NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Check for updates

Reallocation of Temporary Identities:

Applying 5G Cybersecurity and Privacy Capabilities

NIST Cybersecurity White Paper

NIST CSWP 36C ipd

Michael Bartock

Jeffrey Cichonski

Murugiah Souppaya

Information Technology Laboratory

Karen Scarfone

Scarfone Cybersecurity

Parisa Grayeli

Sanjeev Sharma

The MITRE Corporation

November 2024

Initial Public Draft

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

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 project at the National Cybersecurity Center of Excellence (NCCoE). This white paper provides additional details regarding how 5G protects subscriber identities (IDs). It focuses on how the network reallocates temporary IDs to protect users from being identified and located by an attacker. Unlike previous generations of cellular systems, new requirements in 5G explicitly define when the temporary ID must be reallocated (refreshed). 5G network operators should be aware of how this standards-defined security capability protects their users and subscribers. Operators should ensure that their 5G technologies are refreshing temporary identities as described in the 5G standards.

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, privacy, reallocation of temporary identities (IDs), Subscription Concealed Identifier (SUCI), Subscription Permanent Identifier (SUPI), Globally Unique Temporary user equipment Identity (GUTI)

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

5G networks don't 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. The operator also stores the SUPI in the operator's subscriber database (UDM) as part of the provisioning of the subscriber's services. When a mobile device connects to a 5G network for the first time, it uses its SUPI to establish the connection. 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. All subsequent signaling communication between the network and the device leverages the temporary ID (5G-GUTI) instead of the permanent ID (SUPI).

What's the problem?

Changing or refreshing the temporary IDs with new values, also known as reallocation, supports user privacy by making it hard for malicious actors to track a specific device. In 4G networks, operators chose the frequency of reallocating devices' temporary IDs (GUTIs). It was subsequently discovered that many networks did not refresh the temporary IDs often enough, which caused them to become quasi-permanent.[1] This led to increased cybersecurity and privacy risks for 3G and 4G network subscribers.[2] For example, a malicious actor could passively collect GUTIs and use them for verifying a subscriber's presence in a certain area or for revealing their past movements in that area and enabling tracking of their future movements.[3,4] Tracking subscriber movement can result in subscriber loss of trust in the networks and related consequences for an operator (e.g., loss of reputation).

[1] 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

[2] Locate UE: 5G-GUTI reuse. https://fight.mitre.org/techniques/FGT5012.003

[3] A. Shaik et al., "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," NDSS '16, San Diego, California, February 21-24, 2016. Available: https://arxiv.org/pdf/1510.07563.pdf

[4] 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

How do the 5G standards address the problem?

The 5G standards starting with 3GPP release 15 in 2019 require all 5G networks to reallocate 5G-GUTIs often. It's no longer completely left up to individual operators to determine and implement an appropriate frequency; it's mandatory to reallocate the 5G-GUTI based on certain events associated with a specific user. The reallocation process of 5G-GUTIs decreases the link between a subscriber and their phone's identifiers, which makes the tracking of the subscriber's movements more difficult and protects the subscriber's activities from exposure.[5] This increases the overall privacy protections in the system by supporting the objective of disassociability.

Figure 1 is a simplified version of the 5G architecture that shows the components involved in 5G-GUTI allocation (from a SUPI context) and reallocation (from a 5G-GUTI context), 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. Note that SUPI is encrypted into a Subscription Concealed Identifier (SUCI) while it is signaled from the UE to CN[6]. During initial registration and authentication, the Access and Mobility Management Function (AMF), Authentication Server Function (AUSF), and Unified Data Management (UDM) are involved in SUCI to SUPI translation. The AMF sets up a local 5G-GUTI to SUPI context during the full authentication procedure (shown as [SUPI context] in figure). Afterwards, the 5G-GUTI reallocations are managed by AMF (also called serving AMF).

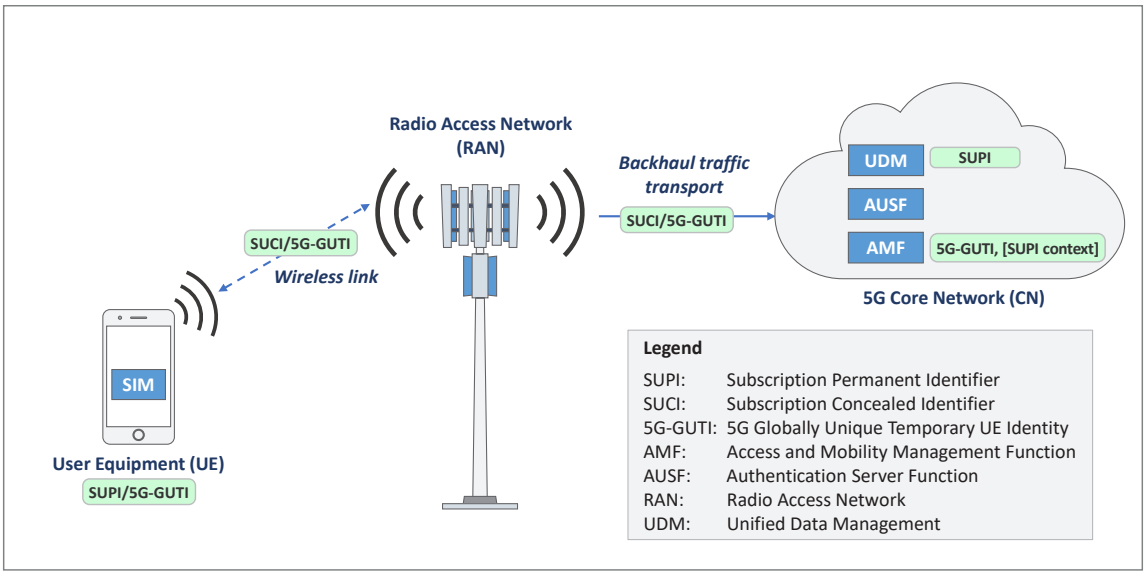

Figure 1. 5G architecture components involved in the temporary ID reallocation capability

[5] The NIST "Catalogue of Problematic Data Actions and Problems" provides examples of problematic data actions and problems that individuals could experience as the result of data processing or their interactions with systems, products, or services. This catalogue describes surveillance, induced disclosure, and loss of trust.

[6] Bartock M. et al. (2024) "Protecting Subscriber Identifiers with Subscription Concealed Identifier." Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.36A.ipd.pdf

How can I use reallocation of temporary IDs?

5G network functions compliant with 3GPP release 15 or later are required to support the mandatory reallocation of the 5G-GUTI based on certain events associated with a specific user: paging, initial registration, and mobility registration update procedures. The network can be configured to also allocate a new 5G-GUTI after each service request and the periodic registration update of the UE.

Network operators are encouraged to coordinate with their 5G equipment vendors to verify that the 5G-GUTIs in their network are reallocated when one of the above-mentioned scenarios occurs.

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 5G-GUTIs are reallocated as expected.

What else should I know about reallocation of temporary IDs?

Figure 2 shows all of the subscriber or UE related identities. The 5G-GUTI is assigned and maintained by the serving AMF, which may or may not be in the subscriber's home network (i.e. UE may be in a visited network in roaming cases). The 5G-GUTI consists of the identity of the mobile user's home network, i.e., Mobile Country Code (MCC) and Mobile Network Code (MNC), the AMF Identifier, and the 5G-Temporary Mobile Subscriber Identity (5G-TMSI). For completeness, it also shows a permanent identifier associated with the mobile handset itself called the International Mobile station Equipment Identity (IMEI), which may be used to make emergency calls if the SIM is not available.

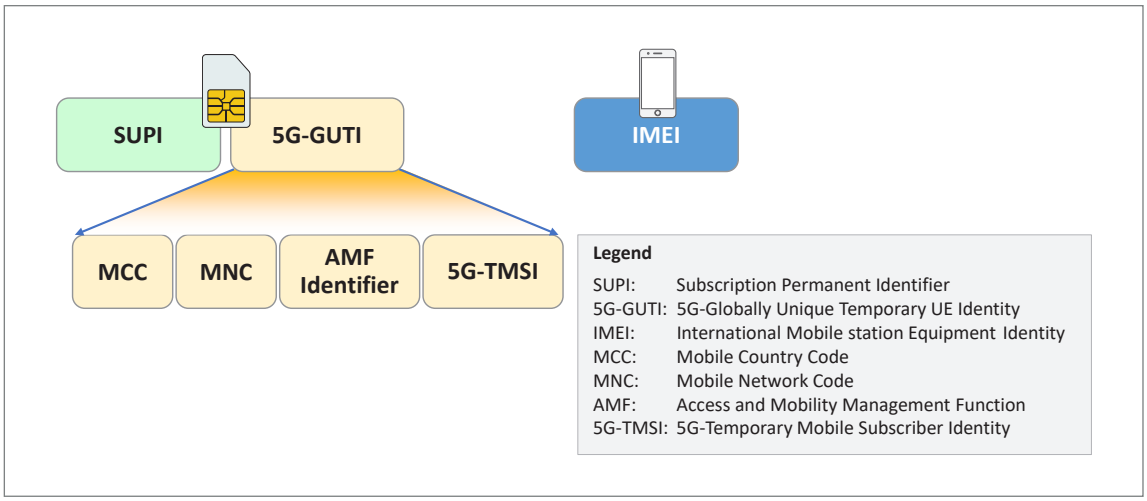

Figure 2: Subscriber or UE related identities

Each time a 5G-GUTI is assigned, the new 5G-GUTI is stored in non-volatile memory in the SIM if possible, else in the non-volatile memory in the mobile device. This means the 5G-GUTI will be retained even if the UE is turned off or switched to airplane mode.

The next time the UE turns on, it may be in a new geographic location, even another country. The user's home network may not be available in the new location. In this case, the UE may try to connect to a visited network for service. Since each 5G-GUTI is globally unique, the UE can still attempt to identify itself in the visited network using its 5G-GUTI. If the visited network cannot recognize the UE (i.e., it cannot retrieve the UE's SUPI within its local context because old 5G-GUTI was assigned by a different AMF), a full authentication with the permanent ID SUPI/SUCI is required. In some cases like lack of roaming agreement between visited and home network, the connection may be refused by the visited network. This results in the UE deleting its stored 5G-GUTI. Note that there is no timer on the UE side to delete the 5G-GUTI.

Summary

Previous generations of cellular systems sought to avoid subscriber tracking issues by using temporary UE IDs. However, because of the lack of uniform rules around refreshing those IDs, they remained quasi-permanent in some networks — leaving their subscribers vulnerable to cybersecurity and privacy risks. This paper explains how 5G systems have mitigated this problem. A 5G-GUTI is required to be reallocated on the occurrence of certain events associated with a specific user: paging, initial registration, and mobility registration update procedures. The network can be configured to also allocate a new 5G-GUTI after each service request and the periodic registration update of the UE.

Technical Details of Reallocation of Temporary IDs

The rest of this white paper is intended for readers seeking more in-depth knowledge of reallocation of temporary IDs 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 reallocation of temporary IDs

Mobile operators should make sure that their deployments are validated against the mandatory 5G-GUTI reallocation use-cases described in the 3GPP standards (Release 15+)[7]. Some of these use-cases are detailed in the next section. Deployment configurations simply generated from pre-5G operator-specific rules will likely fail this validation.

Confirming that reallocation of temporary IDs is occurring as expected

For this project, the NCCoE 5G demonstration network was used to emulate the following scenarios. The temporary IDs must be reallocated in these scenarios:

a) During a successful initial registration procedure

b) During a successful registration procedure for mobility registration update

c) After a successful service request procedure invoked as a response to a paging request from the network and before the release of the N1 NAS signaling connection

It is also recommended to reallocate the temporary ID:

d) During a successful registration procedure for periodic registration update

Protection was verified by using taps and tools to look at the contents of specific protocol messages flowing across different interfaces.

We divided the scenarios mentioned above into two experiments. The first experiment covers scenarios a) and d). The second experiment covers scenarios a), b), and c).

We have two RAN nodes connected to the core network in our lab. Each RAN node comprises the radio, baseband unit, antenna, and radio resource controller (among other components such as scheduler and transport network communications support). We label these two nodes as gNB1 and gNB2.

[7] See 3GPP TS 24.501, section 5.3.3

The first experiment to cover scenarios a) and d) involves a single RAN node, i.e., gNB2 and is described below (see Figure 3):

- Step 1: The UE (Samsung S22) camps (does cell selection) on gNB2.
- Steps 2 - 5: A Radio Resource Control (RRC) connection is needed to transport the messages between the UE and core network via RAN. First the RRC connection is established between the UE and gNB2. Then the UE does "initial registration" with the core network via gNB2. The UE starts from a condition where no Temporary ID was allocated to it, and it uses the encrypted version of SUPI i.e. SUCI in the registration request. A Temporary ID is allocated by the AMF and provided to the UE. After some time, the RRC connection between gNB2 and UE is released.
- Steps 6 - 10: At the expiry of the periodic registration update timer at UE, an RRC connection is established again between the UE and gNB2. The UE does another registration with the type of registration as "periodic registration updating" and the previously allocated Temporary ID is used for identification. The Temporary ID is reallocated by AMF and provided to the UE. After some time, the RRC connection between gNB2 and UE is released.

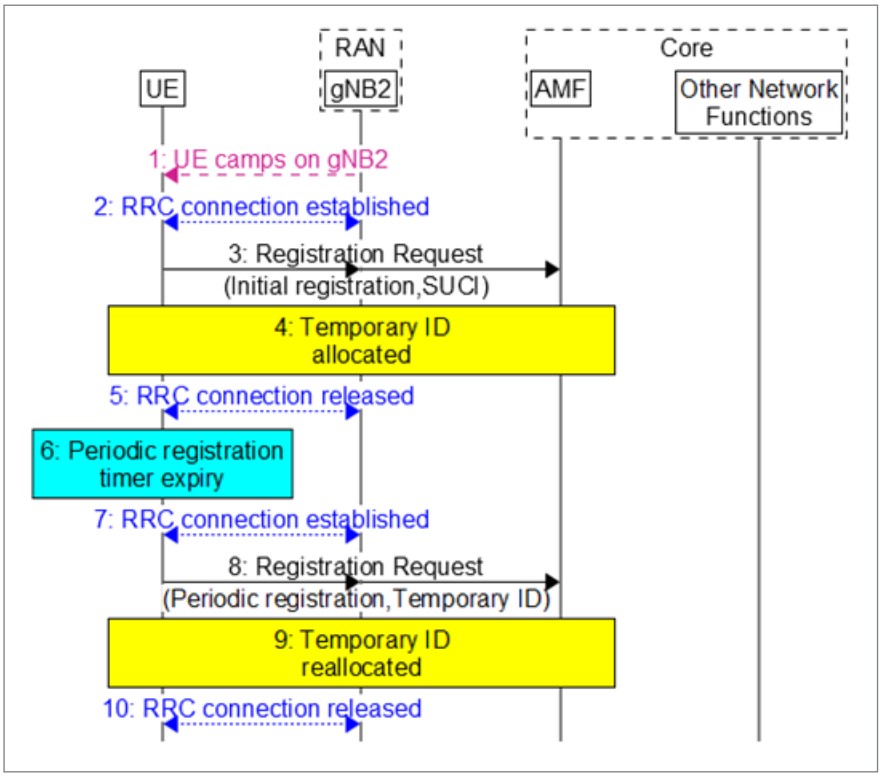

Figure 3. First experiment: scenarios a) and d)

The corresponding Wireshark packet log is shown in Figure 4. The second-to-last column shows the type of identity used in the registration request. 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 apparently 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 get distributed among them.

Time	Source	Destin	procedureCode	Message type	Registration or service type	Type of id	5G-TMSI
163.13…	gNB2	AMF	id-InitialUEMessage	Registration request	initial registration	SUCI	
163.34…	gNB2	AMF	id-UplinkNASTransport	Security mode complete,Regi…	initial registration	SUCI	
163.65…	AMF	gNB2	id-DownlinkNASTransport	Registration accept		5G-GUTI	3250586114
163.66…	AMF	gNB2	id-DownlinkNASTransport	Configuration update command			
944.90…	gNB2	AMF	id-InitialUEMessage	Registration request,Regist…	periodic registratio…	5G-GUT…	3250586114
944.91…	AMF	gNB2	id-DownlinkNASTransport	Registration accept		5G-GUTI	3250586115

Figure 4. Wireshark packet log at gNB2

The second experiment involves two RAN nodes, i.e., gNB1 and gNB2, and is as described below (see Figure 5). This is an example sequence of various scenarios triggered during our lab test; however, these could be independently triggered in another order. Note that for brevity, the messages sequence chart skips showing some intermediate steps like mutual authentication and key agreement between the UE and core network. Also, multiple instances of the same scenario are shown only once.

- Steps 1 - 3: gNB1 is locked (radio turned on) and gNB2 is unlocked (radio turned off). The UE (Samsung S22) camps (does cell selection) on gNB2.
- Steps 4 - 7: An RRC connection is established between the UE and gNB2. UE does “initial registration” with the core network via gNB2 with the previously saved Temporary ID. The Temporary ID is reallocated by AMF and provided to the UE. After some time, the RRC connection between gNB2 and UE is released.
- Steps 8 - 13: The core network pages the UE via gNB2. An RRC connection is established between the UE and gNB2, and the UE responds to paging with a “Mobile terminated services” Service Request. The Temporary ID is reallocated by AMF and provided to the UE. After some time, the RRC connection between gNB2 and UE is released.
- Steps 14 - 18: Some UE application triggers uplink data activity. An RRC connection is established between the UE and gNB2, and the UE sends a “High priority access” Service Request to the core. The Temporary ID is reallocated by AMF and provided to the UE. After some time, the RRC connection between gNB2 and UE is released.
- Steps 19 - 21: gNB2 is locked. The core network tries to page the UE via gNB2, but gNB2 cannot transmit the pages to UE. As a result, UE does not respond to multiple paging requests.
- Steps 22 - 23: gNB1 is unlocked and UE reselects to gNB1.
- Steps 24 - 27: Some UE application triggers uplink data activity. An RRC connection is established between the UE and gNB1 and the UE sends a “High priority access” Service Request to the core. The Temporary ID is reallocated by AMF and provided to the UE. Notice that UE does not do a registration (“mobility registration updating”) because gNB1 and gNB2 share the same tracking area.
- Steps 28 - 29: gNB1 is locked before the RRC connection between gNB1 and UE is released. The UE experiences RRC connection failure.
- Steps 30 - 31: gNB2 is unlocked and UE reselects back to gNB2.
- Steps 32 - 35: An RRC connection is established between the UE and gNB2. UE does registration (“mobility registration updating”) with the core network via gNB2, because of the earlier RRC connection failure at gNB1. The Temporary ID is reallocated by AMF and provided to the UE. After some time, the RRC connection between gNB2 and UE is released.

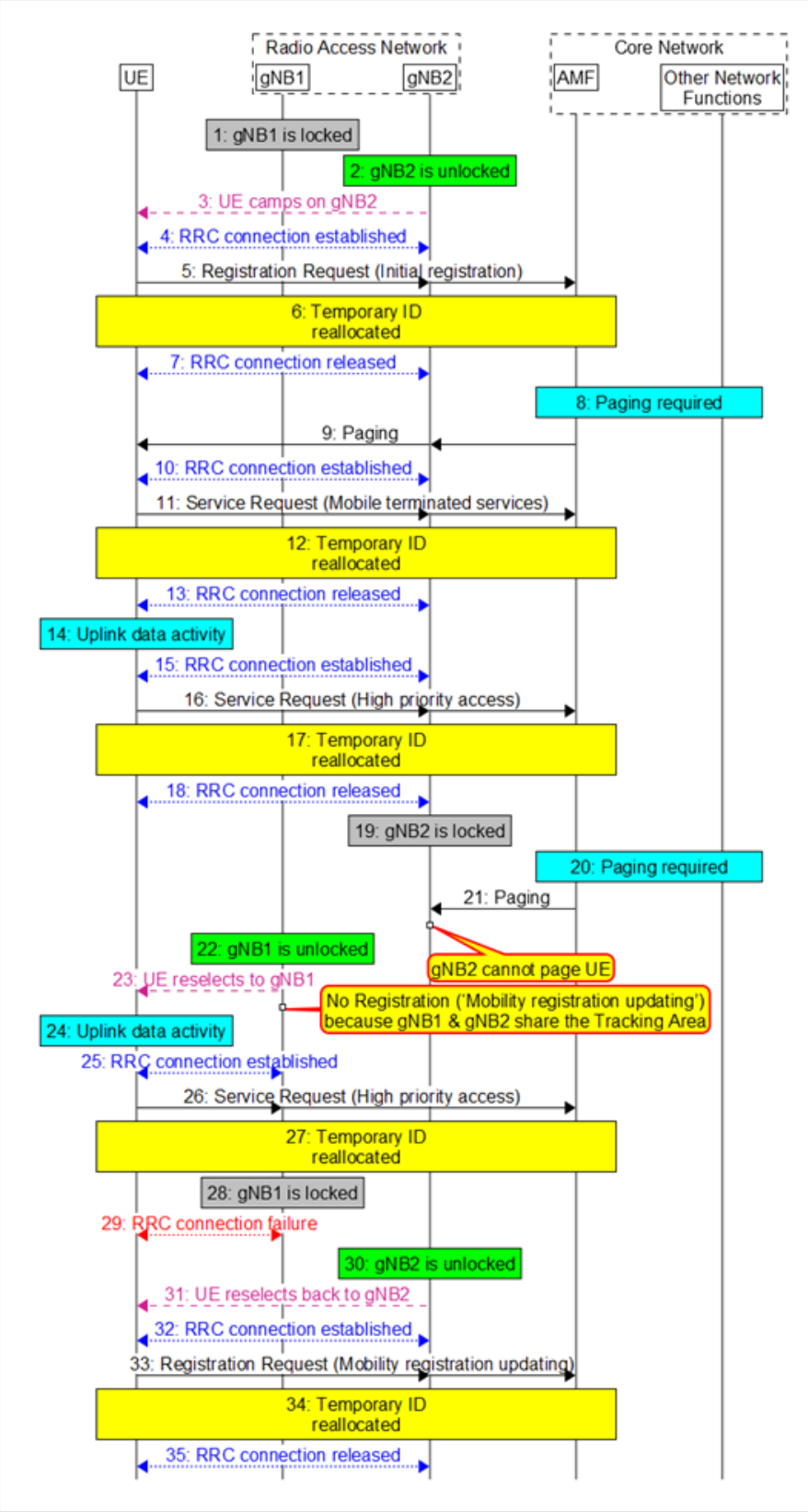

Figure 5. Second experiment: scenarios a), b), and c)

Figure 6 shows the packet log captured with Wireshark at gNB2. Likewise, Figure 7 shows the packet log captured with Wireshark at gNB1. From these two logs, it can be seen that the UE is camped with gNB2 between timestamps 165.16 – 400.78s. It loses coverage from timestamps 534.21 – 639s, when it cannot be paged. Then it is camped with gNB1 from timestamps 639.68 – 703.28s. Eventually it reselects back to gNB2 around timestamp 854.94s. 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 apparently 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 get distributed among them.

Time	Source	Destin	procedureCode	Message type	Registration or service type	5G-TMSI
165.16…	gNB2	AMF	id-InitialUEMessage	Registration request,Regist…	initial registration,initi…	3267362902
165.36…	AMF	gNB2	id-DownlinkNASTransport	Registration accept		3267362904
165.37…	AMF	gNB2	id-DownlinkNASTransport	Configuration update command		
282.56…	AMF	gNB2	id-Paging			3267362904
283.29…	gNB2	AMF	id-InitialUEMessage	Service request,Service req…	Mobile terminated services…	3267362904
283.29…	AMF	gNB2	id-InitialContextSetup	Service accept		
283.40…	AMF	gNB2	id-DownlinkNASTransport	Configuration update command		3267362905
400.66…	gNB2	AMF	id-InitialUEMessage	Service request,Service req…	High priority access,High …	3267362905
400.67…	AMF	gNB2	id-InitialContextSetup	Service accept		
400.78…	AMF	gNB2	id-DownlinkNASTransport	Configuration update command		3267362906
534.21…	AMF	gNB2	id-Paging			3267362906
541.29…	AMF	gNB2	id-Paging			3267362906
548.26…	AMF	gNB2	id-Paging			3267362906
555.39…	AMF	gNB2	id-Paging			3267362906
562.54…	AMF	gNB2	id-Paging			3267362906
576.88…	AMF	gNB2	id-Paging			3267362906
591.28…	AMF	gNB2	id-Paging			3267362906
605.24…	AMF	gNB2	id-Paging			3267362906
641.11…	AMF	gNB2	id-Paging			3267362906
648.30…	AMF	gNB2	id-Paging			3267362906
854.94…	gNB2	AMF	id-InitialUEMessage	Registration request,Regist…	mobility registration upda…	3267362908
855.06…	AMF	gNB2	id-InitialContextSetup	Registration accept		3267362909

Figure 6. Wireshark packet log at gNB2

Time	Source	Destin	procedureCode	Message type	Registration or service type	5G-TMSI
639.68…	gNB1	AMF	id-InitialUEMessage	Service request,Service req…	High priority access…	3267362906
639.74…	AMF	gNB1	id-InitialContextSetup	Service accept		
639.83…	AMF	gNB1	id-DownlinkNASTransport	Configuration update command		3267362907
703.14…	gNB1	AMF	id-InitialUEMessage	Service request,Service req…	High priority access…	3267362907
703.15…	AMF	gNB1	id-InitialContextSetup	Service accept		
703.28…	AMF	gNB1	id-DownlinkNASTransport	Configuration update command		3267362908

Figure 7. Wireshark packet log at gNB1

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. (2024) Reallocation of Temporary Identities: Applying 5G Cybersecurity and Privacy Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 36C ipd. https://doi.org/10.6028/NIST.CSWP.36C.ipd

Public Comment Period

November 6, 2024 - December 6, 2024

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).

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE