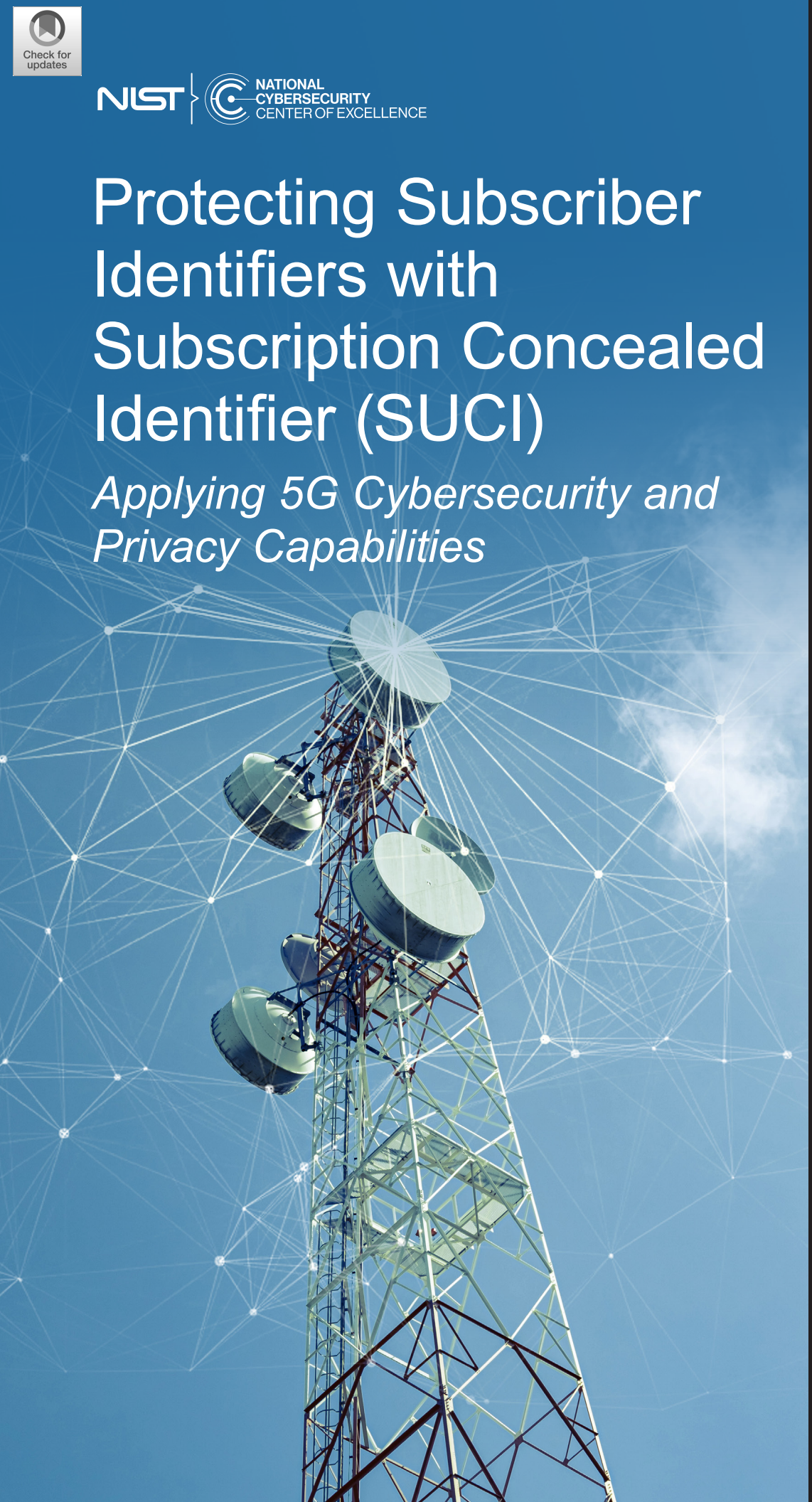
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Protecting Subscriber Identifiers with Subscription Concealed Identifier (SUCI)

Applying 5G Cybersecurity and Privacy Capabilities



NIST Cybersecurity White Paper

NIST CSWP 36A

Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya *
Information Technology Laboratory

Karen Kent
Trusted Cyber Annex

Parisa Grayeli
Sanjeev Sharma
Charles Teague *
The MITRE Corporation

**Former employee; all work for this publication was done while at that organization*

March 2026
Final

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

Abstract

This white paper describes how Subscription Concealed Identifier (SUCI) protection can be enabled in 5G networks. SUCI protection is defined by 5G standards as an optional security capability for operator deployments. Although it is optional, it provides important security and privacy protections for subscriber identifiers. By enabling SUCI on their 5G networks and subscriber SIMs, and configuring SUCI to use a non-null encryption cipher scheme, 5G network operators can provide their customers with the advantages of SUCI's protections. The network operators should carefully evaluate the risks of not enabling this critical capability. 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 demonstrated and verified on the National Cybersecurity Center of Excellence (NCCoE)'s 5G Cybersecurity testbed.

Audience

Technology, cybersecurity, and privacy professionals who are involved in using, managing, or providing 5G-enabled services and products. This includes potential private 5G network operators, commercial mobile 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, Subscription Concealed Identifier (SUCI), Subscription Permanent Identifier (SUPI)

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, Kori Rongey, Steve Vetter *

Dell Technologies: Dan Carroll

Intel Corporation: Steve Orrin

Keysight Technologies: Corey Piggott

MiTAC Computing Technology Corp.: Simon Hwang

The MITRE Corporation: Sallie Edwards *, John Kent, Mary Raguso *, Theresa Suloway

NIST: Cherilyn Pascoe, Adam Sedgewick *, Kevin Stine

Nokia: Gary Atkinson, Rajasekhar Bodanki, Robert Cranston, Jorge Escobar, Don McBride

Palo Alto Networks: Aarin Buskirk, Bryan Wenger

T-Mobile: Todd Gibson

** Former employee; all work for this publication was done while at that organization*

Overview

5G networks don't associate users by their names; instead, users are managed by their subscription information and are often called subscribers. Networks use a permanent identifier called the Subscription Permanent Identifier (SUPI) that is associated with each user's subscription. The SUPI is written into the Subscriber Identity Module (SIM), which is implemented as either a physical Universal Integrated Circuit Card (UICC) or an embedded SIM (eSIM). Since 3G days, these modules have evolved to support more secure features which are implemented as the Universal Subscriber Identity Module (USIM) application. SUPI is the 5G equivalent of 4G's IMSI, short for International Mobile Subscriber Identity.

What's the problem?

Without additional protections in place, the SUPI will be sent in the clear over the air from the subscriber's device to the cell tower. This process would allow eavesdroppers to intercept and use it to track the subscriber's location, which can lead to correlation of movement and may pose as a cybersecurity risk to organizations as well as a privacy risk to individuals. If subscribers' identities are exploited in this manner, it can result in subscriber loss of trust in cellular networks and related consequences for operators (e.g., loss of reputation).[1] This isn't a new issue; the same risk of capturing subscriber identifiers exists in 4G systems and is known as ***IMSI catching***. Mobile handsets will attach to whichever base station is broadcasting as their preferred carrier network and is transmitting at the highest power level. A rogue base station[2] that is broadcasting at a higher power than a legitimate base station may trick a handset into attempting to connect to its malicious network, potentially sending the SUPI in clear text.

How does SUCI address the problem?

Starting with 3GPP release 15 in 2019, 5G standards support an optional feature that encrypts the SUPI with the public key of the home operator to create the ***Subscription Concealed Identifier (SUCI)***. The SUCI is a ciphered version of the subscriber's identity that is always unique; when this ciphered identity is used, an attacker can't correlate it to the subscriber. The SUCI is calculated by the mobile device or SIM using elliptic curve cryptography. The SUCI is then sent over the air instead of the SUPI, so that only the Unified Data Management (UDM) for the subscriber's network operator, which has access to the corresponding private key, can decrypt the identifier and know which subscriber is associated with it. Without using this optional 5G feature, the SUPI is sent in the clear [1].

Figure 1 shows a simplified version of the 5G architecture that highlights the architectural components involved in SUCI, with all other components omitted. When the SUCI is used instead of the SUPI, the components shown are the primary elements involved in its operation.

[1] The NIST "Catalogue of Problematic Data Actions and Problems" provides additional 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, and describes surveillance, induced disclosure, and loss of trust. Available: https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk- assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md

[2] The Electronic Frontier Foundation (EFF) provides in-depth technical details on how these rogue base stations operate. https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks.

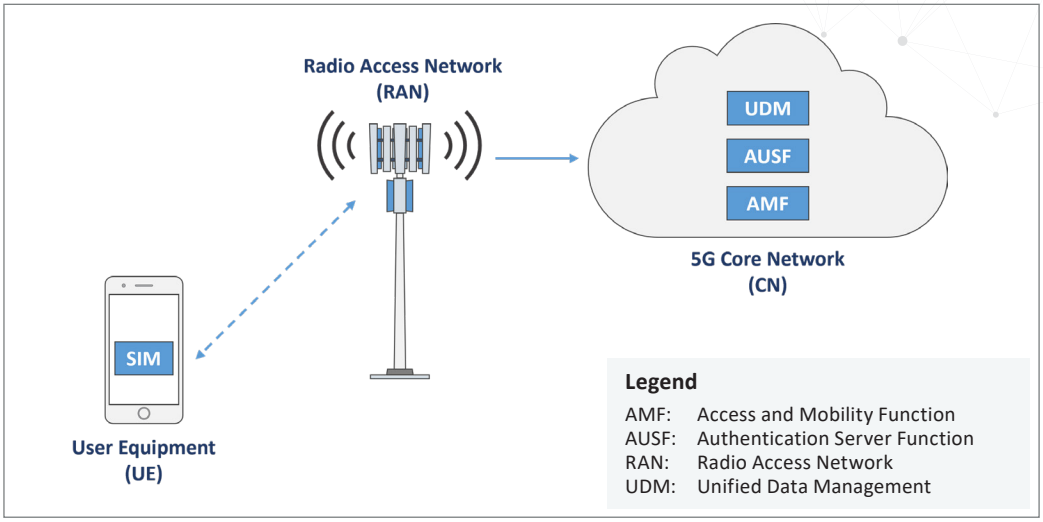


Figure 1. 5G architecture components involved in the SUCI capability

How can I use SUCI?

5G devices and network functions compliant with 3GPP release 15 or later are required to support the SUCI security capability, but turning the capability on in 5G networks is optional for network operators. The SIM card being used in conjunction with the 5G device also needs to support SUCI calculation. If your 5G operator has enabled SUCI on their 5G network and on your SIM, SUCI will be used automatically when you connect to your 5G operator's network. If the SUCI is generated with a null encryption cipher scheme, the SUPI will not actually be encrypted, so it is necessary for an operator to configure their network with a valid non-null protection scheme when enabling SUCI.

In addition, the Federal Communications Commission (FCC) has published recommendations that network operators configure networks to use "non-null" ciphers to conceal subscribers' personal identifiers whenever possible. The FCC Communications Security, Reliability, and Interoperability Council (CSRIC) comprises a group of industry and government advisors to the FCC focusing on security and reliability for communications systems in the U.S. A 2021 report [2] from CSRIC recommends that U.S. operators use the SUCI capability and do not use a null encryption scheme except when the 5G device is unknown to the operator and is requesting emergency services.

To confirm SUCI protection is enabled, the following should be verified:

- Network operators confirm that their 5G equipment vendors support SUCI.
- SUCI is enabled on the operator's 5G networks.
- SUCI information is available on the subscribers' SIMs.
- SUCI is configured to use a non-null encryption cipher scheme.

What else should I know about SUCI?

SUCI only protects 5G subscriber information when connecting to 5G networks; it does not offer any protection when devices are connected to previous generations of networks, such as 4G LTE.

In some scenarios, like visiting another country, also known as roaming, the 5G device may have to gain radio access via the visited network having a roaming agreement with the user's home network. The visited network may only be supporting the null protection scheme for its subscribers, which is a security concern. However, the UDM function of the roaming subscriber resides in the subscriber's home network. Its SUCI is transferred from the visited network to the home network for de-concealment, and the home network proceeds with the access authorization. This ensures that the subscriber identity remains protected in the normal roaming case, independent of the visited network's capabilities.

However, as seen in Figure 2, SUCI always includes the subscriber's network operator and country information (i.e., Home Network Identifier) in clear text, even when the permanent identifier is encrypted. These clear text information elements are used as routing information and can validate subscribers' access eligibility. In this roaming scenario, these identifiers could be used by an adversary in detecting an outlier among other subscribers' network identifiers [3].

In addition, under emergency conditions, a subscriber may have to gain access via a visited network, domestic or international, that does not have a roaming agreement with the subscriber's home network. The FCC regulations require completion of emergency (9-1-1) calls from unauthenticated devices [2]. The cause of such an emergency request is explicitly tagged by the device so that the visited network can bypass the access authorization. In this case, the device may reveal the SUPI to the visited network [4].

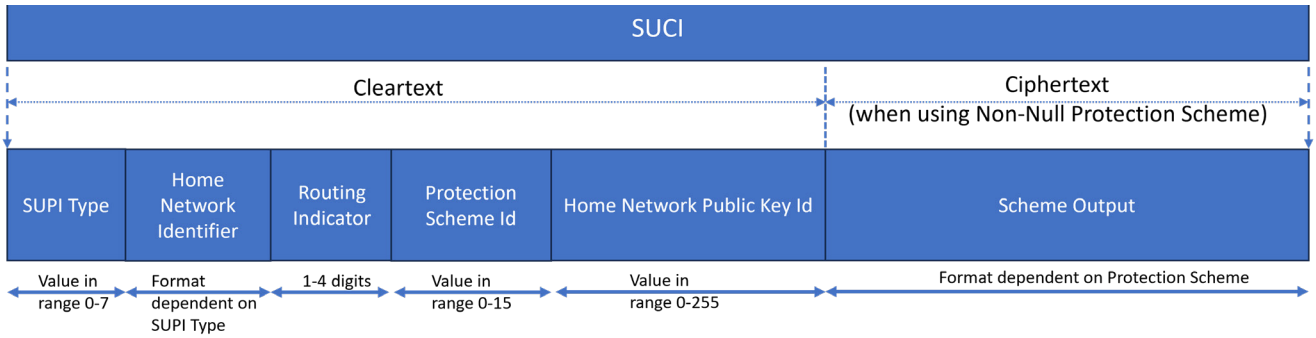


Figure 2: Structure of SUCI (adapted from 3GPP TS 23.003) [5]

Technical Details of SUCI Implementation and Use

The rest of this white paper is intended for readers seeking more in-depth knowledge of SUCI functionality. The technical information presented here is implemented and observed in the NCCoE 5G Cybersecurity testbed.

> 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 [6].

Encrypting the SUPI into the SUCI

The SUCI calculation procedure is based on the Elliptic Curve Integrated Encryption Scheme (ECIES) [7] as described in 3GPP TS 33.501. 5G standards currently define two sets of ECIES parameters (referred to as protection schemes), Profile A and Profile B. Either Profile A or B can be used. However, Profile B is defined to use a curve and parameters consistent with recommendations found in NIST SP 800-56A [8]. Initially, the home network generates private-public key-pairs for various protection schemes. The private keys are retained by the home network and the public keys may (or may not) be provided to subscribers via a pre-provisioned SIM or an over-the-air update. If multiple protection schemes are assigned to an individual subscriber, the operator may also assign the priorities for selection of these schemes.

Figure 3 shows how SUPI is encrypted into SUCI by the UE (the 5G device). When registering with the core network, the UE generates its own ephemeral public-private key pair. The private key is combined with the home network public key to derive an ephemeral shared key. This shared key is then used to derive keys for encryption and integrity protection. The plaintext block (hexadecimal digits for IMSI or octet string for NSI) is then encrypted into ciphertext. The ciphertext is fed into the integrity function and the MAC-tag [9] value is calculated. The final scheme output consists of ephemeral public key, ciphertext, and MAC-tag concatenated together.

PROFILE B IS DEFINED TO USE A CURVE AND PARAMETERS CONSISTENT WITH RECOMMENDATIONS FOUND IN NIST SP 800-56A

There are different SUPI types defined for 5G systems:

- **International Mobile Subscription Identity (IMSI)**. When the SUPI is of type IMSI, the operator programs the IMSI in the SIM or eSIM. In this case, the public key is also stored in the USIM. The IMSI format consists of three identifiers: Mobile Country Code (MCC), Mobile Network Code (MNC), and Mobile Subscriber Identification Number (MSIN). During SUCI calculation, the part of the IMSI representing the subscription identifier MSIN is coded as hexadecimal digits using Packed Binary Coded Decimal (BCD) Coding [10] and used as the plaintext block in Figure 3. The MCC and MNC portions of the IMS remain clear text.
- **Network Specific Identifier (NSI).** When the SUPI is of type NSI, the subscription identifier part of the SUPI (which is a character string) is encoded to an octet string according to Unicode Transformation Format-8 (UTF-8) encoding [11] rules and used as the plaintext block in Figure 3.
- **Global Cable Identifier (GCI) and Global Line Identifier (GLI).** For GCI and GLI, the subscription identifier part of the SUPI (which is a character string) is encoded to an octet string according to UTF-8 encoding rules like the NSI case, but the encoding rules are slightly different for GCI and GLI.

Figure 3 shows how SUPI is encrypted into SUCI by the UE.

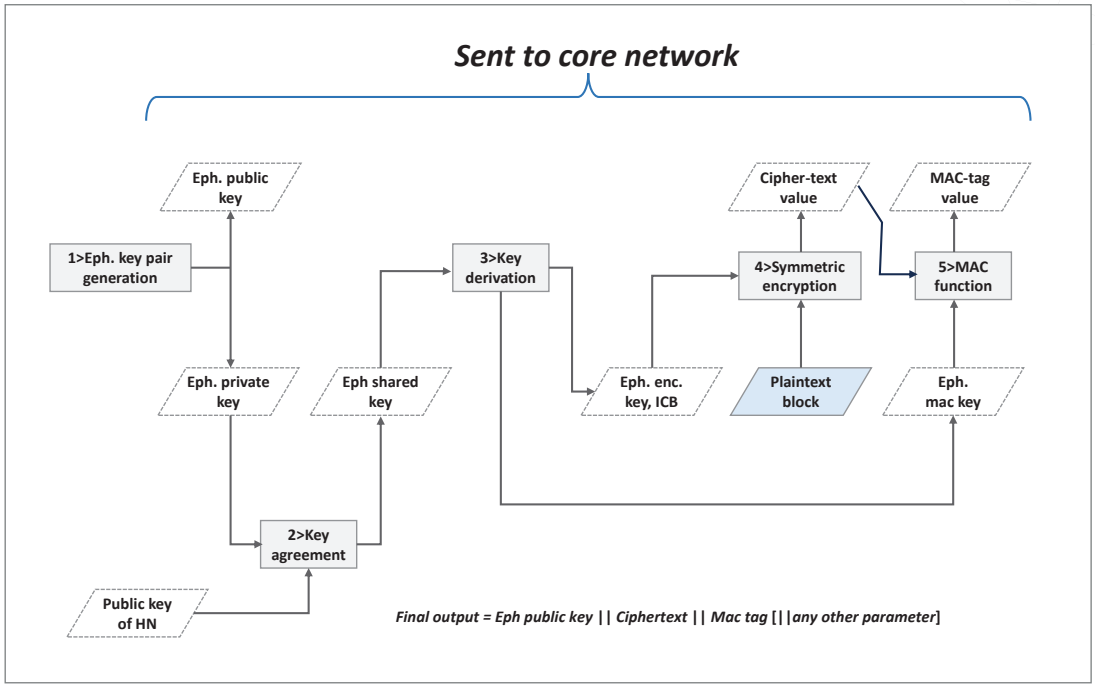


Figure 3: Encryption based on ECIES at UE (adapted from 3GPP TS 33.501, C.3.2-1) [12]

On the core network side, the received SUCI is decrypted back to SUPI as shown in Figure 4. The UDM network function offers the Subscription Identifier De-concealing Function (SIDF) service for this decryption.

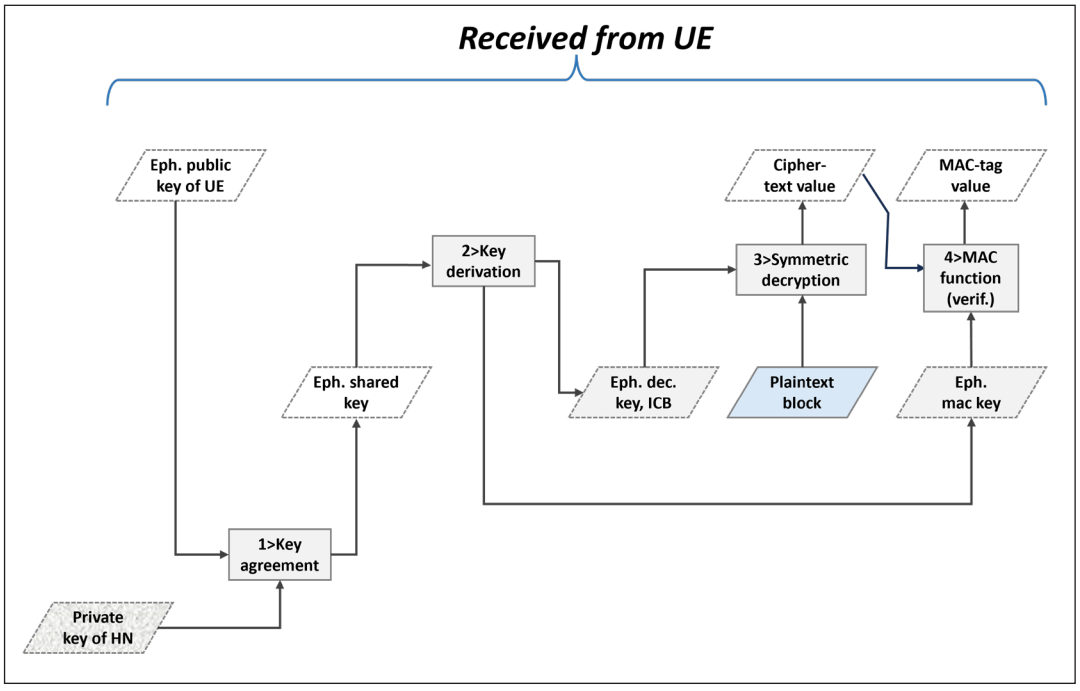


Figure 4: Decryption based on ECIES at home network (adapted from 3GPP TS 33.501, C.3.3-1) [12]

Configuration settings to enable SUCI

A mobile operator can control the SUCI feature at the individual subscriber level by configuring the following parameters for the USIM

- Set "Subscription Identifier Privacy Support" = True

- If USIM is capable of ECIES
  Set "SUCI calculation by the USIM" = "True"
  else
  Device will calculate it

- Configure USIM to use the following from list of protection schemes:
  0: Null 1: Profile A 2: Profile B

- Set the Priority of the protection schemes as Profile B, Profile A, Null

- Configure list of home network public keys:
  a. Home network public key identifier
  b. Actual value of the home network public key

Confirming that SUCI is enabled

For this project, the NCCoE confirmed that SUCI could be enabled, configured, and verified as operating correctly based on our implementation in the NCCoE's 5G testbed. Various SUCI configurations, including disabled, enabled with a null protection scheme, and enabled with a non-null protection scheme, were used for the NCCoE 5G demonstration network. Protection was verified by using network taps and mobile device testing tools to look at the contents of specific protocol messages flowing across different interfaces. We let the UE connect to the network and run data applications, while capturing the UE debug log using device testing tools. Messages showing the SUPI being encrypted into ciphertext would indicate that SUCI is enabled and working as expected.

As part of our analysis, we identified the applicable 5G messages from our network captures and debug logs. We examined the contents of the "Non-Access Stratum (NAS) Registration Request" message. As Figure 5 shows, the fields of interest were "Type of Identity" and "Protection Scheme ID" within the "5GS mobile identity" (IE) included in the "NAS Registration Request" message.

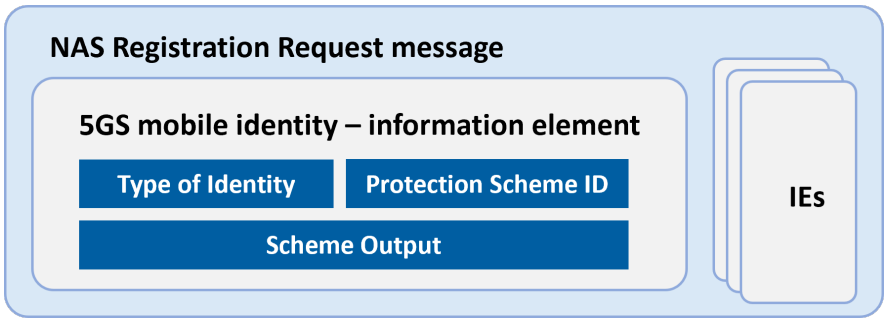


Figure 5: NAS Registration Request

Figure 6 shows a decoded part of the "NAS Registration Request" message for SUCI configurations, where USIM had "Subscription identifier privacy support" disabled (not Active); or enabled with a null protection scheme. In both these cases, because the null protection scheme is used, the SUPI (MSIN) can be seen as plaintext ("6200002012").

```
5GS mobile identity (hex data: 000d0100 f110f0ff 00002600 000221)
  Type of identity: SUCI
  SUPI format: IMSI
  MCC: 1
  MNC: 1
  Routing indicator digits: 0
  Protection scheme identifier: Null scheme
  Home network PKI: 0
  MSIN: 6200002012
```

Figure 6: Use of null protection scheme

Figure 7 shows the same part of the corresponding message from a different SUCI configuration, where USIM had "Subscription identifier privacy support" active and "Profile B" was set as the highest priority protection scheme. As the decoded message shows, the SUPI was encrypted into ciphertext (seen as the long hex data string in the first line of the excerpt). In this case, only the home network would be able to decrypt the SUCI back into the SUPI. This observation demonstrates the importance of using a non-null protection scheme for the actual subscription identity concealment.

```
5GS mobile identity (hex data: 00360100 f1100071 020c0336 8ab22d46 12506870
  Type of identity: SUCI
  SUPI format: IMSI
  MCC: 1
  MNC: 1
  Routing indicator digits: 0017
  Protection scheme identifier: ECIES scheme profile B
  Home network PKI: 12
```

Figure 7: Use of ECIES Profile B protection scheme

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] CSRIC VII (2021) Report on recommendations for identifying optional security features that can diminish the effectiveness of 5G security. Available at https://www.fcc.gov/file/20606/download

[3] MITRE Corporation (2024) *Subscriber Profile Identifier Discovery: Intercept Home Network Via SUCI.* Available at https://fight.mitre.org/techniques/FGT5019.001/

[4] MITRE Corporation (2024) *Subscriber Profile Identifier Discovery: Intercept Unencrypted SUPI*. Available at https://fight.mitre.org/techniques/FGT5019.004/

[5] 3rd Generation Partnership Project. Specification # 23.003: Numbering, addressing and identification. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729

[6] 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/5g-cybersecurity

[7] Certicom Research (2009) SEC 1: *Elliptic Curve Cryptography* (Standards for Efficient Cryptography Group). Available at https://www.secg.org/sec1-v2.pdf

[8] Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key- Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[9] Wagner D, Weaver N, Kao P, Shakir F, Law A, Ngai N (2024). Message Authentication Codes (MACs). Computer Security, Chapter 8. Available at https://textbook.cs161.org/crypto/macs.html

[10] Douglas W. Jones (2024). BCD Arithmetic, a tutorial. *The Arithmetic Tutorial Collection.* Available at https://homepage.divms.uiowa.edu/~jones/bcd/bcd.html

[11] Stewart Weiss (2024) Unicode and UTF-8. Software Design Lecture Notes. Available at https://www.cs.hunter.cuny.edu/~sweiss/resources/Unicode.pdf

[12] 3rd Generation Partnership Project. Specification # 33.501: *Security architecture and procedures for 5G system*. Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

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 Kent: 0000-0001-6334-9486

Murugiah Souppaya: 0000-0002-8055-8527

How to Cite this NIST Technical Series Publication:

Bartock M, Cichonski J, Souppaya M, Kent K, Grayeli P, Sharma S, Teague C. (2026) Protecting Subscriber Identifiers with Subscription Concealed Identifier (SUCI): Applying 5G Cybersecurity and Privacy Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 36A. https://doi.org/10.6028/NIST.CSWP.36A

Contact Information

5g-security@nist.gov

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