NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Check for updates

Initial NAS Message Security

Applying 5G Cybersecurity and Privacy Capabilities

NIST Cybersecurity White Paper

NIST CSWP 36F ipd

Michael Bartock
Jeffrey Cichonski

Information Technology Laboratory

Parisa Grayeli
Sanjeev Sharma

The MITRE Corporation

August 2026
Initial Public Draft

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.36F.ipd

Initial NAS Message Security

Abstract

This white paper is part of a series called Applying 5G Cybersecurity and Privacy Capabilities, which covers 5G cybersecurity- and privacy-supporting capabilities that were implemented as part of the 5G Cybersecurity testbed at the National Cybersecurity Center of Excellence (NCCoE). This white paper provides details regarding how 5G protects the initial Non-Access Stratum (NAS) message. Unlike previous generations of cellular systems, new requirements in 5G allow the User Equipment (UE) to send the security-sensitive contents of the initial NAS message in an encrypted and integrity-protected form. This paper also describes how the NCCoE 5G project demonstrated these capabilities and explains how organizations can verify these protections in deployed networks. 5G network operators should be aware of how these standards-defined security capabilities protect their users and subscribers. Operators should ensure that their 5G technologies protect sensitive content as described in the 5G standards. Mobile users should be cautious that this 5G security feature will not be available if their devices roam to previous generations of wireless systems.

Audience

Technology, cybersecurity, and privacy professionals who are involved in using, managing, or providing 5G-enabled services and products. This includes commercial mobile network operators, potential private 5G network operators, and end-user organizations. Readers should already be familiar with the basics of mobile network architectures and components.

Keywords

3GPP, 5G, cybersecurity, initial NAS message, Key set identifier.

Note to Reviewers

NIST is particularly interested in your feedback on the following questions:

1. How do you envision using this paper? What changes would you like to see to improve that use?
2. What additional information would you like this paper to provide?
3. What other 5G cybersecurity and privacy capabilities are you most interested in learning more about?

Acknowledgments

We are grateful to the following individuals for their generous contributions.

AMI: Muthukkumaran Ramalingam, Stefano Righi

AT&T: Jitendra Patel, Bogdan Ungureanu

CableLabs: Tao Wan

Cisco: Kori Rongey

Dell Technologies: Dan Carroll

Intel Corporation: Steve Orrin

Keysight Technologies: Corey Piggott

The MITRE Corporation: John Kent, Theresa Suloway, Thomas Walters

NIST: Cherilyn Pascoe, Kevin Stine

Nokia: Robert Cranston, Jorge Escobar

Palo Alto Networks: Aarin Buskirk, Julie Klein

T-Mobile: Todd Gibson

Overview

When cellular User Equipment (UE) is powered on, one of its early actions is to attempt establishment of a cellular connection. The UE determines its mobile operator based on locally stored subscription parameters, which include a list of preferred networks. It then searches for the preferred operator network and, once found, begins establishing a connection to access mobile services via the available network. Enabling security as early as possible during this process helps to ensure critical information is not at risk of interception or manipulation.

The mobile network is comprised of two high-level parts:

1. Radio Access Network (RAN), which takes care of the wireless (radio) communication with the UE and
2. Core Network (CN), which handles service aspects like authorization, session management, internet connectivity, mobility, etc.

Figure 1 shows the Cellular communication links between a UE, RAN, and CN. These links are established using a communication protocol stack, which consists of the radio technology-specific lower layers (Access Stratum or AS) and the radio-agnostic upper layers (Non-Access Stratum or NAS). The AS layers establish a "radio link" between the UE and the RAN. Using procedures defined in the AS protocols, the UE scans the radio frequencies, selects a suitable cell, and establishes radio resources. This is where specific time, frequency, and modulation allocations are agreed upon to transmit and receive radio signals. Once the "radio link" is ready, the NAS layers establish an end-to-end communication channel between the UE and the CN. As shown in Figure 1, the NAS channel passes over the "radio link" hop and then on to the "tower to datacenter backhaul" (Fiber, Microwave, RF) to reach CN.

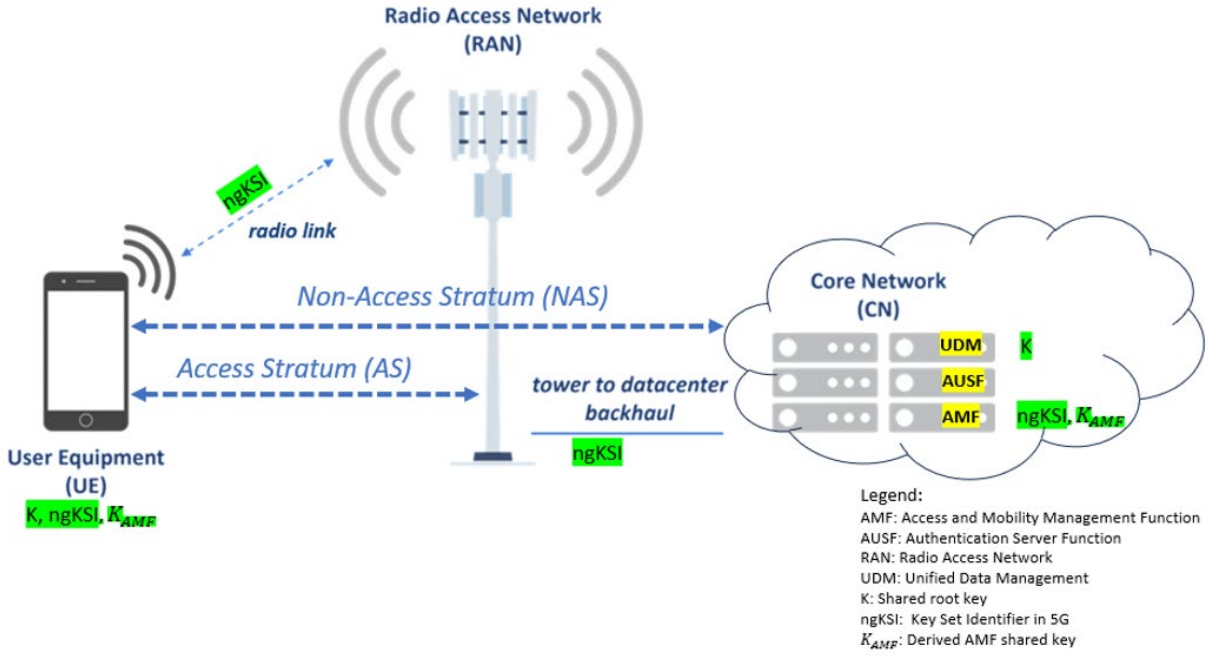

Figure 1: 5G architecture components involved in the establishment of AS and NAS connections

Once the AS connection between the UE and the RAN is established, the UE must handshake with the 5G core. This handshake is initiated with the initial NAS message. It is the first NAS message sent by the UE, in which the UE identifies itself to the CN and indicates potentially sensitive information, such as the security capabilities it can support and the services it is requesting.

What's the problem?

During the initial handshake, it is desirable for the UE to transfer as much information as needed by the CN to quickly establish the desired services and limit the number of round-trip messages. However, if the communication channel between the UE and the CN is not yet secure, all this information would be visible to a third party listening on the channel.

In 4G, all parts of the initial NAS message are sent in the clear without encryption and/or integrity protection. This leaves the 4G UE or the CN vulnerable to man-in-the-middle (MITM) attacks. MITM may be a malicious actor sitting in the middle of an authorized RAN and CN that intercepts the messages. In other cases, MITM may be a malicious RAN (Rogue Base Station [1] also known as a False Base Station [2]) that tricks the UE into establishing an AS connection with it and controls UE messages before sending them to the CN. RAN may also be untrusted in case of radio access via inter Public Land Mobile Network (PLMN) roaming partners, private networks, and Non-Terrestrial Networks (NTN). This may lead to the following cybersecurity and user privacy-related risks in 4G:

a) The initial NAS message may be tampered with, leading to denied or degraded service (also known as a DoS attack). For example, if an attacker changes the initial NAS message contents to signal that the UE can only support null schemes for confidentiality and integrity protection, then subsequent messages will also remain unprotected and subject to further tampering [3]. Such cases fall under cybersecurity risks.

b) Some UE- or CN-specific sensitive information may be revealed. This may lead to either compromising the privacy of users or exposing the network to further attacks. For example, the initial NAS message may reveal the UE's identity, and malicious actors may track the targeted user's movements (a privacy risk). The initial NAS message may also reveal the requested identifier of a network slice, which allows for follow-on behaviors against that slice with the help of that identifier (cybersecurity risk) [4][5].

A critical attribute for securing the NAS communication channel is that a mutual Authentication and Key Agreement (AKA) is performed between UE and CN at least once. After the AKA completes, the UE and CN can start using the agreed keys to successfully encrypt/decrypt subsequent NAS messages. The completion of the AKA establishes a "security context" between the UE and the CN.

The CN services a large number of UEs. So, when a UE starts an initial handshake with CN, the CN needs to determine things like:

- Which UE is trying to connect to it?
- What security capabilities does this UE support?
- Has this UE previously undergone mutual AKA and stored a security context that could be reused?

For the CN to successfully understand this information, locate the UE security context, or perform AKA, at least some parts of the initial NAS message must be sent as cleartext.

The above observations lead to the following challenges:

a) A UE cannot avoid sending at least some information as cleartext, meaning that at least some information remains vulnerable to eavesdropping or MITM attacks.

b) For the UE, including as much information as possible in the initial NAS message is more efficient and enables a quicker handshake, but protecting each piece of information individually increases the protocol complexity.

How do the 5G standards address the problem?

From the beginning, 5G specifications provided a set of capabilities to address these challenges and secure the initial NAS message as much as possible. The initial NAS message protection is achieved by splitting the message into two parts after the Message Header (Figure 2).

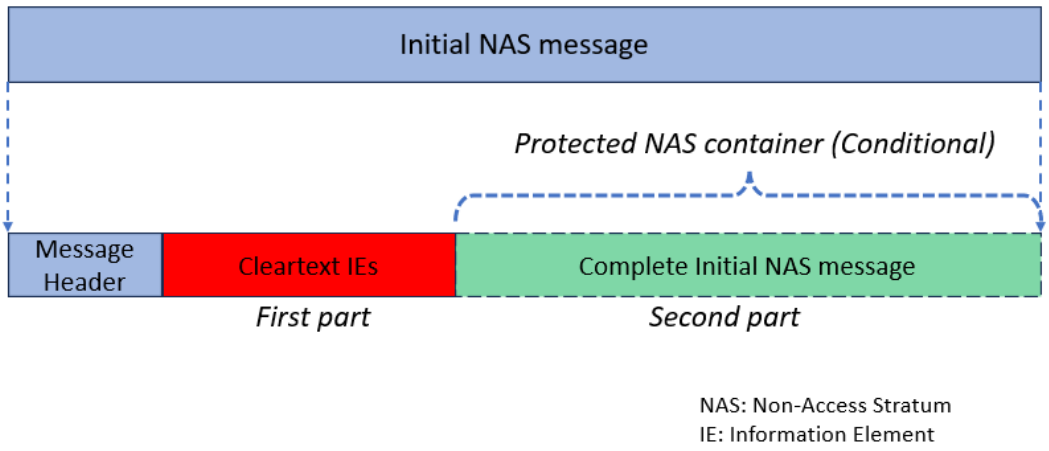

Figure 2: Initial NAS message

Cleartext Information Elements (IEs) (First Part): The network needs this information in cleartext to recognize the device requesting service. This limited set of IEs is the minimum information needed to either establish or identify the security context between the UE and the CN. The IEs sent in cleartext include UE subscription identifiers, UE security capabilities, the 5G Key Identifier (i.e., ngKSI, used to maintain the security context), etc.

Complete initial NAS message (Second Part): This is an integrity and confidentiality-protected NAS Container. It includes the same cleartext IEs of the first part, as well as the other more security-sensitive initial NAS IEs. The network compares the IEs in the first part to ensure they match the deciphered contents of the second part. If they do not match, the core network knows that the first part has been tampered with and can throw away the initial NAS message. This comparison helps protect against MITM attacks.

The initial NAS message is sent with only the cleartext IEs (First part) if the device has not successfully authenticated and no security context exists (which can happen when the device first appears on the network). If the device has previously completed a successful authentication and a security context is established, the initial NAS message is sent with both the Cleartext IEs (First part) and the Complete NAS message (Second part) (this often happens as a device moves between idle and active states).

The transfer and protection of the initial NAS message is illustrated in Figure 3 [6]. Here, AMF stands for Access and Mobility Management function inside the core network. The solid horizontal line in Figure indicates that Step is always applicable (Steps 1, 5); and the dashed line indicates that Step is applied on a need basis (Steps 2 to 4). Likewise, for the message label for each step, the fields within square braces are also applicable on a need basis. Note that the RAN is not explicitly shown between the UE and the AMF in Figure 3. Here, the focus is on NAS messages between the UE and the AMF over a logical interface (known as N1), even though they are carried as payload over a physical interface (known as NG) between the UE and the RAN.

Unlike previous generations, 5G makes integrity protection of signaling messages mandatory upon completion of the Security Mode procedure (except for the case of emergency services).

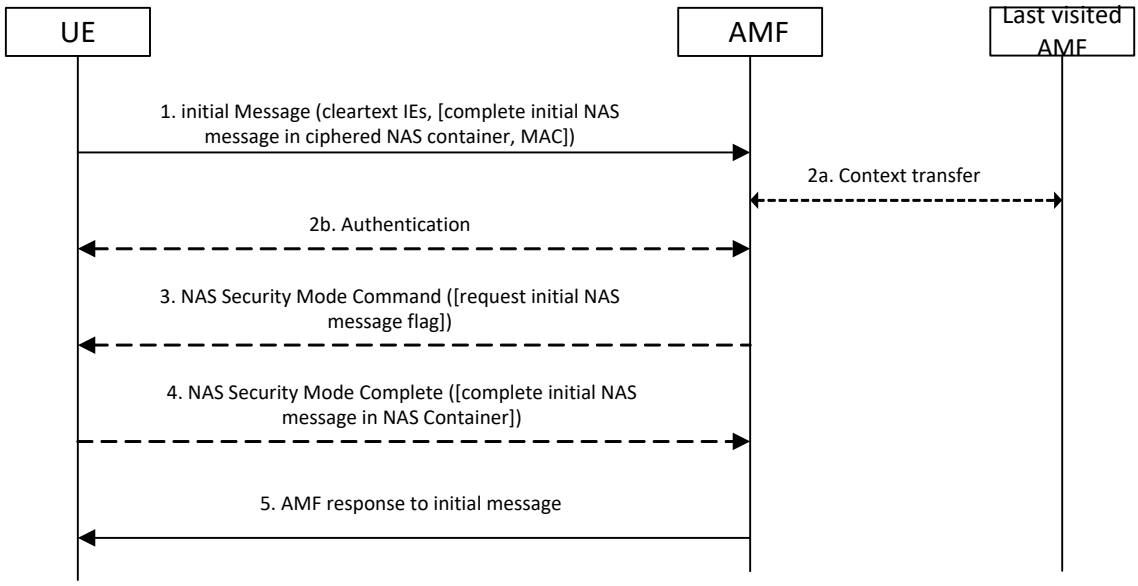

Figure 3: Initial NAS message flow diagram

While sending the initial NAS message, two conditions are possible:

I. The UE has no NAS security context (i.e., it does not have valid encryption or integrity keys). In this case, 5G standards prescribe a limited set of information elements that the UE sends in cleartext within the Initial Message (Step 1). The cleartext part ("first part" in Figure 2) is necessary to establish a security context between the UE and the CN. During the establishment of the security context (Steps 2 to 4), AMF requests the retransmission of the initial NAS message, and the complete initial NAS message ("second part") is included in the NAS Security Mode Complete message (as the integrity- and ciphering-protected NAS Container).

II. The UE already has a security context (i.e., it has valid encryption or integrity keys): the UE sends a message that consists of the cleartext IEs ("first part") and complete initial NAS message inside the integrity/ciphering protected NAS Container ("second part"), with the whole message's integrity protected (Step 1). In this case, there are two possibilities:

- The core network has the same security context, and the initial message passes integrity/ciphering check. In this case, steps 2 to 4 may be omitted.
- The initial message fails the integrity/ciphering check on the core network side (e.g., the AMF

cannot find the used security context in its database). In this case, a new security context is set up. During this setup, AMF requests to retransmit the initial NAS message, and then the complete initial message ("second part" in Figure 2) is included in the NAS Security Mode Complete message in a NAS Container (Steps 2 to 4).

Finally, the NAS transaction proceeds according to the UE request (Step 5).

The integrity- and ciphering-protected NAS Container ("second part") mitigates man-in-the-middle attacks for most IEs of the initial NAS message. 5G standards also provide protection of the cleartext information elements (IEs) in other specified ways. For example:

a) User privacy-related mitigations:

- UE identity is protected as discussed in NIST Cybersecurity White Paper (CSWP) 36A: Protecting Subscriber Identifiers with Subscription Concealed Identifier (SUCI) [7] and NIST Cybersecurity White Paper (CSWP) 36C: Reallocation of Temporary Identities [8].

b) Cybersecurity-related mitigations:

- 5G core network rejects the initial NAS message if the 'UE capability information' included in the message indicates that the UE does not support the integrity protection of signaling messages. For more details, see Case 4 under the clause "Technical Details of initial NAS message" of this whitepaper.
- 'UE capability information' included in the uplink message (Step 1 of Figure 3) is also replayed in the integrity-protected downlink message 'NAS Security Mode Command' (Step 3 of Figure 3). If UE detects a mismatch due to potential MITM tampering, it rejects the downlink message.
- All of the cleartext information is copied inside the protected NAS Container of the uplink (UE to network) message in either Step 1 or Step 4 of Figure 3 (depending on the NAS security context conditions described above). This means that CN can detect and mitigate potential tampering of the complete initial NAS message at either of these steps.

How can I use initial NAS message security?

5G systems compliant with 3GPP release 15 or later are capable of supporting a comprehensive protection of the initial NAS message. This is achieved by packaging most of the IEs into a secure NAS container and specifying other ways to protect the remaining cleartext IEs. These enhanced security features are only available in the 5G Stand-Alone (SA) deployments (i.e., 5G RAN with 5G core). A 5G Non-Stand-Alone (NSA) deployment uses 5G RAN with a 4G core network and lacks this cybersecurity feature. Network operators should consider the following:

Network operators are encouraged to upgrade to 5G SA deployments for comprehensive initial NAS message security.

Network operators are encouraged to leverage all of 5G security features applicable to the UE identity cleartext IEs (SUCI, GUTI, TMSI). See NIST Cybersecurity White Paper (CSWP) 36A: Protecting Subscriber Identifiers with Subscription Concealed Identifier (SUCI) [7] and NIST Cybersecurity White Paper (CSWP) 36C: Reallocation of Temporary Identities [8].

Network operators should make sure that the 5G core is processing the initial NAS message correctly and disregarding messages attempting to ask for unsupported security configurations (e.g., NULL NAS Integrity (See Case 4 under clause “Technical Details of initial NAS message security” of this whitepaper).

Organizations using 5G technologies should understand how this capability can mitigate cybersecurity and privacy risks and check with their service provider to ensure that initial NAS messages are protected as expected.

What else should I know about initial NAS message security?

After establishing a security context between the UE and the CN, integrity protection of signaling messages is mandatory in 5G (except for emergency services), while encryption is optional.

Allowed cleartext IEs

Some IEs can be sent in clear text. The 3GPP groups work together to evaluate the cybersecurity and privacy risks when an IE is determined to be allowed to be sent in the clear. These allowed cleartext IEs include UE subscription identifiers, UE security capabilities, 5G Key Set Identifier (i.e., ngKSI, used to maintain security context), etc.

The allowed cleartext IEs in various types of initial NAS messages, as specified in 3GPP TS 24.501 [9], are listed below.

IE Name	Purpose	Presence
Extended protocol discriminator	Message header	All
Security header type	Message header	All
Spare half octet	Message header	All
Message identity	Message header	All
Message type	Registration type, De-registration type, Service type, Control plane service type	All
ngKSI	NAS key set identifier	All
5GS mobile identity	Subscription identifiers (e.g. Subscription Concealed Identifier, SUCI or Globally Unique Temporary UE Identity, GUTI)	REGISTRATION REQUEST, DEREGISTRATION REQUEST
5G S-Temporary Mobile Subscription Identifier (5G-S-TMSI)	Subscription identifier	SERVICE REQUEST
UE security capability	Security capabilities of UE	REGISTRATION REQUEST
UE status	Indication that the UE is moving from EPC	REGISTRATION REQUEST
Additional GUTI	A valid 5G-GUTI that was previously assigned by the same PLMN, an equivalent PLMN or any other PLMN	REGISTRATION REQUEST
Evolved Packet System (EPS) NAS message container	IE containing the TAU Request in the case idle mobility from LTE	REGISTRATION REQUEST
Network Identifier (NID)	Included if the 5G-GUTI in the 5GS mobile identity IE was assigned by a Stand-alone Non-Public Network (SNPN) other than the SNPN with which the UE is registering	REGISTRATION REQUEST
UE determined Public Land Mobile Network (PLMN) with disaster condition	To support disaster roaming services	REGISTRATION REQUEST

5G Key Set Identifier (ngKSI)

5G Key Set identifier (ngKSI) is a value between 0 and 7. It is used to maintain the security context (i.e., ciphering and integrity keyset) between UE and CN. A value of 7 means UE has no stored security context. In this case, UE first completes AKA as described in Figure 3. During AKA, both UE and CN generate and store a new ciphering and integrity keyset. This keyset generation is described in 3GPP TS 33.501 [6]. CN provides the UE with an ngKSI value other than 7 for managing the new keyset. As shown in Figure 1, only an ngKSI is transmitted from either the CN or the UE (not the actual keyset). When the initial NAS message needs to be sent, UE leverages this ngKSI to look up the stored keyset and apply message security.

Summary

The initial NAS message is the first message needed to establish a connection between the UE and the CN. If sensitive information elements in the initial NAS messages are not integrity- and encryption-protected, the UE and CN may remain vulnerable to man-in-the-middle attacks. This was the case with 4G core networks. To mitigate these security and privacy risks, 5G standards have split the initial NAS message structure into two parts. The first cleartext part is sent by the UE regardless of whether a security context exists between the UE and the CN. However, the second protected NAS container part is sent only when a security context exists. This ensures that sensitive information is transferred from UE to CN as soon as possible, without the risk of tampering. This kind of protection is not available in previous generations of core networks. While evaluating their cybersecurity and privacy risks, network operators and organizations should be mindful of this new 5G capability. By transitioning to 5G standalone core deployments, operators and organizations can reduce their cybersecurity risks while also considering associated privacy implications.

Technical details of initial NAS message security

The rest of this white paper is intended for readers seeking more in-depth knowledge of initial NAS message security.

> For background information on the NCCoE 5G Cybersecurity project, including the architecture and components of the 5G standalone network built within the demonstration testbed environment, see NIST SP 1800-33 Volume B, 5G Cybersecurity, Approach, Architecture, and Security Characteristics [10].

How mobile operators can validate their initial NAS message security

3GPP has specified a few test cases to validate the security of the initial NAS message in TS 33.512 [11]. To demonstrate the implementation of these requirements, we ran registration tests in our 5G testbed across various cases and captured traffic between the gNB and the AMF. From the analysis of the packet capture tool logs, it can be verified how the initial NAS messages are being protected.

Case 1: There is no initial security context during UE registration, and the network is configured to turn OFF encryption of NAS messages (this network configuration is useful for understanding the full handshake between UE and AMF). In this case (Figure 4), the packet capture tool can decode all NAS messages. Figure 4 shows that the Authentication and Key Agreement (lines 2-3) occurs immediately after the initial registration message (line 1), and a new KSI (0) is assigned to the derived K_{AMF}. After receiving the Security mode command (line 4), both the UE and the network are ready to begin using the new security context associated with KSI 0. Note that the initial registration message is simply replayed inside the container part of the Security mode complete message (line 5), and the KSI value 7 in that container indicates the security context that existed before the security mode command was received. However, the UE has already switched to KSI 0 to protect the full uplink Security mode complete message.

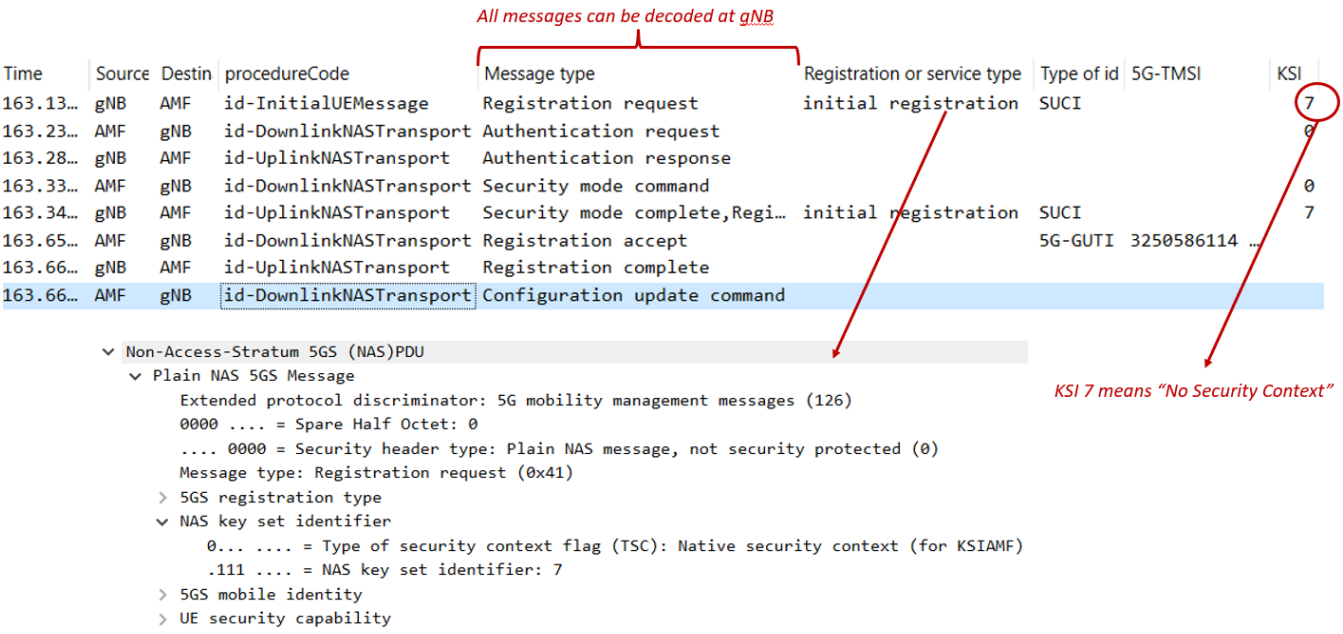

Figure 4: Initial NAS message Case 1

Case 2 (preferred): There is no initial security context during UE registration, and the network is configured to turn ON encryption of NAS messages (this network configuration is the desired operation mode). In this case (Figure 5), the packet capture tool can decode all parts of NAS messages until the security mode command (line 4). Here, a new KSI (0) is assigned during Authentication and Key Agreement (lines 2-3). The uplink security mode complete message (line 5) is not decoded because the UE has already switched to using a new security context, and the uplink message is ciphered with keys corresponding to KSI 0. The second security mode command (line 6) is likely a retransmission of the first (line 4). This may happen if the uplink message (line 5) is somehow late to arrive or lost.

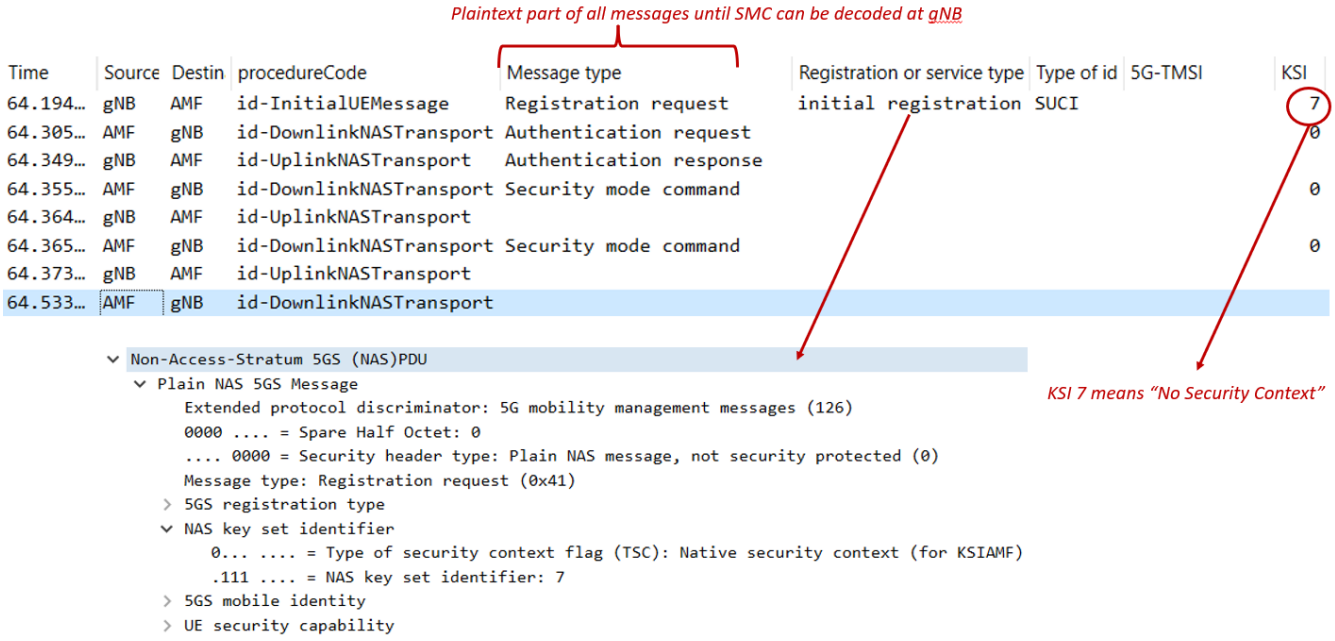

Figure 5: Initial NAS message Case 2

Case 3: This case is a sequel to case 2. An initial security context is established during UE registration, and the network is configured to enable the encryption of NAS messages. In this case (Figure 6), the packet capture tool can decode only the plaintext part of NAS messages until the Security Mode Command. Reviewing the messages reveals that the KSI has changed from 4 to 5 between the registration request (line 1) and the security mode command (line 4), implying that the intermediate, non-decoded messages (lines 2-3) correspond to the Authentication request/response.

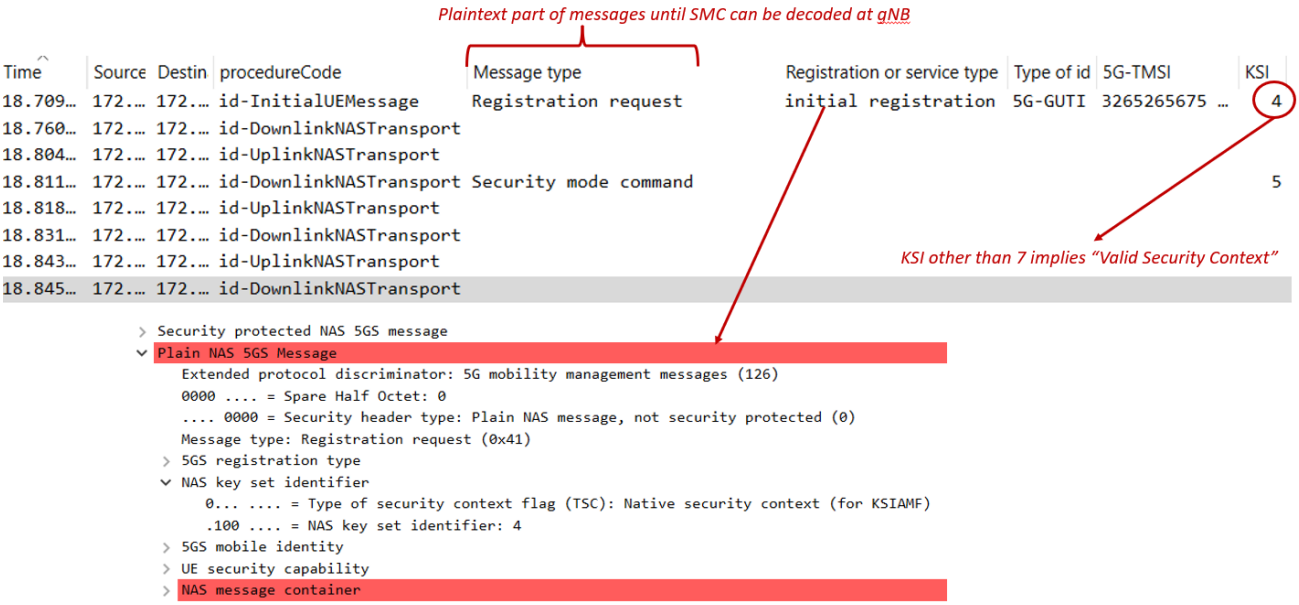

Figure 6: Initial NAS message Case 3

Case 4: To highlight the importance of protecting the initial NAS message, we set up a False Base Station [2] in the lab. In this scenario, we tamper with the UE-capability part (which is plaintext) of the 'Registration request' message. By doing so, we intend to check whether the network would accept the registration of a UE that claims not to support 5G NAS message integrity. This test aligns with clause 4.2.2.6.1 of 3GPP TS 33.512 [11].

The tampered UE capability content of the Registration Request is shown in Figure 7. Left-side content is the original information element (within the first part of the initial NAS message; see Figure 2, and right-side content is the tampered one. The modified bits are shown in red boxes.

```
UE security capability                          UE security capability
    Element ID: 0x2e                                Element ID: 0x2e
    Length: 4                                       Length: 4
    1... .... = 5G-EA0: Supported                   1... .... = 5G-EA0: Supported
    .1.. .... = 128-5G-EA1: Supported               .0.. .... = 128-5G-EA1: Not supported
    ..1. .... = 128-5G-EA2: Supported               ..0. .... = 128-5G-EA2: Not supported
    ...1 .... = 128-5G-EA3: Supported               ...0 .... = 128-5G-EA3: Not supported
    .... 0... = 5G-EA4: Not supported               .... 0... = 5G-EA4: Not supported
    .... .0.. = 5G-EA5: Not supported               .... .0.. = 5G-EA5: Not supported
    .... ..0. = 5G-EA6: Not supported               .... ..0. = 5G-EA6: Not supported
    .... ...0 = 5G-EA7: Not supported               .... ...0 = 5G-EA7: Not supported
    0... .... = 5G-IA0: Not supported               1... .... = 5G-IA0: Supported
    .1.. .... = 128-5G-IA1: Supported               .0.. .... = 128-5G-IA1: Not supported
    ..1. .... = 128-5G-IA2: Supported               ..0. .... = 128-5G-IA2: Not supported
    ...1 .... = 128-5G-IA3: Supported               ...0 .... = 128-5G-IA3: Not supported
    .... 0... = 5G-IA4: Not supported               .... 0... = 5G-IA4: Not supported
    .... .0.. = 5G-IA5: Not supported               .... .0.. = 5G-IA5: Not supported
    .... ..0. = 5G-IA6: Not supported               .... ..0. = 5G-IA6: Not supported
    .... ...0 = 5G-IA7: Not supported               .... ...0 = 5G-IA7: Not supported
    1... .... = EEA0: Supported                     1... .... = EEA0: Supported
    .1.. .... = 128-EEA1: Supported                 .1.. .... = 128-EEA1: Supported
    ..1. .... = 128-EEA2: Supported                 ..1. .... = 128-EEA2: Supported
    ...1 .... = 128-EEA3: Supported                 ...1 .... = 128-EEA3: Supported
    .... 0... = EEA4: Not supported                 .... 0... = EEA4: Not supported
    .... .0.. = EEA5: Not supported                 .... .0.. = EEA5: Not supported
    .... ..0. = EEA6: Not supported                 .... ..0. = EEA6: Not supported
    .... ...0 = EEA7: Not supported                 .... ...0 = EEA7: Not supported
    0... .... = EIA0: Not supported                 0... .... = EIA0: Not supported
    .1.. .... = 128-EIA1: Supported                 .1.. .... = 128-EIA1: Supported
    ..1. .... = 128-EIA2: Supported                 ..1. .... = 128-EIA2: Supported
    ...1 .... = 128-EIA3: Supported                 ...1 .... = 128-EIA3: Supported
    .... 0... = EIA4: Not supported                 .... 0... = EIA4: Not supported
    .... .0.. = EIA5: Not supported                 .... .0.. = EIA5: Not supported
    .... ..0. = EIA6: Not supported                 .... ..0. = EIA6: Not supported
    .... ...0 = EIA7: Not supported                 .... ...0 = EIA7: Not supported
```

Figure 7: Tampered UE capability information

As shown in Figure 8, the AMF repeatedly denies registration with the cause "UE security capabilities mismatch." KSI value of 7 in the last column indicates that UE does not have a valid security context. Because it is mandatory to support NAS message integrity in 5G, the AMF does not accept any UE that claims not to support it. This scenario illustrates that a properly configured 5G core network is able to mitigate tampering of the cleartext UE Capability IE. However, it is impractical to protect all IEs with such specialized handling. Whenever possible, those IEs are protected within the NAS container, as shown earlier in Figure 2.

Time	Source	Destinati	procedureCode	Message type	Registration or service typ	Reject cause	Type of id	KSI
83.32…	10.5…	10.53.…	id-InitialUEMessage	Registration request	initial registration		SUCI	7
83.32…	10.5…	10.53.…	id-DownlinkNASTransport	Registration reject		UE security capabilities mismatch		
93.60…	10.5…	10.53.…	id-InitialUEMessage	Registration request	initial registration		SUCI	7
93.60…	10.5…	10.53.…	id-DownlinkNASTransport	Registration reject		UE security capabilities mismatch		
103.9…	10.5…	10.53.…	id-InitialUEMessage	Registration request	initial registration		SUCI	7
103.9…	10.5…	10.53.…	id-DownlinkNASTransport	Registration reject		UE security capabilities mismatch		
114.2…	10.5…	10.53.…	id-InitialUEMessage	Registration request	initial registration		SUCI	7
114.2…	10.5…	10.53.…	id-DownlinkNASTransport	Registration reject		UE security capabilities mismatch		
124.4…	10.5…	10.53.…	id-InitialUEMessage	Registration request	initial registration		SUCI	7
124.4…	10.5…	10.53.…	id-DownlinkNASTransport	Registration reject		UE security capabilities mismatch		
200.8…	10.5…	10.53.…	id-InitialUEMessage	Registration request	initial registration		SUCI	7
200.8…	10.5…	10.53.…	id-DownlinkNASTransport	Registration reject		UE security capabilities mismatch		
211.1…	10.5…	10.53.…	id-InitialUEMessage	Registration request	initial registration		SUCI	7
211.1…	10.5…	10.53.…	id-DownlinkNASTransport	Registration reject		UE security capabilities mismatch		
221.4…	10.5…	10.53.…	id-InitialUEMessage	Registration request	initial registration		SUCI	7
221.4…	10.5…	10.53.…	id-DownlinkNASTransport	Registration reject		UE security capabilities mismatch		

Figure 8: Initial NAS message Case 4

Case 5: In this scenario, the UE does not have any security context, and we tamper with the 'Registration type' value (which is plaintext) of the 'Registration request' message. We use a False Base Station [2] for this tampering. By doing so, we intend to check if the network would request retransmission of the initial NAS message, and UE registration would be processed after the security context setup. This test aligns with clause 4.2.2.3.4 of 3GPP TS 33.512 [11].

The packet capture log is shown in Figure 9. The 'Registration type' value in the first 'Registration request' message is tampered with from 'initial registration' to 'mobility registration.' KSI value in the last column is 7, which implies that the UE does not have a security context when the first message is sent. AMF proceeds with the authentication procedure and, after its completion, sends the 'Security mode command,' where it flags that retransmission of the initial NAS message is needed. When UE sends the 'Security mode complete', it retransmits the complete 'Registration request' message inside integrity protected NAS container (note that ciphering is intentionally set to NULL in this lab test setup for full visibility of message contents). Inside the protected NAS container, AMF receives the correct value of Registration type (i.e. 'initial registration'). After this, AMF and UE proceed with the completion of the registration procedure.

Time	Sourc	Destinati	procedureCode	Message type	Registration or service typ	Reject cause	Type of id	KSI
1004.949…	10.5…	10.53.…	id-InitialUEMessage	Registration request	mobility registratio…		SUCI	7
1004.963…	10.5…	10.53.…	id-DownlinkNASTransport	Authentication requ…				0
1004.999…	10.5…	10.53.…	id-UplinkNASTransport	Authentication fail…		Synch failure		
1005.002…	10.5…	10.53.…	id-DownlinkNASTransport	Authentication requ…				1
1005.079…	10.5…	10.53.…	id-UplinkNASTransport	Authentication resp…				
1005.081…	10.5…	10.53.…	id-DownlinkNASTransport	Security mode comma…				1
1005.099…	10.5…	10.53.…	id-UplinkNASTransport	Security mode compl…	initial registration		IMEISV…	7
1005.108…	10.5…	10.53.…	id-InitialContextSetup	Registration accept			5G-GUTI	
1005.312…	10.5…	10.53.…	id-UERadioCapabilityIn…	Registration comple…				

Figure 9: Initial NAS message Case 5, UE has no security context

For comparison, if the UE already has a security context, the packet capture log looks like Figure 10. KSI value in the last column is 3. If the Registration request passes the integrity check on the AMF side, the authentication and security mode commands are bypassed. AMF and UE proceed directly with the completion of the registration procedure.

Time	Sourc	Destinati	procedureCode	Message type	Registration or service typ	Reject cause	Type of id	KSI
1.9416…	10.5…	10.53.…	id-InitialUEMessage	Registration reques…	initial registration…		5G-GUT…	3,3
1.9489…	10.5…	10.53.…	id-InitialContextSetup	Registration accept			5G-GUTI	
2.1690…	10.5…	10.53.…	id-UERadioCapabilityIn…	Registration comple…				

Figure 10: Initial NAS message case 5, UE has security context.

References

[1] Cichonski JA, Franklin JM, Bartock MJ. 2016. Guide to LTE Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-187. https://doi.org/10.6028/NIST.SP.800-187

[2] Tao Wan. 2019. False Base Station or IMSI Catcher: What You Need to Know. Available at https://www.cablelabs.com/blog/false-base-station-or-imsi-catcher-what-you-need-to-know

[3] Chlosta M, Rupprecht D, Holz T, Pöpper C. 2019. LTE Security Disabled—Misconfiguration in Commercial Networks. *WiSec '19, May 15–17, 2019, Miami, FL, USA* (Association for Computing Machinery). https://doi.org/10.1145/3317549.3324927

[4] MITRE Corporation. 2024. *Discover Network Slice Identifier*. Available at https://fight.mitre.org/techniques/FGT5028/

[5] MITRE Corporation. 2024. *Spoof Network Slice Identifier*. Available at https://fight.mitre.org/techniques/FGT5027

[6] 3rd Generation Partnership Project. *Specification # 33.501: Non-Access-Stratum (NAS) protocol for 5G System* Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[7] Bartock M, Cichonski J, Souppaya M, Scarfone K, Grayeli P, Sharma S, Teague C. 2026. Protecting Subscriber Identifiers with Subscription Concealed Identifier (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 36A. https://doi.org/10.6028/NIST.CSWP.36A

[8] Bartock M, Cichonski J, Souppaya M, Scarfone K, Grayeli P, Sharma S. 2026. Reallocation of Temporary Identities (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 36C. https://doi.org/10.6028/NIST.CSWP.36C

[9] 3rd Generation Partnership Project. *Specification # 24.501: Non-Access-Stratum (NAS) protocol for 5G System.* Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3370

[10] Bartock M, Cichonski J, Souppaya M, Dey S, Grayeli P, Mulugeta B, Sharma S, Teague C, Scarfone K, Righi S, Ramalingam M, Rhea P, Santharam M, Mosley R, Ungureanu B, Patel J, Wan T, Romness P, Hyatt M, Lebel L, Carroll D, Orrin S, Brown L, Zhou Y, Piggott C, Jones M, Yeh M, Atkinson G, Eustace D, Wenger B, Morgan S, Balmakhtar M, Schumacher G. 2022. 5G Cybersecurity. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-33B. Available at https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf

[11] 3rd Generation Partnership Project. *Specification # 33.512: 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF).* Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3445

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements

NIST Technical Series Publication Identifier Syntax

Author ORCID IDs

Michael Bartock: 0000-0003-0875-4555
Jeffrey Cichonski: 0009-0006-1137-2549

How to Cite this NIST Technical Series Publication:

Bartock M. et al. (2026) Initial NAS Message Security: Applying 5G Cybersecurity and Privacy Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 36F ipd. https://doi.org/10.6028/NIST.CSWP.36F.ipd

Public Comment Period

August 6, 2026 – September 7, 2026

Submit Comments

5g-security@nist.gov
Or submit the web form at https://www.nccoe.nist.gov/5g-cybersecurity
National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory 100 Bureau Drive (Mail Stop 2000)
Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at https://www.nccoe.nist.gov/5g-cybersecurity, including related content, potential updates, and document history.
All comments are subject to release under the Freedom of Information Act (FOIA).