

# No SUPI-Based Paging: *Applying 5G Cybersecurity and Privacy Capabilities*

---

Michael Bartock  
Jeffrey Cichonski  
Murugiah Souppaya  
*Information Technology Laboratory*

Karen Scarfone  
*Scarfone Cybersecurity*

Parisa Grayeli  
Sanjeev Sharma  
*The MITRE Corporation*

January 2025  
Initial Public Draft

## Abstract

This white paper provides an overview of “no Subscription Permanent Identifier (SUPI) based paging,” a 5G capability for protecting users from being identified and located by an attacker. Unlike previous generations of cellular systems, new requirements in 5G protect subscriber confidentiality by using a temporary identity (ID) instead of SUPI for the paging protocol, and explicitly define when the temporary ID must be reallocated (refreshed). 5G network operators and organizations using 5G technologies are encouraged to verify that the paging is happening as described in the 5G standards. 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 project](#) at the National Cybersecurity Center of Excellence (NCCoE).

## 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, paging, privacy, Subscription Concealed Identifier (SUCI), Subscription Permanent Identifier (SUPI)

## 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: Matt Hyatt, Steve Vetter

Dell Technologies: Dan Carroll

Intel: Steve Orrin

Keysight Technologies: Corey Piggott

MITAC Computing Technology Corp.: Michael Yeh

The MITRE Corporation: Sallie Edwards, Mary Raguso, Theresa Suloway, Charles Teague

NIST: Cherilyn Pascoe, Adam Sedgewick, Kevin Stine

Nokia Bell Labs: Gary Atkinson, Rajasekhar Bodanki, Don McBride

Palo Alto Networks: Aarin Buskirk, Bryan Wenger

T-Mobile: Todd Gibson

## Overview

Previous generations of cellular systems often used permanent or quasi-permanent IDs for paging the subscribers – leaving them vulnerable to cybersecurity and privacy risks. This paper explains how 5G networks have mitigated this problem by removing the *Subscription Permanent Identifier (SUPI)* relationship from paging protocol. Only temporary IDs are used to page UEs, and reallocating the temporary IDs is required when certain events associated with a specific user occur, including paging. We refer to this 5G standards enhancement as “no SUPI-based paging.” If mobile user equipment (UE) roams back from 5G to a previous generation system, these new protections may not be available.

## How does paging work?

All generations of mobile networks alert the UE for incoming calls or messages by broadcasting a cleartext *paging message*, also known as a *paging alert*. The mobile network uses a predefined set of radio resources called a *paging channel* to send the paging alerts. Because there are many UEs registered to the network, paging alerts are distributed across the complete paging channel over several paging occasions (POs), which means that specific radio resources in time and frequency are used to target a certain group of registered UEs. The POs for the group of UEs repeat themselves with a periodicity called a *paging cycle*. In other words, the paging channel consists of several POs which repeat after each paging cycle.

This concept is illustrated in Figure 1 for one paging cycle. For simplicity, the paging channel is shown as a contiguous set of radio resources. However, these resources don't need to be contiguous. In this example, PO1 is used to alert UEs 1, 2, and 3; PO2 is used to alert UE 4; PO4 is used to alert UE 5; and PO5 is used to alert UEs 6 and 7. All the UEs are monitoring their respective POs (solid or dashed lightning icons indicate that a page could potentially be transmitted to the UE), but only UEs 1, 5, and 7 are actually paged (shown as the solid yellow lightning icons; the dashed icons indicate a page could have arrived but it didn't). Depending on the presence or absence of certain UEs in a given area, some POs, like PO3, may be unused in any paging cycle.

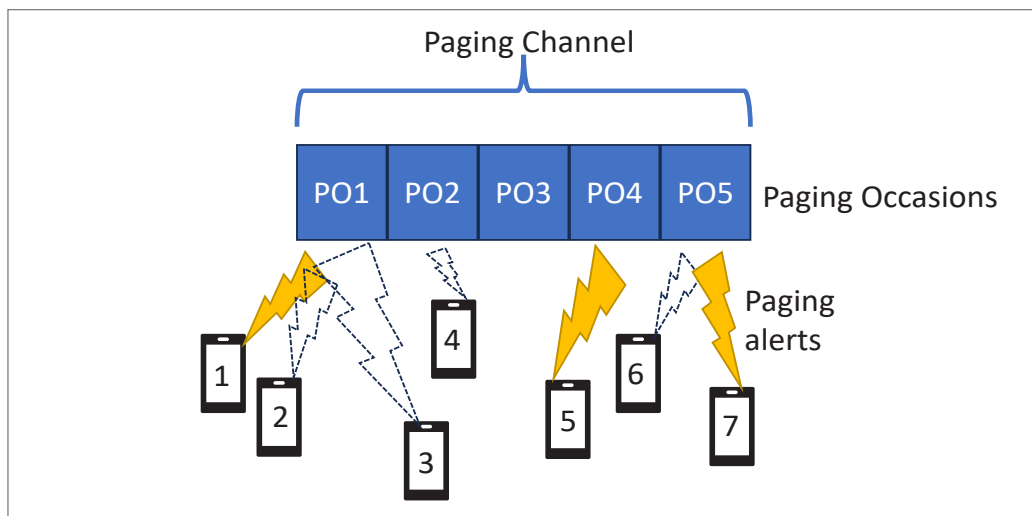


Figure 1. Example paging scenario for seven UEs

It should be evident from the above example that both the network and a given UE should know which PO would be used for alerting that UE. In cellular networks, a PO is calculated based on the subscriber/UE identity. 5G networks do not associate subscribers by their names. Instead, they use a permanent identifier called the *Subscription Permanent Identifier (SUPI)* for managing each subscription. The SUPI is written into the *Subscriber Identity Module (SIM)* provided by the subscriber's network operator. SUPI is the 5G equivalent of 4G's *International Mobile Subscriber Identity (IMSI)*. During the connection process (also referred to as "registration" in technical specifications), a temporary identifier called the 5G Globally Unique Temporary UE Identity (5G-GUTI) is calculated by the network, then associated with and stored within the user equipment (UE) — the mobile device and its SIM. Figure 2 shows these subscriber or UE identities.

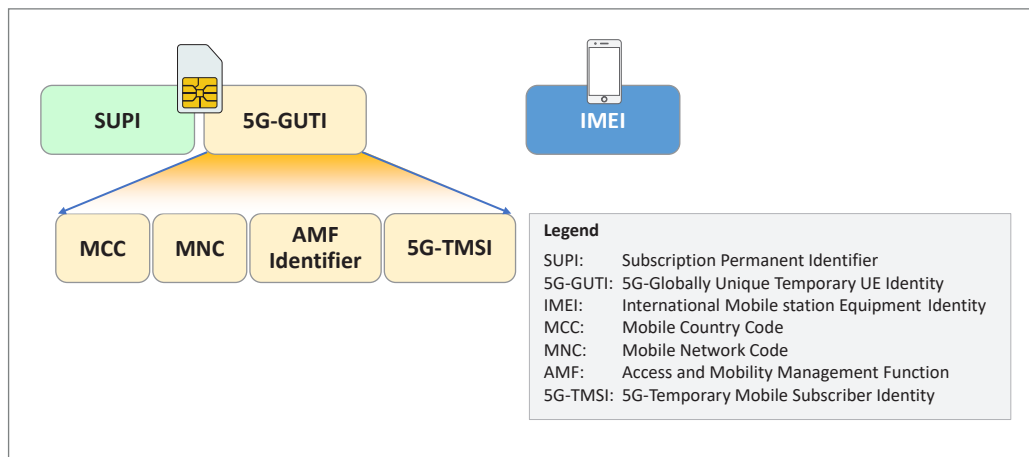


Figure 2: Subscriber or UE-related identities

## What's the problem?

The mobile network distributes its paging alerts for all users in a predefined manner. To conserve its battery, a UE shuts off radio frequency activity when it is idle and turns the radio hardware on at its PO to check if any paging alert is addressed for it. In 3G and 4G networks, there were three primary weaknesses discovered around paging. These weaknesses introduced privacy implications for users/subscribers. For instance, paging could allow an attacker to infer a victim's location based on the victim's permanent identifier or to inject fabricated emergency alerts.<sup>1</sup>

- The PO was related to the subscriber's permanent identifier (IMSI) based on a formula. This became a vulnerability because by listening to specific POs, one could infer the presence of specific group of IMSIs/UEs in that area.
- For paging channel efficiency reasons, multiple UEs fall under the same PO. To uniquely identify a specific user, the paging alert would also contain the permanent identifier or shorter version of the temporary identifier as plaintext. In case of the former, one could directly know the presence of specific IMSIs/UEs in that area by decoding the cleartext paging alerts.

<sup>1</sup> A. Singla et al., "Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks," Proceedings on Privacy Enhancing Technologies, 2020, pp. 126-142. Available: <https://petsymposium.org/2020/files/papers/issue1/popets-2020-0008.pdf>

- c. It was subsequently discovered that many networks did not refresh the temporary IDs often enough, which caused them to become quasi-permanent.<sup>2</sup> Again, one could infer the presence of specific UEs in that area by decoding the cleartext paging alerts.

To summarize, before 5G the POs had a direct relationship with the permanent UE identity, and each broadcasted cleartext paging alert contained a permanent or quasi-permanent UE identity. This made the paging protocol vulnerable to attacks that could have severe repercussions, including privacy risks to users/subscribers.

## How does “no SUPI-based paging” address the problem?

Starting with 3GPP release 15 in 2019, 5G networks resolved the weaknesses as follows:

- a. 5G networks always determine paging timing based on a temporary identifier (called 5G-Serving Temporary Mobile Subscriber Identifier or 5G-S-TMSI). Note that 5G-S-TMSI is derived from 5G-GUTI, as explained in the next section.
- b. The paging alert contains the temporary identifier 5G-S-TMSI only.
- c. It is mandatory for the network to reallocate or change the temporary identifier 5G-GUTI after each paging.<sup>3</sup>

In other words, 5G does not have a SUPI-based relationship in either the paging occasion calculation or the paging alert contents. Now that there is no long-term association between paging and the UE identity, it is impractical to attack the paging protocol. This approach of limiting device identification protects user confidentiality and, by extension, user privacy.<sup>4</sup>

Figure 3 is a simplified version of the 5G architecture that shows the architectural components involved in the paging, with all other components omitted. The UE comprises a SIM and a mobile handset. There is a wireless link between the UE and the Radio Access Network (RAN). On the other side, the RAN is connected to the Core Network (CN) via backhaul traffic transport. The green highlighted UE identifiers are shown either stored at the related component or flowing over the signaling paths. 5G-GUTI is managed by the Access and Mobility Management Function (AMF).

<sup>2</sup> Byeongdo Hong et al., “GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier,” NDSS ’18. Available: [https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018\\_02A-4\\_Hong\\_paper.pdf](https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_02A-4_Hong_paper.pdf)

<sup>3</sup> Bartock M. et al. (2024), “Reallocation of Temporary Identities.” <https://doi.org/10.6028/NIST.CSWP.36C.ipd>

<sup>4</sup> P. K. Nakarmi, “Fighting IMSI catchers: A look at 5G cellular paging privacy.” Available: <https://www.ericsson.com/en/blog/2019/5/fighting-imsi-catchers-5g-cellular-paging-privacy>

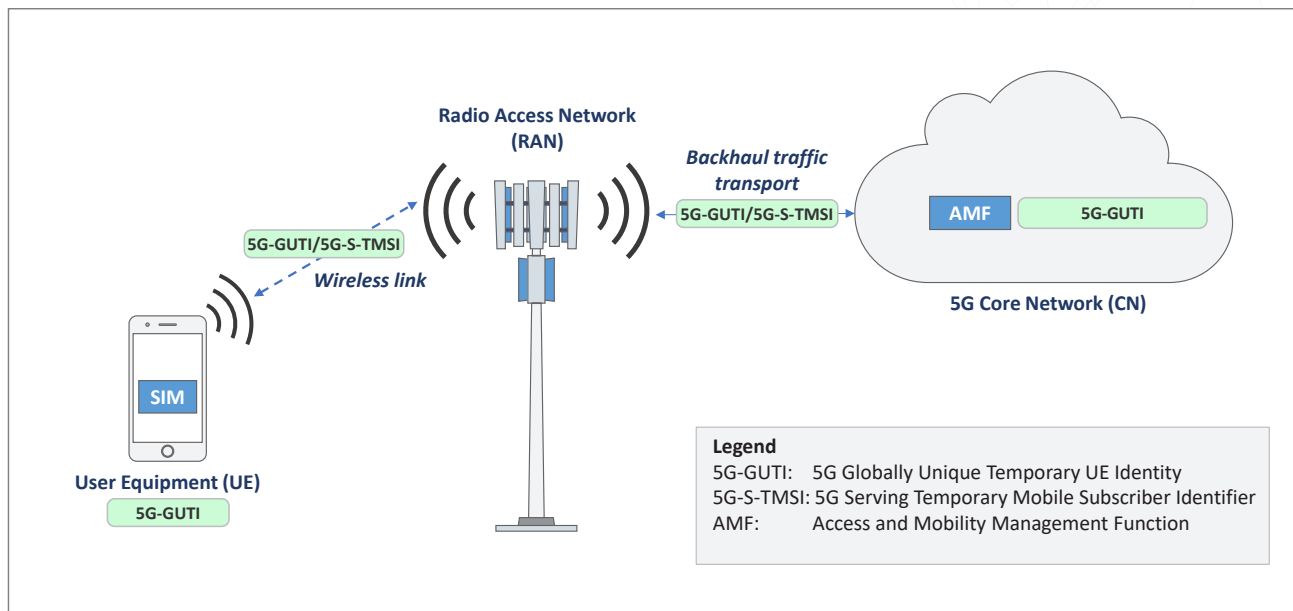


Figure 3. 5G architecture components involved in the paging capability

## How can I use “no SUPI-based paging?”

5G network functions compliant with 3GPP release 15 or later are required to support no SUPI-based paging.

Network operators are encouraged to coordinate with their 5G equipment vendors to verify that the paging protocol for UEs is not based on SUPI and the temporary IDs are reallocated as expected.

Organizations using 5G technologies are encouraged to understand how this capability can mitigate cybersecurity and privacy risks and to check with their service provider to ensure that the paging protocol for UEs is as expected.

## What else should I know about “no SUPI-based paging?”

5G-S-TMSI is an important identifier to know in the paging context. In the paging and service request procedures, a shortened form of the 5G-GUTI, the 5G-S-TMSI, is used to enable more efficient radio signaling. If the UE has a valid 5G-GUTI, it also has a valid 5G-S-TMSI. This relationship is shown in Figure 4. Because 5G-S-TMSI has a direct relationship to 5G-GUTI, it changes/refreshes each time 5G-GUTI changes or is reallocated. AMF and the UE can derive the 5G-S-TMSI from the current 5G-GUTI. The UE stores the full 5G-GUTI locally. However, for the paging procedure, it calculates the paging occasion based on the derived 5G-S-TMSI and listens for the matching 5G-S-TMSI on the paging channel.

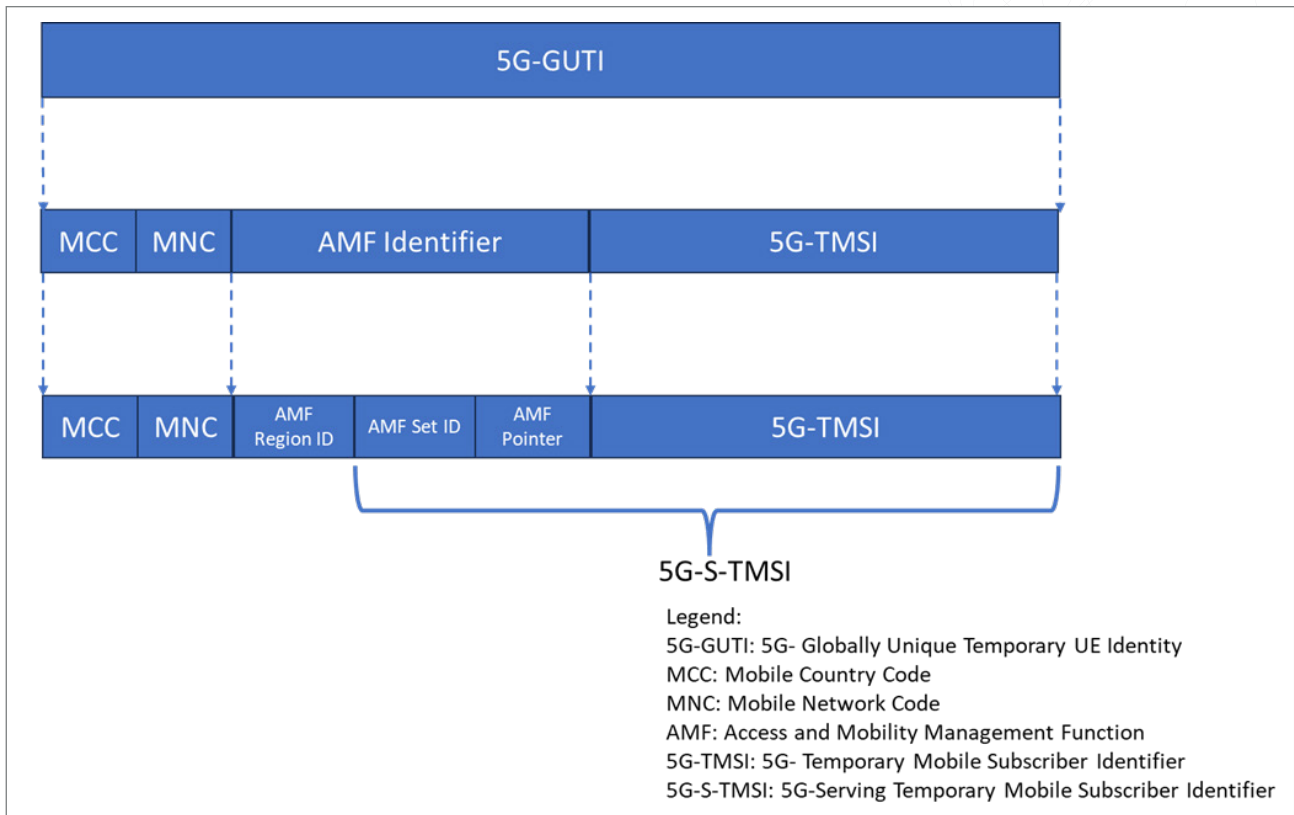


Figure 4. 5G-S-TMSI structure

## Summary

5G standards have mitigated the UE paging-related cybersecurity and privacy risks of previous generations of cellular networks. The enhancement, which is referred to as “No SUPI-based paging” in this white paper, ensures that permanent or quasi-permanent IDs are not used in the 5G paging protocol. Network operators and organizations using 5G technologies are encouraged to understand this enhancement and expect that if a UE roams back from 5G to a previous generation system, these new protections may not be available.

## Additional Technical Details

The rest of this white paper is intended for readers seeking more in-depth knowledge of “no SUPI-based paging” functionality.

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

## How mobile operators can validate their “no SUPI-based paging”

The mobile operators must make sure that their deployments are validated against the UE paging protocol described in the 3GPP standards (Release 15+).

## Confirming that “no SUPI-based paging” is occurring as expected

For this project, the NCCoE 5G demonstration network was configured to emulate some scenarios where paging was triggered at the core network. Protection was verified by using network taps and tools to look at the contents of specific protocol messages flowing across different interfaces. The overall scenario is as described below (see Figure 5). This is an example sequence of different scenarios triggered during our lab test; however, these could be independently triggered in another order. Note that for brevity, the message sequence chart omits some intermediate steps like mutual authentication and key agreement between the UE and core network. It also skips showing the intermediate Radio Resource Control (RRC) connection establishment/release between the UE and the RAN node, i.e., gNB (the RRC connection is needed to transport the messages between the UE and core network via the RAN). Also, multiple instances of the same scenario are shown only once. The term “Temporary ID” is used to imply either 5G-GUTI or 5G-S-TMSI, depending on the procedure.

- Step 1: The UE (Samsung S22) camps (does cell selection) on gNB.
- Steps 2 - 3: UE does “initial registration” with the core network via gNB. It uses the encrypted version of SUPI, namely SUCI, in the registration request. A Temporary ID is allocated by AMF and provided to the UE.
- Steps 4 - 6: At the expiry of the periodic registration update timer at UE, it does another registration. This time the type of registration is “periodic registration updating” and the Temporary ID is used for identification. A new Temporary ID is allocated by AMF and provided to the UE.
- Steps 7 - 9: Some UE application triggers uplink data activity. The UE sends a “High priority access” Service Request to the core. A new Temporary ID is allocated by AMF and provided to the UE.
- Steps 10 - 13: Due to a mobile terminated service (like incoming call), paging is required by the core network. The AMF pages the UE via gNB. The UE responds to paging with a “Mobile terminated services” Service Request. A new Temporary ID is allocated by AMF and provided to the UE.



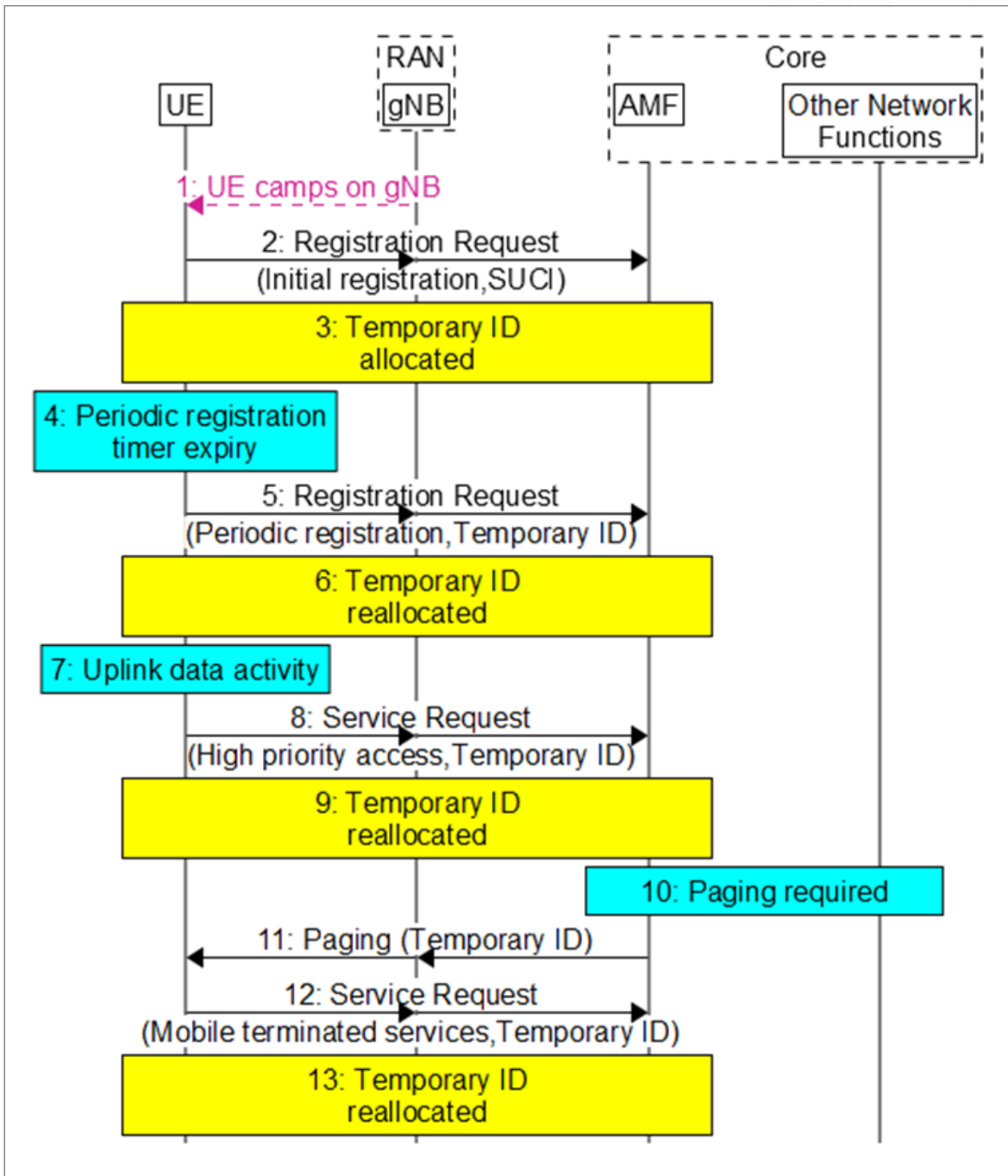



Figure 5. Paging scenario

Figure 6 shows the packet log captured with Wireshark at gNB. The timestamps 163.13 – 163.66s correspond to steps 2 – 3 (initial registration). Steps 4 – 6 (periodic registration) correspond to the timestamps 944.90 – 944.91s. Steps 7 – 9 (service request) correspond to the timestamps 1006.2 – 1006.4s. Finally, steps 10 – 13 (paging) correspond to the timestamps 1125.4 – 1126.2s. The last column shows the 5G-TMSI value used in the corresponding transaction. A value change from the previous rows indicates the temporary ID reallocation. Notice that here the temporary IDs are sequential because we have a single UE connecting to the lab network. However, in practice the reallocated values for a specific UE will be difficult to track because hundreds of UEs are connecting to the live network randomly and these values are distributed among them.

Time	Source	Destin	procedureCode	Message type	Registration or service type	Type of identity	5G-TMSI
163.13...	gNB	AMF	id-InitialUEMessage	Registration request	initial registration	SUCI	
163.34...	gNB	AMF	id-UplinkNASTransport	Security mode complete, Regi...	initial registration	SUCI	
163.65...	AMF	gNB	id-DownlinkNASTransport	Registration accept		5G-GUTI	3250586114
163.66...	AMF	gNB	id-DownlinkNASTransport	Configuration update command			
944.90...	gNB	AMF	id-InitialUEMessage	Registration request, Regist...	periodic registration upda...	5G-GUTI, 5G-...	3250586114
944.91...	AMF	gNB	id-DownlinkNASTransport	Registration accept		5G-GUTI	3250586115
1006.2...	gNB	AMF	id-InitialUEMessage	Service request, Service req...	High priority access, High ...	5G-S-TMSI, 5...	3250586115
1006.2...	AMF	gNB	id-InitialContextSetup	Service accept			
1006.4...	AMF	gNB	id-DownlinkNASTransport	Configuration update command		5G-GUTI	3250586116
1125.4...	AMF	gNB	id-Paging			fiveG-S-TMSI	3250586116
1126.1...	gNB	AMF	id-InitialUEMessage	Service request, Service req...	Mobile terminated services...	5G-S-TMSI, 5...	3250586116
1126.1...	AMF	gNB	id-InitialContextSetup	Service accept			
1126.2...	AMF	gNB	id-DownlinkNASTransport	Configuration update command		5G-GUTI	3250586117

Figure 6. Wireshark packet log at gNB



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

Karen Scarfone: 0000-0001-6334-9486

Murugiah Souppaya: 0000-0002-8055-8527

### **How to Cite this NIST Technical Series Publication:**

Bartock M. et al. (2025) No SUPI-Based Paging: Applying 5G Cybersecurity and Privacy Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 36D ipd.

<https://doi.org/10.6028/NIST.CSWP.36D.ipd>

### **Public Comment Period**

January 30, 2025 - February 28, 2025

### **Submit Comments**

[5g-security@nist.gov](mailto: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).**