SUCI)", which provides subscriber identity privacy. That is, the "subscriber permanent identifier (SUPI)" can be concealed from third-parties (providing external identity privacy).[14] The *identify presentation* procedure is logically a part of the AKA protocols, but they are not integrated in the 3GPP systems. This is, in some ways, a missed opportunity, as the SUCI identify presentation, which entails using an "elliptic curve integrated encryption scheme (ECIES)", could have been integrated with the 5G-AKA protocol. This opportunity was explored by the author in [13]. The system could then even have benefited from the elliptic curve Diffie–Hellman (ECDH) secret derived during the ECIES part (this would have allowed *forward secrecy* since the scheme involves ephemeral ECDH keys).

The UMTS-AKA protocol is defined in TS 33.101 [14] and the EPS-AKA protocol is defined in TS 33.401 [15]. For more information about the 5G-AKA protocol and the SUCI scheme, the reader is advised to consult TS 33.501 [16] (which is the main security specification for 5G).

3 The Big Picture (IMT-2030 and Beyond)

3.1 The IMT-2030 Framework and 6G System Architecture

The IMT-2030 framework and vision for what 6G is supposed to be is captured in the ITU-R recommendation "Framework and overall objectives of the future development of IMT for 2030 and beyond" [2]. Additionally, we have a report on "Future technology trends..." for IMT-2030 [1] and a feasibility report on radio technologies.[15] Apart from these, there are no other authoritative inputs on IMT-2030. There are some security-related papers published, but it is early days with respect to 6G. Some of these papers were mentioned in Section 1.5.

The recommendation for "IMT for 2030 and beyond" [2] provides the high-level vision and framework for 6G. The ITU does not specify the actual 6G design. Instead, the vision is input to the 3GPP, which defines the technical specifications (TSs) that define the actual systems. In this case, the IMT-2030 vision corresponds to 6G, which in the 3GPP release oriented

[14]The SUPI is a generic term, and it may in fact be an IMSI (there are other options).

[15]Not applicable to this paper.

scheme, starts off as Release 21. That is, there will be extensive studies carried out during Release 20 as well. The 3GPP[16] is an organization that develops technical reports and specification. Formally, it isn't a standards body, but for most cases the TSs tend to be ratified as-is. The TSs are provided with version numbers and are organized in *releases*.[17] When one investigates the 3GPP releases, one will notice that the releases form an evolution of the overall system. For a new generation, there will usually be major changes to the architecture, but there also tend to be major concessions to backwards compatibility aspects, etc. Formally, Release 20 will be designated as "5G Advanced" (with study items concerning 6G) and Release 21 will be a 6G release. From the 3GPP Releases information, we have that:

> On this occasion, the target date for "Technology proposals for IMT-2030" has been defined by ITU to be early 2029, and resulting specifications (i.e. full system definition) are to be submitted by mid-2030 at the latest.

3.2 Future Technology Trends

The ITU-R Report M.2516-0 on the future technology trends [1] provides important insights into the technology trends assumed to be the basis for 6G.

3.2.1 New services and application trends

The M.2516-0 report highlight the following *key drivers* (section 4.2).

- Energy efficiency
- Data rate, latency and jitter
- Sensing resolution and accuracy
- Connection density
- Coverage and full connectivity
- Mobility
- Spectrum utilization
- Simplified user-centric network
- Native artificial intelligence (AI)
- **Security/trustworthiness**
- Dynamically controllable radio environment.

All these drivers are posed to influence the IMT-2030 system design. For our purpose, we shall only investigate the *security/trustworthiness* driver.

[16] See https://www.3gpp.org/about-us

[17] See https://www.3gpp.org/specifications-technologies/releases

Concerning security, it is noted that the designs need to be future-proof, which here largely means that the cryptography needs to quantum-safe. That is, one must assume the presence of so-called cryptographically relevant quantum computers (CRQCs), and design the security with this in mind. We note that AI/ML will be integrated in almost all aspects of the system.

3.3 The Wheel and Palette Diagrams Implications

The wheel and palette diagrams from the IMT-2030 framework [2] illustrates high-level objectives for the system. Given the broad and very ambitious scope, we do not expect all capabilities to be universally available.

3.3.1 The wheel diagram

The wheel diagram provides high-level usage scenarios for IMT-2030. The depicted version of the Wheel diagram, Figure 1, is from the ITU-R webpage entitled "IMT towards 2030 and beyond (IMT-2030)".[18] It is an adapted version of figure 1 in [2] (the IMT-2030 vision/framework recommendation).

Three of the usage scenarios extend the existing IMT-2020 goals:

- Immersive communications
- Massive communications
- Hyper reliable and low-latency communications (HRLLC).

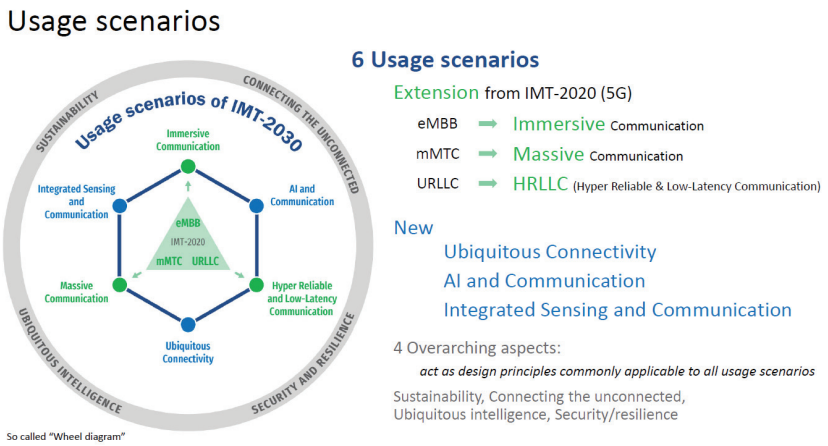

Figure 1 The "wheel diagram."

[18] itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx

The wheel also introduces three new usage scenarios:

- AI and communications
- Integrated sensing and communications (ISAC)
- Ubiquitous connectivity.

3.3.2 The palette diagram

The palette diagram, Figure 2, provides fairly concrete high-level goals for the performance of the system. We will not go into all the details, but the capabilities include:

- *User experience data rate* of 300–500 Mbit/s (or more)
- *Area traffic capacity* of 30–50 Mbit/s/m^2 (or more)
- *Connection density* goals for up to 10^8 devices/km^2.
- *Mobility*, with defined QoS and seamless handover, of 500–1000 km/h.
- *Latency* of 0.1–1 ms (over the air interface)
- *Positioning* with accuracy of 1–10 cm.

The goals are not necessarily going to be reflected in real networks. Rather, they are *design* goals, and many of the goals are additionally stated

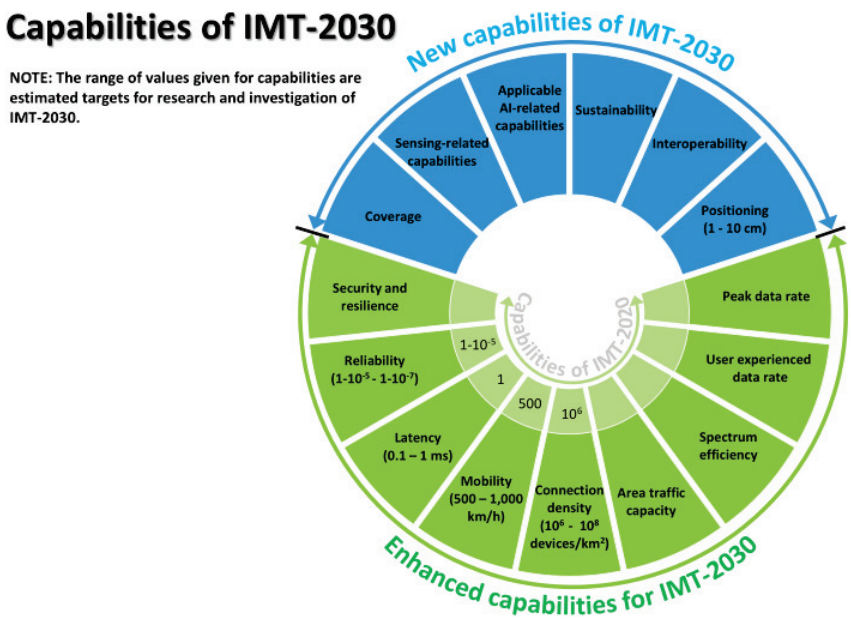

Figure 2 The "palette diagram"; Figure 2 in [2].

as research goals. Then there is the issue of implementing the design, producing the equipment, etc., and deploying and using the system. Thus, many of the capabilities will probably only be offered locally and probably not until the mid/late 2030s. However, one must design the system architecture and the security architecture for the whole range of usage scenarios and capabilities as captured and visualized in the Wheel- and Palette diagrams. That implies that the access security must cater to a diverse range of goals and capabilities. This would be reflected in networks and terminals that needs to cater to multiple radio access technologies, specialized antennas, greatly varying computing resource requirements, etc. Some terminal types will likely be integrated in critical infrastructures, some will be used in industrial automation and in autonomous operations of various sorts.

4 A New 6G SIM

4.1 Remote SIM Provisioning

A basic premise for the new SIM concept and the associated AKA protocol((s) is that the SIM is now downloadable. That is, the eSIM/iSIM is downloadable, and it seems highly likely that most SIMs issued will be downloadable. Given this, we assume that SIMs issued specifically for IMT-2030 will predominantly be downloadable.

4.2 New Threats

The downloable SIM concept is already established, so these are not really new threats. Weaknesses and vulnerabilities in the hardware/firmware of the eUICC/TRE will potentially be devastating. One should also be aware of configuration and policy aspects, which may lead to unwanted behaviours.

Then there is the remote SIM provisioning mechanism and infrastructure. There could be serious weaknesses/vulnerabilities in the transfer protocol and/or the associated infrastructure, and this would potentially be debilitating. There could be flaws in the design, error in the implementation or misconfigurations, etc.

There is nothing new here, since these infrastructures already exist, but we note that a successful attack could potentially scale to disastrous levels. That is, should an intruder succeed in compromising the RSP infrastructure, they will be able to deploy compromised SIMs and at a very high rate.

Additionally, one cannot entirely ignore the fact that many operational procedures (distribution and management at large) were devised with a physical UICC in mind. Thus, a physical UICC may be an unstated premise in threat/risk evaluations, and this may lead to unforeseen risks. The paper "Analysis of eSIM/iSIM for Critical Communications" [17] investigates these aspects for critical communications, but the threats are not specific to critical communications.

4.3 Backwards Compatibility Aspects

Backwards compatibility is a thorny issue for security schemes. Usually, one provides mapping functionality between the security credentials/contexts such that one may use the AKA protocol of generation $N-1$ in a generation N network (and visa versa). For our purposes, we suggest that the USIM, when necessary, may be permitted to co-exist with a 6G SIM. Then, using the 6G SIM would be the preferred solution, with the USIM serving as a backup for compatibility reasons. Of course, for native 6G devices attaching to pure 6G networks, the only permitted solution must be using the 6G SIM.

5 Profiles and Policies

The 6G Basic AKA protocol must include support for profiles, extension and policy requirements. These should not affect the authentication part per se, but would be instructions for how to handle the key hierarchy, etc. The profiles and policies should have explicit identifers and version specifier.

5.1 Terminal Diversity and Associated Requirements

We have made the case that 6G will have considerable terminal diversity. There could be different security requirements for different terminal types. The following is only meant to illustrate the concept, and is not meant to be taken as a proposal.

5.1.1 Policy options

The policy options may include aspects such as:

- Identity privacy requirement: To use SUCI or SUPI and the frequency of the GUTI assignment.
- Security level
  - (Strong, normal, lightweight)

  - Key-length policy
  - Algorithm choice
  - Security context lifetime
  - Key renewal policy.
- Backwards compatibility restriction (if any)
- Geo-locked functionality
- User data policy.

5.2 A Baseline Profile

The baseline profile would encompass cases covered by the ubiquitous connectivity usage scenario as well as parts of the immersive communications usage scenario. Other non-critical parts of HRLLC may be covered too. This profile will largely adopt default algorithm choices, etc.

5.3 The IoT/m2m Security Profile (Massive Communications)

The National Institute of Standards and Technology (NIST) has recently standardized the ASCON algorithms, directly tailored for use with IoT/m2m devices. Known as the Ascon-Based Lightweight Cryptography Standards for Constrained Devices (NIST Special Publication 800-232 [18]), the standard contains a set of cryptographic functions well suited for IoT/m2m devices and even for RFID tags and medical implants.

In particular, we note that NIST SP 800-232 supports a lightweight Ascon-based authenticated encryption mode-of-operation. Other lightweight functions also exists, and could be included in an IoT/m2m profile.

5.4 A Hyper-reliable (High-performance) Profile

There may be a need for a hyper-reliable/high-performance profile. It would be suitable for real-time industrial control systems (ICS), for autonomous operations (drones, robotics control), etc.

This would encompass much of the IMT-2030 ISAC, HRLLC and immersive communications usage scenarios. Amongst the possibilities for this profile would be (if deemed necessary) to have a high-performance TRE to permit fast response times even for computationally expensive primitives.

6 Design of the Baseline AKA Protocol

In this section we define a 6G baseline AKA (6G-BAKA) protocol.

6.1 Background and Related Research

There already exist a few papers that explore various aspects of access security for 6G. Some of these pre-date the ITU-R report on technology trends [1] (late 2022) and the ITU-R "IMT-2030 and Beyond" framework recommendation [2]. Amongst these we find [19–22]. These papers are early works. That notwithstanding, they also contain insights worth keeping in mind.

There are also newer publications and those that focus on "post-quantum cryptography" (PQC) [23, 24]. For our purpose, we shall not dive into the specifics of the cryptographic primitives. Therefore, we here avoid requiring specific primitives or specific details concerning the primitives. Having said that, the IMT-2030 requires the design to be quantum-safe. The 5G access security algorithms, MILENAGE included, are based on symmetric-key primitives and hash/MAC functions. These are generally not thought to be vulnerable given a large enough key. The exception for 5G is the SUCI/ECIES mechanism, which is not quantum-safe. A broken SUCI/ECIES scheme would amount to subscriber identity privacy being lost.

The author has contributed with a "concept proposal" [25]. This paper contains an analysis of the shortcomings and omissions of the 5G-AKA protocols and a set of lessons learned. Furthermore, it contains a proposal for a 6G "authentication and context establishment" (ACE) protocol. The proposal was a high-level outline and a quantum-safe design that focused on context establishment, anchor keys and inclusion of all principals. Another background document that is useful is the NIST whitepaper on "crypto agility" [26]. The whitepaper contains many considerations for security protocol designs concerning use of cryptography.

6.2 Post-quantum Cryptographic (PQC)

There is debate about how close one really is to a cryptographically relevant quantum computer (CRQC). There is a lot of hype, and there certainly are many actors that are heavily invested in the "quantum race". Then there are those that point out that the "quantum supremacy" hype is being oversold [27]. We also have a publication that highlights the risk a CRQC will be to cryptography [28].

Finally, while this paper is not primarily concerned with quantum threats, PQC or CRQCs, we would like to point out that the telecom sector is not particularly vulnerable to the quantum threats. As shown in the short McKinsey digital report "When – and how – to prepare for post-quentum

cryptography" [29], the telecom industry generally has a fairly short "system life cycle" and short "data shelf life".

Whatever may be the case, there is no doubt that the 6G systems should, to a practical extent, have quantum-safe designs. That is, one may not necessarily deploy PQC compliant algorithms, but the system architecture should be designed to easily accommodate PQC algorithms. The good news is that such algorithms are being standardized[19] and being deployed. In particular, the module-lattice key-encapsulation-mechanism (ML-KEM) [30], is being extensively used by web browsers and internet infrastructures.[20]

A fully functional CRQC would be very problematic for the classical asymmetric algorithms. For symmetric cryptography and for cryptographic hash functions, it appears that extending the key length (and/or hash output length) will suffice. This should in principle be trivial to accommodate, but the specifications must include requirements for this, both for the input to the algorithms and for key distribution/key agreement schemes.

6.3 Identity Privacy

We advocate retaining the 5G subscription concealed identifier (SUCI) scheme. That is, the SUCI scheme may be adapted to be a better fit with our 6G-BAKA protocol.

The 5G SUCI/ECIES scheme is not quantum-safe. It should be an objective to define a quantum-safe SUCI-scheme for the IMT-2030 systems, but one should not rush the design. Thus, a quantum-safe SUCI-scheme may not initially be available for a 6G system. In any case, the design of a PQC SUCI-scheme is considered outside the scope of this paper.

6.4 Perfect Forward Secrecy (PFS)

The 6G-BAKA design does not have the PFS property. This could have been achieved if one had used the Diffie–Hellman secret (dhs) from the SUCI/ECIES scheme and included it in the derivations. Given that SUCI/ECIES is not quantum-safe, we have chosen not to embed the dhs into the 6G-BAKA protocol.

---

[19]The US National Institute of Standards and Technology (NIST) is standardizing PQC algorithms. This is an ongoing process. See more information at https://csrc.nist.gov/projects/post-quantum-cryptography.

[20]For instance, Google have implemented and deployed ML-KEM in Chrome/Chromium and its infrastructures. See: https://blog.chromium.org/2024/05/advancing-our-amazing-bet-on-asymmetric.html

6.5 Naming Scheme and Definitions

6.5.1 Principal entities

We have three principal entities.

- **U**: The user, represented by the 6G SIM.
- **V**: The VPLMN (or serving network of the HPLMN).
- **H**: The HPLMN.

Note that **V** may in fact be a serving network/radio network belonging to the home environment. Whether **V** belongs to a separate domain or to the home environment has historically not been important, and the AKA protocols do not really distinguish between those cases.

6.5.2 Identifiers

The respective identifiers are denoted as uid, vid and hid respectively. The uid may be a $GUTI$, $SUPI$ or a $SUCI$, depending on the requirements (these are identifiers defined for 5G).

- $GUTI$: The globally unique temporary identifier.
- $SUPI$: The subscription permanent identifier.
- $SUCI$: The subscription concealed identifier.

A successful 6G-BAKA run will result in the VPLMN assigning a new $GUTI$ to the user. The $GUTI$ is spatio-temporally restricted. If the user has a valid $GUTI$, then identification with $GUTI$ is required. To use $SUPI$ in cleartext means to lose identity and location privacy. Devices that are associated[21] with a person should therefore never identify themselves with $SUPI$ in cleartext. That is, they should either identify themselves with a $GUTI$ or a $SUCI$ identifier. Note that the $SUPI$ and $SUCI$ contain information to deduce the hid (HPLMN identifier).

6.5.3 Long-term security contexts

The following long-term security context must exist prior to running the 6G-BAKA protocol.

- **(H,U)**: This is the subscription based context.
- **(H,V)**: This is the roaming agreement based context.

The most common case is likely when the user attaches to a serving network run by the HPLMN, and then only the **(H,U)** context applies.

[21] That is, can be *linked* to a person.

6.6 Cryptographic Algorithms and Requirements

The 6G-BAKA protocol itself will only use symmetric-key cipher primitives. These are generally believed to be quantum-safe provided a long enough key. To be quantum-safe would then mean to use 256-bit keys.

6.6.1 Symmetric key encryption/decryption

We require that the functions can operate on 128-bit and 256-bit keys. Furthermore, we require that an "authenticated encryption with associated data" (AEAD) mode-of-operation is used. This is in line with requirements for TLS 1.3 (Section 5.2 in [31]), and affords us both confidentiality and integrity protection. The ad field will have integrity protection only. The ad is not necessarily transferred in the message, but may be extracted from the context. The ciphertext, c, includes the integrity check value (tag).

$AE_K(m, ad) \rightarrow c$
$AD_K(c, ad) \rightarrow m.$

6.6.2 Key derivation function

We require that the function can generate both 128-bit and 256-bit keys. The controlling (input) key, K, is required to be 256-bit wide. In our case, the $kdf()$ will include a function code (fc) to indicate the key type, as is the case for key hierarchy derivation in 4G and 5G.

$kdf_K(fc||parameters) \rightarrow key$

6.6.3 Pseudo-random function

We require that the function can generate both 128-bit and 256-bit pseudo-random output (nonces).

$prf(\cdot) \rightarrow nonce.$

6.6.4 Channels

There are two types of channel.

$\rightarrow$ denotes an unprotected channel.
$\Rightarrow$ denotes a fully protected channel.

Communications between H and V should be fully protected (mutually authenticated and AEAD encrypted). The HV-channel is not associated with any specific subscriber per se. The communications between U and V, which can include radio access, is through a dedicated logical channel. This channel

is initially not protected. Subsequent to running the 6G-BAKA protocol and setting up appropriate security contexts, the UV-channel will be protected according to the stated policy requirements.

6.6.5 BAKA policy descriptor

The 6G-BAKA policy descriptor (pd) is a field that describes the usage policy, cryptographic requirements, etc. It is suggested that the descriptor be encoded in similar ways as the UTF-8 encoding [32]. That is, the encoding starts with one byte, but extends to multi-byte encoding should the need arise. To simplify matters, it may be useful to express common property sets as "profiles". For the purpose of this paper, we merely state that one needs a policy descriptor to be included in the protocol.

6.7 An Alice-Bob Outline of the BAKA Protocol

In 5G and before, one separated the user identity presentation from the AKA protocol. The 6G-BAKA protocol shall include identity presentation and an authenticated challenge.

6.7.1 Pre-existing knowledge

We have that:

- U **knows/has:**
  - Subscription contract with H
  - K: authentication key, pre-shared with H
  - pd_{uh}: policy descriptor
  - Credentials associated with the SUPI/SUCI transform
  - Knowledge of its own subscription identifier ($SUPI$)
  - Knowledge of the permanent HPLMN identifier (hid).
- V **knows/has:**
  - Roaming agreement with H
  - Secured channel with H
  - Knowledge of H and V identifiers (hid, vid).
- H **knows/has:**
  - Subscription contract with U
  - K: authentication key, pre-shared with U
  - Credentials associated with the SUPI/SUCI transform
  - Knowledge of subscription identifier(s) ($SUPI$)

- Roaming agreement with V
- Secured channel with V
- Knowledge of H and V identifiers (hid, vid).

6.7.2 Notation and information elements

We have that:

- $rand_n$: denotes a nonce from entity n
- $randset$: $(rand_u, rand_v, rand_h)$
- pd_n: policy descriptor. n is uh or uv.
- $block$: denotes an AEAD encrypted block (including the tag).
- ad: additional/associated data.
- uid: user/subscription identifier (SUPI, SUCI or GUTI)
- hid: public HPLMN identifier
- vid: public VPLMN identifier
- $idset$: $(SUPI, hid, vid)$.

The VPLMN will need to be informed of the hid in the first message. For $SUCI$, the hid is embedded in the scheme. $SUPI$ directly includes the HPLMN identification, and $GUTI$ will have been established during a prior 6G-BAKA run (with HPLMN identification in place). We let "[]" enclose *SUPI*, to indicate that it is only included when necessary (i.e. when the *uid* was *SUCI*). AEAD encrypted contents is indicated with $\{|...|\}_K$. The ad is not transferred and hence not depicted as encrypted. The order of the elements in the messages and functions is significant.

6.7.3 Main design outline

The 6G-BAKA protocol has multiple goals. The primary goal is to mutually authenticate the U and H entities. This is achieve by a dual challenge-response scheme, which uses AEAD as its main cryptographic primitive. The ad may then serve as the authenticated response. Both U and V supply fresh nonces to this exchange.

While the authentication is between U and H, the scope encompasses V as well. That is, V is included in the derived security context. This also establishes the main operational security contexts UV and UH.

- UV: The home-user primary security context.
- UH: The visited-user roaming security context.

The secondary goal is to derive two anchor keys (for the main operational security contexts). This is achieved by using the nonces supplies by U and H,

and a nonce supplied by V. Thus, the derived anchor keys are dependent on all three nonces.

6.7.4 The basic AKA protocol (Alice–Bob like notation)

Protocol outline:

1. U→V: M1($uid, ChallengeUH$)
2. V⇒H: M2($(uid, ChallengeUH, rand_v$)
3. H⇒V: M3($[SUPI], K_{uv}, ResponseUH$)
4. V→U: M4($AssignGUTI, ResponseUH$)
5. U→V: M5($ConfirmGUTI, ResponseHU$)
6. V→U: M5u($ConfirmPD$)
7. V⇒H: M5h($ResponseHU$)

Action before message M1:

U: $prf(\cdot) \rightarrow rand_u$
U: Encrypt $ChallengeUH$

- $ad := idset$
- $AE_K(rand_u, pd_{uh}, ad) \rightarrow ChallengeUH.$

The inclusion of the $idset$ in ad authenticates the $idset$ to H.

Action before message M2:

V: $prf(\cdot) \rightarrow rand_v$
V: if received uid was $GUTI$, then let uid be $SUPI$ toward H.

Action before message M3:

H: If uid was SUCI, then de-conceal uid and fetch relevant credentials
H: $prf(\cdot) \rightarrow rand_h$
H: Decrypt $ChallengUH$

- $ad := idset$
- $AD_K(challengeUH, ad) \rightarrow rand_u, pd_{uh}$
- This verifies the authenticity of the ad and encrypted contents

H: Minor modifications may be made to pd_{uh}
H: $kdf_K(rand_u, rand_v, rand_h) \rightarrow K_{uv}$; (anchor key for UV-context)
H: $kdf_K(rand_u, rand_h, rand_v) \rightarrow K_{uh}$; (anchor key for UH-context)
H: Encrypt $ResponseUH$

- $ad := rand_u, idset$
- $AE_K(rand_h, rand_v, pd_{uh}, ad) \rightarrow ResponseUH.$

When H decrypts $ChallengeUH$, it will have the assurance of the challenge and the $idset$. The key derivations include a function code, fc (not depicted), and it may include the $idset$. The $ResponseUH$ element include the challenge from H towards U. The authenticity of the $ResponseUH$ element, which includes ad, is in effect the response from H.

Action before message M4:

V: Assign SUPI to context (if necessary) and construct $GUTI$
V: Accept K_{uv} as anchor key for UV-context
V: Encrypt $AssignGUTI$

- $ad := idset$
- $AE_{K_{uv}}(GUTI, ad) \rightarrow AssignGUTI$.

Action before message M5:

U: Decrypt $ResponseUH$

- $ad := rand_u, idset$
- $AD_K(ResponseUH, ad) \rightarrow rand_h, rand_v, pd_{uh}$
- The authenticity of $ResponseUH$ is the response from H

U: $kdf_K(rand_u, rand_v, rand_h) \rightarrow K_{uv}$; (anchor key for UV-context)
U: $kdf_K(rand_h, rand_h, rand_v) \rightarrow K_{uh}$; (anchor key for UH-context)
U: Decrypt $AssignGUTI$

- $ad = idset$
- $AD_{K_{uv}}(AssignGUTI, ad) \rightarrow GUTI$
- Assign $GUTI$ to **(UV)** context

U: Encrypt $ResponseHU$

- $ad = rand_h, rand_u$
- No data, only integrity/authenticity
- $AE_K(ad) \rightarrow ResponseHU$

U: Encrypt $ConfirmGUTI$

- $ad := GUTI$
- Confirm $GUTI$ and submit pd_{uv}
- $EA_{K_{uv}}(pd_{uv}, ad) \rightarrow ConfirmGUTI$.

Action before message M5u):

V: Decrypt $ConfirmGUTI$

- $ad := GUTI$

- $DA_{K_{uv}}(ConfirmGUTI) \rightarrow pd_{uv}$
- Inspect pd_{uv}, possibly modify it

V: Encrypt $ContextActivation$

- ad is empty.
- $AE_{K_{uv}}(pd_{uv}, ad) \rightarrow ContextActivation.$

Action after receiving message M5h):

H: Decrypt $ResponseHU$

- $ad := rand_h, rand_u$
- $DA_K(ResponseHU, ad) \rightarrow null.$

The authenticity of ad completes the mutual authentication of U and H.

6.8 Local Rekeying and GUTI Assignment

The local UV security context is initialized during a successful 6G-BAKA run. The context includes the K_{uv} anchor key, which will be used when the local (UV) key hierarchy is generated.

1. `U` $\Rightarrow$ `V: NewKeys(`$tvp, params$`)`
2. `V` $\Rightarrow$ `U: NewGuti(`$GUTI$`).`

The time-variant parameter (tvp) may be a pseudo-random number (nonce), a time-stamp, a serial number or a combination of these.

Today, there is rekeying for handover events. With this in mind, it may also be beneficial to let $param$ include the global cell-id or similar data to have a spatial binding to the derived key hierarchy.

$kdf_{K_{uv}}(tvp, param) \rightarrow [keyhierachy...]$

The `NewKey()` message should be protected with the K_{uv} key. The `NewGuti()` message should be protected with a newly created session key.

7 Summary and Discussion

In the present paper we have made the case for a new native 6G SIM application. It may be realized on a new 6G compatible ICC or on a 6G compatible TRE. In fact, we assume that a 6G SIM will be downloadable and delivered by the remote SIM provisioning scheme.

A new 6G SIM will no longer be restricted by the USIM design choices, and so a 6G-BAKA protocol can be design without these constraints. We

have proposed the 6G-BAKA protocol, although this is more an example than proposal. Thus we will not analyse the 6G-BAKA protocol further here.

7.1 Must There Be a New SIM?

We have implicitly, throughout the paper, made the assumption that there must be a SIM for 6G. Well, there must be some way of identifying the subscriptions. There must also entity authentication and key establishment to support protected communications.

However, this *may* be realized in other ways than devising yet another SIM. The most important part, from a practical point of view, is probably to retain the SUPI as the identifier. Then, one may for instance use digital certificates. This comes with its own requirements for infrastructure, etc., but it is clearly doable. Of course, one must then require that the certificates and the verification methods be quantum-safe.

At present, it seems that a new SIM scheme imposes few changes on the overall architecture, and the symmetric-key approach used is known to be quantum safe. We therefore argue that a new SIM should be seen as the default choice for the IMT-2030/6G systems.

7.2 Must There Be an AKA Protocol for 6G?

A new AKA protocol seems a reasonable design choice. Of course, it may be a new 6G-AKA based on the USIM and extensions to the 5G-AKA protocol. Nevertheless, a new AKA protocol seems a very likely design choice.

8 Conclusion

The currently used subscriber identity module used in 3GPP-based mobile systems, the USIM, dates back from 2000 and the 3G/UMTS system. It's not a bad basis per se, but it does impose restrictions on the authentication and key agrement protocols. Previously, the cost of switching the SIM was associated in a large part with the procurement cost and logistics introduced in switching the physical secure element (the smart card, UICC). With the advent of the remote SIM provisioning concept, and its increasing popularity as a deployment platform, the importance of the UICC is diminishing, and by 2030 it will be largely replaced in many markets and usage niches. The new physical platform will likely be the TRE, implemented as an enclave on the

main processor, but a new "eUICC" that supports a 6G SIM would also be acceptable. Devices that are 6G capable should not have any problems with these requirements.

A new 6G native SIM can therefore be introduced without prohibitive costs concerning the deployment platform. This will enable new freedom in designing a 6G-BAKA protocol. We have made a concrete suggestion for a 6G-BAKA protocol, and while the extensibility is useful and necessary for fulfilling the IMT-2030 vision [2], the 6G-BAKA protocol itself is merely an illustration of the possibilities.

References

[1] ITU-R. Future technology trends of terrestrial International Mobile Telecommunications systems towards 2030 and beyond. Report M.2516-0, ITU, 11 2022.

[2] ITU-R. Framework and overall objectives of the future development of IMT for 2030 and beyond. Recommendation M.2160-0, ITU, 11 2023.

[3] GSMA. Security Algorithm Deployment Guidance. Permanent Reference Document FS.35 v3.0, GSMA, 04 2022.

[4] 3GPP. TS 33.205 - Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General. Technical Specification 35.205 v19.0.0, 3GPP, 03 2025.

[5] 3GPP. TS 33.206 - Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification. Technical Specification 35.206 v18.0.0, 3GPP, 03 2024.

[6] NIST. Advanced Encryption Standard (AES). Federal Information Processing Standards Publication FIPS 197, NIST, 05 2023.

[7] 3GPP. TS 33.207 - Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' test data. Technical Specification 35.207 v18.0.0, 3GPP, 03 2024.

[8] 3GPP. TS 33.208 - Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data. Technical Specification 35.208 v18.0.0, 3GPP, 03 2024.

[9] ETSI. Smart Cards; UICC-Terminal interface; Physical and logical characteristics. Technical Specification ETSI TS 102 221 v18.2.0, ETSI, 06 2024.

[10] ETSI. Secure Elements; Additional UICC form factors and environmental conditions; Physical and logical characteristics. Technical Specification ETSI TS 102 671 v18.1.0, ETSI, 09 2024.

[11] GSMA. RSP Architetcure. Technical Specification SGP.21 v3.1, GSMA, 12 2023.

[12] GSMA. RSP Technical Specification. Technical Specification SGP.22 v3.1, GSMA, 12 2023.

[13] Geir M. Køien. The SUCI-AKA authentication protocol for 5G systems. *Wireless Personal Communications*, (3).

[14] 3GPP. TS 33.102 - 3G Security; Security architecture. Technical Specification 33.102 v19.1.0, 3GPP, 06 2025.

[15] 3GPP. TS 33.401 - Security architecture. Technical Specification 33.401 v19.0.0, 3GPP, 07 2025.

[16] 3GPP. TS 33.501 - Security architecture and procedures for 5G system. Technical Specification 33.501 v19.3.0, 3GPP, 07 2025.

[17] Shahzana Liaqat and Geir M. Køien. Analysis of eSIM/iSIM for Critical Communications. In Kevin Daimi and Abeer Al Sadoon, editors, *Proceedings of the Third International Conference on Innovations in Computing Research (ICR'24)*, pages 441–448. Springer Nature Switzerland, 2024.

[18] Meltem Sönmez Turan, Kerry McKay, Jinkeon Kang, John Kelsey, and Donghoon Chang. Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions. Special Publication NIST SP 800-232, NIST, 08 2025.

[19] Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Liyanage, Andrei Gurtov, and Mika Ylianttila. The roadmap to 6g security and privacy. *IEEE Open Journal of the Communications Society*, 2:1094–1122, 2021.

[20] DongHyun Je, Jungsoo Jung, and Sunghyun Choi. Toward 6g security: Technology trends, threats, and solutions. *IEEE Communications Standards Magazine*, 5(3):64–71, 2021.

[21] Van-Linh Nguyen, Po-Ching Lin, Bo-Chao Cheng, Ren-Hung Hwang, and Ying-Dar Lin. Security and privacy for 6g: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials*, 23(4):2384–2428, 2021.

[22] Volker Ziegler, Peter Schneider, Harish Viswanathan, Michael Montag, Satish Kanugovi, and Ali Rezaki. Security and trust in the 6g era. *IEEE Access*, 9:142314–142327, 2021.

[23] Jong Hyuk Park and Minji Kim. Quantum-resilient security for 6g networks: a comprehensive survey on challenges, solutions, and research opportunities. *The Journal of Supercomputing*, 81(9):1086, 2025.

[24] Togu Novriansyah Turnip, Birger Andersen, and Cesar Vargas-Rosales. Towards 6g authentication and key agreement protocol: A survey on hybrid post quantum cryptography. *IEEE Communications Surveys & Tutorials*, pages 1–1, 2025.

[25] Geir M. Køien. *Access Security in 6G: The 6G-ACE Protocol (A Concept Proposal)*, chapter 5, pages 93–121. River Publishers, 1 edition, 08 2024.

[26] Elaine Barker, Lily Chen, David Cooper, Dustin Moody, Andrew Regenscheid, Murugiah Souppaya, Bill Newhouse, Russ Housley, Sean Turner, William Barker, and Karen Scarfone. Considerations for Achieving Crypto Agility. Cybersecurity White Paper CSWP 39, NIST, 12 2025.

[27] Peter Gutmann and Stephan Neuhaus. Replication of Quantum Factorisation Records with an 8-bit Home Computer, an Abacus, and a Dog. Cryptology ePrint Archive, Paper 2025/1237, 2025.

[28] Michele Mosca and Marco Piani. Quantum threat timeline report 2024, 12 2024.

[29] Lennart Baumgärtner, Benjamin Klein, Niko Mohr, Anika Pflanzer, and Henning Soller. When—and how— to prepare for post-quantum cryptography, 05 2022.

[30] NIST. Module-Lattice-Based Key-Encapsulation Mechanism Standard. Federal Information Processing Standards Publication 203, NIST, 08 2023.

[31] E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. Standards Track RFC 8446, IETF, 08 2018.

[32] F. Yergeau. UTF-8, a transformation format of ISO 10646. Standards Track RFC 3629, IETF, 11 2003.

Biography

Geir M. Køien received his Ph.D. from Aalborg University on access security for mobile systems. He has also worked for many years in industry, including for LM Ericsson Norway and Telenor R&D. During these years he worked extensively with mobile systems, and with security and privacy. He has also worked with the Norwegian Defence Research Establishment and with the Norwegian Communications Authority on various security and communications related projects. Currently, he is a professor with the University of South-Eastern Norway (USN).