

# **Securing 5G:** CSRIC VII 5G Standalone Network Test Report *Q4 2023*

# Table of Contents

Introduction	
Scope of Report	5
Background	5
Why CSRIC VII	5
CSRIC VII Working Group 3's Report and Recommendations for 5G Standalone Architecture	6
Definition of CSRIC Test Cases	7
Test Results	9
Introduction	9
IPsec Configuration	11
SIM Card Profiles	12
Test Case 1: CSRIC 7 WG 3 – NAS Signaling Confidentiality	12
Part 2: Using NEA2 Encryption	21
Test Case 2: CSRIC 7 WG 3 – RRC Signaling Confidentiality	24
Test Case 3: CSRIC 7 WG 3 – Access Stratum User Plane Confidentiality	31
Test Case 4: CSRIC 7 WG 3 – Access Stratum User Plane Integrity	33
Test Case 5: CSRIC 7 WG 3 – SUPI/SUCI Privacy Enabled	36
Test Case 6: CSRIC 7 WG 3 – IPsec on Transport Links	39
Test Case 7: CSRIC 7 WG 3 – Transport Layer Security for SBA Interfaces	47
Conclusions and Next Steps	60
Appendix: Acronyms	63

# Introduction

# The 5G Security Test Bed Is the Latest Industry Initiative to Advance 5G Security

The wireless industry prioritizes stronger security and reliability with every generation of its mobile networks. With 5G in particular, secure connectivity is the foundation that supports and enhances the many benefits these networks provide. The wireless industry devotes significant resources to 5G security and has expanded its efforts through the 5G Security Test Bed.

Formally launched in 2022, the 5G Security Test Bed is a unique collaborative endeavor between wireless providers, equipment manufacturers, cybersecurity experts, academia, and government agencies, created with a sole focus on testing and validating 5G security recommendations and use cases from government groups, wireless operators, and others. It is the only initiative that uses commercial-grade network equipment and facilities to demonstrate and validate how 5G security standards recommendations will work in practical, real-world conditions.

The 5G Security Test Bed reflects the industry's collaborative approach to 5G security—it was created by the Cybersecurity Working Group (CSWG), an industry initiative that convenes the world's leading telecom and tech companies to assess and address the present and future of cybersecurity. Its members are wireless providers AT&T, T-Mobile, and UScellular; industry partners Ericsson, the MITRE Group, SecureG, and Intel; and academic partners the University of Maryland and Virgina Tech Advanced Research Corporation (VT-ARC).

The 5G Security Test Bed has a Technical Advisory Committee (TAC) made up of its members and the Test Bed Administrator. The TAC advises the Test Bed Administrator on the day-to-day technical and operational activities and decisions related to the Test Bed, including but not limited to: development of use cases to be tested, test plan development and review, raw test data analysis, test result and report generation, and development of recommendations to standards bodies based on results.

The 5G Security Test Bed further works with a broad array of government agencies, policymakers, international standards bodies, thought leaders, and partners in the telecommunications and information technology sectors. These groups include the 3<sup>rd</sup> Generation Partnership Project (3GPP), the International Telecommunication Union (ITU), the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Federal Communications Commission (FCC), among others.

# The 5G Security Test Bed Uses Real-World Equipment, Validating Real-World Applications

One of the 5G Security Test Bed's core values lies in its ability to validate 5G security use cases in a real-world environment, using an actual 5G network architecture. Leveraging a significant investment and in-kind contributions, the Test Bed's founding members built this state-of-the-art, private 5G network from scratch for the singular purpose of evaluating 5G network security.

The 5G Security Test Bed's previous testing activities have worked to validate the recommendations of the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) advisory group, for both non-standalone and standalone network configurations. In addition, the Test Bed draws on recommendations from its own Technical Advisory Committee to address emerging vulnerability research. The first report in this series focused on the validation of the CSRIC non-standalone configurations, while this report addresses the CSRIC standalone configuration recommendations and network slicing. The 5G Security Test Bed will continue evaluating additional recommendations and use cases from CSRIC and other entities in future tests. It is not set up to be a platform for identifying vulnerabilities or conducting penetration testing of networks or equipment.

# **Real-World Testing**

The 5G Security Test Bed advances wireless security by:

- Conducting real-world tests in a rigorous, transparent, and replicable manner that can assess and validate theoretical and policy concerns and overcome hypothetical laboratory testing limitations.
- Drawing on the expertise of government, wireless providers, and equipment manufactures to evaluate specific use cases and support new equipment development.
- Testing security functionality in different scenarios, enabling industry and government to identify, mitigate, and respond to evolving threats while protecting consumers, businesses, and government agencies.

# **Real-World Applications**

The 5G Security Test Bed's tests and outcomes support several applications that can drive new technology and transform cities, government, and industries. Use cases include government and enterprise applications, general network security protections, and smart city applications such as:

- Primary Use Cases: Network Security
  - o Protecting Information in Transit
  - o Roaming Security
  - o Subscriber Privacy
  - o Zero Trust Network Security
  - o False Base Station Detection and Protection
  - o 5G Cloud Network Security

# • Secondary Use Cases: Devices and Applications

- o High-Resolution Video Surveillance (e.g. Smart Cities, Large Venues)
- o LTE/5G Drones with High-Resolution Video Feedback (e.g. Smart Cities)
- o Dynamic Supply Chain Verification (Real-Time Monitoring and Logistics)
- o Automated, Reconfigurable Factories
- o Autonomous Vehicles
- o Immersive AR/VR

The 5G standalone network architecture tested for this report makes up key components of these applications because they enable service to be customized to diverse needs and requirements. The test cases outlined here show how these new and evolving uses can successfully adopt enhanced security capabilities while improving performance and capability.

# **Scope of Report**

This report addresses recommendations derived from the FCC's Communications Security, Reliability, and Interoperability Council VII March 2021 report, *Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security.*<sup>1</sup> The report focused on the implementation of security protections in 5G "standalone" (SA) networks (that is, networks designed and built specifically for 5G) by assessing security features from 3GPP TS 33.501, the primary technical standard for 5G SA. (By contrast, non-standalone networks offer 5G service together with 4G LTE over shared infrastructure.) The first report from the 5G Security Test Bed focused on NSA networks supporting both 5G and 4G traffic.

This 5G STB report's scope is to evaluate and verify CSRIC VII's recommendations for SA architecture by investigating the security features associated with 5G network infrastructure and the devices that can access a 5G SA network.

# Background

# Why CSRIC VII

The Communications Security, Reliability, and Interoperability Council is a federal advisory committee that provides the Federal Communications Commission with recommendations to enhance the security, reliability, and interoperability of communications systems. CSRIC provides a forum for industry and government technical experts to assess developing technology and analyze complex issues. It is a leading venue for stakeholders in and outside of government to share ideas and best practices, and to help the FCC stay abreast of cutting-edge technology

<sup>&</sup>lt;sup>1</sup> CSRIC VII WG3, Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security (Mar. 2021), <u>https://www.fcc.gov/file/20606/download</u>.

and security issues affecting the communications sector. CSRIC's work continues to influence government and industry agendas and activities.

The FCC charters CSRIC every two years. CSRIC VII's charter was from March 2019 to March 2021, and it focused on a range of public safety and homeland security-related communications matters, including issues related to 5G network evolution. 5G offers significant and novel capabilities compared with previous generations of wireless networks, but new capabilities, infrastructure, and equipment can also introduce security risks. The FCC tasked CSRIC VII with examining these security risks and making recommendations associated with the evolving standards' optional security features. Because 5G standards and specifications continue to develop, CSRIC VII's work offered an opportunity to update future standards.

Likewise, the 5G Security Test Bed's work in testing CSRIC's recommendations can be used both to inform network architecture and operation, and to enhance future 5G standards.

# CSRIC VII Working Group 3's Report and Recommendations for 5G Standalone Architecture

# CSRIC VII's Recommendations

CSRIC VII worked to identify and evaluate optional features in the 3GPP standards that would potentially cause security gaps in 5G if not implemented. In March 2021, CSRIC's Working Group 3 (WG3, "Managing Security Risk in Emerging 5G Implementations") released a report, *Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security.*<sup>2</sup> The report focused on identifying optional features in proposed 3GPP standards that might diminish the effectiveness of 5G security, and made recommendations to address these gaps.

Several security features outlined in 3GPP TS 33.501 releases 15 and 16 were mandatory for equipment vendors to implement, but optional for 5G network operators to deploy. CSRIC VII WG3 looked at the optional security features and conducted a risk assessment and analysis on those measures, including: confidentiality for Non-Access Stratum (NAS) signaling,<sup>3</sup> user plane confidentiality and integrity, radio resource control signaling confidentiality, Subscription Permanent Identifier (SUPI)/International Mobile Subscriber Identity (IMSI) privacy, and network security, including IP security (IPsec) and transport layer security (TLS).

<sup>&</sup>lt;sup>2</sup> Id.

<sup>&</sup>lt;sup>3</sup> "NAS signaling" carries the user data from the user equipment to the MME through the S1 pathway.

# Based on its assessment, CSRIC VII WG3 made eight recommendations:

- **Previous CSRIC Recommendations:** Communications sector members and stakeholders should adopt CSRIC-recommended 5G SA threat mitigations from previous CSRIC VI, V, and IV reports.<sup>4</sup>
- NAS Signaling Confidentiality: Operators should convey only non-user identity related information until security context is established. (CSRIC noted that 3GPP TS 33.501 encrypts all NAS messages after security context is established.)
- User Plane Confidentiality: Operators should apply user plane (UP) confidentiality protections at the Packet Data Convergence Protocol (PDCP) layer.
- User Plane Integrity: OEM and network infrastructure vendors should support, and operators should implement, the 3GPP TS 33.501 Release 16 and 128-NIA3 capabilities of supporting integrity protection and user data replay protection at the full data rate available to the user equipment. (Release 15 required only 64kbps.)
- **RRC Signaling Confidentiality:** Operators should protect RRC-signaling (Radio Resource Control) confidentiality and convey only non-identity related information prior to establishing security context.
- **SUPI/IMSI Privacy:** Devices and networks in the U.S. should use IMSI privacy, and permit the null encryption only for making emergency services calls (i.e. 9-1-1).
- Network Security—IPsec: Operators should apply IPsec or a tunneling technology such as VPN tunnels for transport.
- Core Network Security—Transport Layer Security (TLS): Operators should apply TLS for Service-Based Architecture (SBA) interfaces.

# **Definition of CSRIC Test Cases**

Based on the CSRIC VII WG3 recommendations, the 5G STB established and executed seven test cases described in this report, as follows:

# 1. NAS Signaling Confidentiality:

a. <u>CSRIC VII WG3 Recommendation</u>: Operators should convey only non-user identity related information until security context is established.

<sup>&</sup>lt;sup>4</sup> See CSRIC VI WG3, Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks (Sept. 2018), <u>https://www.fcc.gov/file/14500/download;</u> CSRIC V WG6, Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network (making recommendations for security-by-design principles in the core communications network) (March 2016), <u>https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6\_FINAL\_%20wAppendix\_0316.pdf</u>; and CSRIC IV WG4, Wireless Segment Cybersecurity Risk Management and Best Practices (March 2015), <u>https://transition.fcc.gov/pshs/advisory/csric4/CSRIC\_IV\_WG4\_Final\_Report\_031815.pdf</u>.

b. <u>5G STB Test Case 1:</u> Demonstrate how user identity related information can be transmitted confidentially by testing the implementation of NAS Signaling encryption. Once an encrypted channel is established, only non-user identity related information should be observable.

# 2. RRC Signaling Confidentiality:

- a. <u>CSRIC VII WG3 Recommendation:</u> Operators should protect RRC-signaling confidentiality and convey only non-identity related information prior to establishing security context.
- b. <u>5G STB Test Case 2:</u> Demonstrate that the PDCP provides RRC signaling confidentiality between the user equipment and NG-RAN (Next Generation Radio Access Network) using 128-bit NEA algorithms.

## 3. Access Stratum User Plane (Payload Data) Confidentiality:

- a. <u>CSRIC VII WG3 Recommendation</u>: Operators should apply user plane confidentiality protections at the PDCP layer.
- b. <u>5G STB Test Case 3</u>: To demonstrate that the PDCP provides user plane data confidentiality between the user equipment and NG-RAN using 128-bit NEA algorithms.

## 4. Access Stratum User Plane (Payload Data) Integrity:

- a. <u>CSRIC VII WG3 Recommendation</u>: Operators should apply user plane confidentiality protections at the PDCP layer.
- b. <u>5G STB Test Case 4-1</u>: Demonstrate that the PDCP provides user plane data integrity protection at the full rate.

#### 5. SUPI/IMSI User Privacy:

- a. <u>CSRIC VII WG3 Recommendation</u>: Devices and networks in the U.S. should use IMSI privacy.
- b. <u>5G STB Test Case 5-1</u>: Register a device on the test network by exchanging identity information using the subscription concealed identifier (SUCI) to encrypt the SUPI.

#### 6. Network Security:

- a. <u>CSRIC VII WG3 Recommendation:</u> Apply IPsec or tunneling technology to protect network security during transport.
- b. <u>5G STB Test Case 6:</u> Use IPsec to transmit user plane and control plane (CP) messaging while protecting confidentiality, integrity, and replay.

- 7. Core Network Security (Transport Link Encryption):
  - a. <u>CSRIC VII WG3 Recommendation</u>: Use TLS for SBA interfaces and tunneling technology for transport when not using the SBA.
  - b. <u>5G STB Test Case 7:</u> Demonstrate TLS encryption to protect SBA interfaces in the 5G core.

# **Test Results**

# Introduction

This document presents test results based on use cases derived from the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) VII Working Group 3 (WG3) Report 2 recommendations for securing 5G standalone networks based upon its analysis of optional security requirements in 3GPP TS 33.501.

The configuration used for these tests comprises radio access network (RAN) equipment hosted at the University of Maryland (UMD) and a dual-mode core (DMC), that provides both 4G LTE and 5G functionality hosted at the MITRE Corporation. The core is the Ericsson DMC, PCC version 1.19. The connection between the RAN at UMD and the DMC at MITRE goes over the internet and, for the scenarios considered here, is treated as an untrusted link.<sup>5</sup> **Error! Reference source not found.** shows the relevant components of the Test Bed, including available test points. Not all of the test points shown in the diagram were used for these tests.

The routers shown at each location are Ericsson 6672 routers (referred to as R6672, or R6K). The switches shown are each Pluribus Freedom 9372-X switches. For the tests implemented here, the two switches are considered part of the "untrusted" backhaul link. The core is configured to support two network slices. The first slice, referred to as Slice 1 in this report, is considered the default enhanced mobile broadband (eMBB) network slice. The second slice, Slice 2, emulates a private network and includes the ability to form an IPsec tunnel to create a highly secure slice. The IPsec tunnel is configured with one endpoint at the baseband unit (BBU) and the other at the core-side R6672 router. On the server on the core side, there are two virtual web servers instantiated, one for each slice, and isolated from each other. All tests for the test cases discussed in this report were executed on Slice 2.

<sup>&</sup>lt;sup>5</sup> In the actual implementation, there are additional security measures implemented, including an IPsec tunnel between the UMD and MITRE campus/corporate networks. For the purposes of these tests, this tunnel is considered part of the untrusted link and therefore, any encryption implemented for the tests is in addition to these measures.

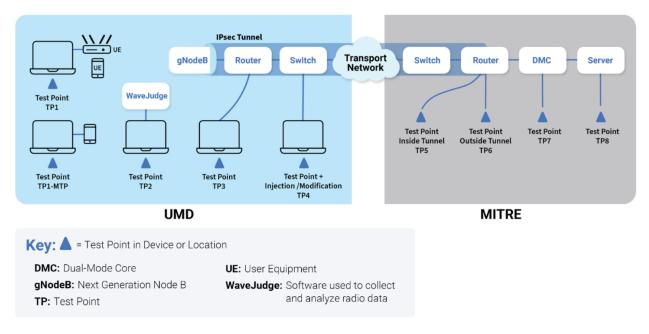


Figure 1: 5G STB Lab Component Block Diagram and Test Points

Tests were run with band N41 for the new radio (NR) using a Sierra Wireless EM9190 card connected to a laptop by USB as a cellular modem, as well as a Qualcomm Mobile Test Platform (MTP) device. For the purposes here, we will refer to the combination of that laptop and the cellular modem as the UE.

Packets are captured on each of the identified test points in Figure 1: at the UE(s) (TP1), on the RAN-side Pluribus switch (TP4), on the Core-side R6K router (TP6), and at the DMC (TP7). These test points are identified with numbers as shown in the figure and described in more detail in Table 1.

#### Table 1: Test Point Descriptions

Test Point	Description and Use
TP1-S	Laptop connected to Sierra Wireless card and/or software-defined radio (SDR); Wireshark captures packets originating at and destined to UE laptop; other tools access SDR controls and data
TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
TP2	WaveJudge interface
TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
TP7	CNOM tool accessing DMC messages and command line interface on core
TP8	Applications running on application server in MITRE facility

# **IPsec Configuration**

3GPP TS 33.401 requires IPsec, when used, to support ESP and IKEv2 with certificates-based authentication. The security gateway (SEG) is optional to use. The following requirements are from 33.401, section 12, Backhaul link user plane protection:

In order to protect the S1 and X2 user plane as required by clause 5.3.4, it is required to implement **IPsec ESP** according to RFC 4303 [7] as profiled by TS 33.210 [5], with confidentiality, integrity and replay protection.

**Tunnel mode IPsec** is mandatory to implement on the eNB for X2-U and S1-U. On the X2-U and S1-U, transport mode IPsec is optional for implementation. NOTE 1: Transport mode can be used for reducing the protocol overhead added by IPsec. On the core network side a **SEG may be used** to terminate the IPsec tunnel.

For both S1 and X2 user plane, **IKEv2 with certificates based authentication shall be implemented**. The certificates shall be implemented according to the profile described by TS 33.310 [6]. IKEv2 shall be implemented conforming to the IKEv2 profile described in TS 33.310 [6].

3GPP TS 33.501 retains these IPsec requirements for 5G SA and NSA, when IPsec is used.

CSRIC 7 WG 2 Report 2 recommends IPsec on untrusted links to provide confidentiality and integrity protection over the S1-MME, S1-U, and management interfaces.

IPsec is implemented on Slice 2, with tunnel endpoints at the RAN and at the core-side R6K.

## **SIM Card Profiles**

Some tests require different SIM card profiles to tests the desired functionality. Table 2 lists the different profiles that were used during each test.

Table 2: SIM Card Profiles

ID	IMSI	Profile
Ν	310 014 791 791 001	N (NULL)
А	310 014 791 791 011	А
В	310 014 791 791 021	В

# Test Case 1: CSRIC 7 WG 3 – NAS Signaling Confidentiality

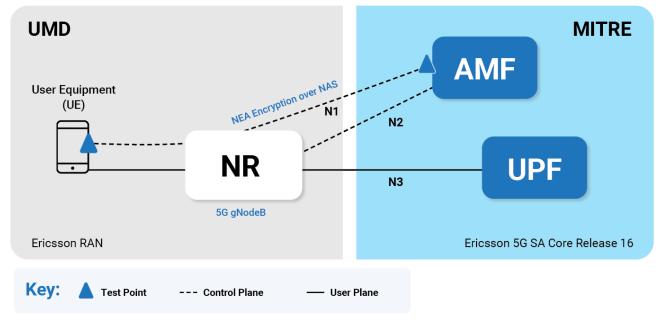


Figure 2: Test Case SA-01 Configuration

## Test Case ID: TC-SA-01

## Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the NAS signaling confidentiality, but optional for service providers to use.

Given this standards requirement, CSRIC VII recommends only non-user identity related information shall be conveyed prior to security context being established. Note, after security context is established, all NAS messages are encrypted according to 3GPP TS 33.501.

This test involves implementation of NAS signaling encryption on the N1 interface. Once encrypted channels are established, user identity info may be securely exchanged.

Used	Test Point	Description and Use			
Х	TP1-S	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop			
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data			
	TP2	WaveJudge interface			
	TP3       Wireshark running on laptop connected to RAN-side R6K rou capture packets inside the tunnel (encrypted packets when is enabled)				
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"			
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"			
х	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC			
	TP7	CNOM tool accessing DMC messages			
	TP8	Applications running on application server in MITRE facility			

# Test points used:

		SIM			
Slice	IP pool	LABEL	SIM LABEL IMSI	DNN	DN SERVERS
				dnn-embb-	
Slice 2	172.24.1.0/24	N21	3100147917910021	stb2.mitre.net	192.168.59.146/28

Network Slice 2 and a UE with Profile B SIM were used throughout the tests. The UE used for Slice 2 was a Sierra Wireless Modem, which is connected and controlled by a laptop outside the Faraday Cage. IPsec for for Slice 2 and control traffic was turned on/off as and when required.

To ensure that the core did not retain the UE state, we deleted the UE context from the core (Figure 3), and ensured that the IPsec tunnel for the transport channel between the RAN and core was up (Figure 4).

```
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh delete_subscriber -imsi 310014791791021
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh delete_subscriber -imsi 310014791791001
Subscriber identity: "310014791791001" is not registered.
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
```

Figure 3: Deleting UE Context from Core

MUMD02AVW> st ipsec						
221118	8-16:31:13 169	9.254.2.2 22.0h	MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317			
====== Ргоху	Adm State	Op. State	MO			
====== 14282		1 (ENABLED)	Transport=1,Router=NRCUCP,IpsecTunnel=1			
====== Total:	1 MOs					

Figure 4: IPsec enabled between BBU and Core-side R6K router

This test has two parts; 1) with NEA0 (no encryption) and 2) with NEA2 activated to encrypt NAS signaling. For Part 1, on the core side, we used a command line interface command to set priority for the NAS encryption algorithm making NEA0 (null algorithm) the highest priority (specifically, priority 1). See Figure 5 for the initial NEA settings, Figure 6 for the commands changing the priority settings, and

```
=== mtramcamiar erv@errc-bc-mm-controtter-a andr ~ # dsu der_uea_ardorrtum -uame ueaa
                   Active Data Planned Data
Parameter
                         20221118164429
timestamp
planState
prio (N1SecurityAlgorithmPriority) 1
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea algorithm -name nea1
                   Active Data Planned Data
Parameter
        . . . . . . . . . .
                         20221109120424
timestamp
planState
prio (N1SecurityAlgorithmPriority) 2
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea2
                    Active Data Planned Data
Parameter
20221118164429
timestamp
planState
prio (N1SecurityAlgorithmPriority) 3
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea3
Parameter
                   Active Data Planned Data
timestamp
                         20220727201309
planState
orio (N1SecuritvAlgorithmPrioritv) 0
```

Figure 7 displaying the encryption setting to NULL (NEA0). For the second part, we set encryption back to NEA2 with the highest priority.

#### Test Results for 5G STB – CSRIC-Inspired SA Use Cases

=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get\_nea\_algorithm -name nea0 Parameter Active Data Planned Data 20221118100928 timestamp planState prio (N1SecurityAlgorithmPriority) 1 === mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea1 Active Data Planned Data Parameter -----20221109120424 \_\_ timestamp planState prio (N1SecurityAlgorithmPriority) 2 === mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get\_nea\_algorithm -name nea2 Active Data Planned Data Parameter timestamp 20221118100928 planState prio (N1SecurityAlgorithmPriority) 3 === mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea3 Active Data Planned Data Parameter -----20220727201309 timestamp planState prio (N1SecurityAlgorithmPriority) 0

Figure 5: Confidentially Core Setting - NEA2 (128-NEA2 cipher algorithm) before configuration change

```
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh modify nea_algorithm -name nea2 -prio 1
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh modify_nea_algorithm -name nea0 -prio 3
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea0
                         Active Data Planned Data
arameter
_____
imestamp
                 20221118100928 20221118161841
                               Modified
lanState
rio (N1SecurityAlgorithmPriority) 1
                                       3
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name nea1
arameter
                          Active Data Planned Data
.....
                           20221109120424
imestamp
lanState
rio (N1SecurityAlgorithmPriority) 2
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea2
                        Active Data Planned Data
arameter
imestamn
                   20221118100928 20221118161826
```

Figure 6: Confidentially cipher algorithm setting changes

```
== mildmcamial elaGelic-bc-ww-contlorel-a ANCR ~ # deu dei ardolitum -uame usaa
Parameter
                  Active Data Planned Data
20221118164429
timestamp
planState
prio (N1SecurityAlgorithmPriority) 1
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea1
Parameter
                     Active Data Planned Data
timestamp
                         20221109120424
planState
prio (N1SecurityAlgorithmPriority) 2
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name nea2
                    Active Data Planned Data
Parameter
20221118164429
timestamp
planState
prio (N1SecurityAlgorithmPriority) 3
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name nea3
Parameter
                   Active Data Planned Data
20220727201309
timestamp
planState
orio (N1SecuritvAlgorithmPrioritv) 0
```

Figure 7: Confidentially Core Setting changes – NEA0 (no encryption) now has the highest priority (priority 1)

```
--- III CI UNICAMITOT CI VUCITE-PE-INNI-CUITIOLICI -O ANCO - # YSH GET HEA ALGUITTINI -HANC HEAV
                        Active Data Planned Data
Parameter
20221118171329
timestamp
planState
prio (N1SecurityAlgorithmPriority) 3
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name neal
                  Active Data Planned Data
Parameter
timestamp
                 20221109120424
planState
prio (N1SecurityAlgorithmPriority) 2
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea2
Parameter
                 Active Data Planned Data
timestamp
                        20221118171329
planState
prio (N1SecurityAlgorithmPriority) 1
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea algorithm -name nea3
Parameter
                  Active Data Planned Data
timestamp
                20220727201309
planState
prio (NlSecurityAlgorithmPriority) 0
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
```

Figure 8: Confidentially Core Setting changes – NEA2 (no encryption) now has the highest priority (priority 1)

#### Part 1: Using NEA0 Encryption

Upon starting the UE, it sends an initial message with a registration request. Figure 9 shows the Wireshark interpretation of the captured message from the UE indicating that for the 5G mobile identity, the type of identity is SUCI, the concealed identifier. Subsequently, the AMF requests

authentication (Figure 10) and the UE responds (Figure 11). After authentication, the core indicates the ciphering algorithm to be used, in this case NEA0, as shown in Figure 12. Subsequent transmissions are processed with the NEA0 (NULL) algorithm, resulting in decipherable messages, as shown in Figure 13 and Figure 14, in which details of the messages are visible such as the UE's IMEISV.

🖉 💿 🚞 🗋 🗙 🖉 🛸	* 철 * 또		. ≪ <u>11</u>	
Time	Source	Destination	Protocol	Length Info
101 2022-11-18 16:48:49.834484	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	182 InitialUEMessage, Registration request
103 2022-11-18 16:48:49.888077	10.205.67.204		NGAP/NAS-5GS	142 DownlinkNASTransport, Authentication request
105 2022-11-18 16:48:50.051307	10.220.67.19	10.205.67.204		142 UplinkNASTransport, Authentication response
106 2022-11-18 16:48:50.074457	10.205.67.204		NGAP/NAS-5GS	134 SACK (Ack=1, Arwnd=32768) , DownlinkNASTransport, Security mode command
107 2022-11-18 16:48:50.085769			NGAP/NAS-5GS/NAS-5GS	258 SACK (Ack=1, Arwnd=16384) , UplinkNASTransport, Security mode complete, Registration requ
108 2022-11-18 16:48:50.091301	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	142 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command
critica	lity: reject (0)			
⊻ value	11.5 5 31.2			
RAN-	UE-NGAP-ID: 1679	9999		
✓ Item 1: id-NAS	-PDU			
<ul> <li>ProtocolIE-</li> </ul>	Field			
	NAS-PDU (38)			
	lity: reject (0)			
∀ value				
			c037819cded0d7f5a43a7f.	2722fd7a3508aad12e3aa50
v	Non-Access-Stratu			
	Plain NAS 5GS			
		= Spare Half Oc		nagement messages (126)
				sage, not security protected (0)
			n request (0x41)	age, not security protected (0)
	✓ 5GS regist		i request (6x41)	
			Request bit (FOR) . No	follow-on request pending
			ration type: initial r	
	V NAS key se			
			curity context flag (T	SC): Native security context (for KSIAMF)
			t identifier: 7	
	✓ 5GS mobile			
	Length	: 54		
	0	= Spare: 0		
	.000 .	= SUPI forma	t: IMSI (0)	
	0	= Spare: 0		
			lentity: SUCI (1)	
			NCC): United States (31	
			NC): TEST IMSI HNI (01	4)
		g indicator: 0		
			scheme Id: ECIES sche	me profile B (2)
			y identifier: 12	
				3508aad12e3aa500508cea89cb781cc7e365b22f8a0
				5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc7e365b
	Cit	hertext: 22f8a0	614b	

Figure 9: Test Case SA-01 Initial UE Message

<pre>csric_tests_01and-05-2_11-18-22_1610.pcap</pre>							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
🛋 🔳 🖉 🐵 🚞 🛅 🗙 🖉 🖛	€ 🔮 🖌 🛓 📃 🦉						
ngap							
No. Time 101 2022-11-18 16:48:49.834484 103 2022-11-18 16:48:49.888077 105 2022-11-18 16:48:50.051307 106 2022-11-18 16:48:50.074457 107 2022-11-18 16:48:50.085769	Source         Destination           10.220.67.19         10.205.67           10.205.67.204         10.220.67           10.220.67.19         10.205.67           10.220.67.19         10.205.67           10.220.67.19         10.205.67           10.220.67.19         10.205.67           10.220.67.19         10.205.67           10.220.67.19         10.205.67	.19 NGAP/NAS-5GS .204 NGAP/NAS-5GS .19 NGAP/NAS-5GS	Length Info 182 InitialUEMessage, Registration request 142 DownlinkNASTransport, Authentication request 142 UplinkNASTransport, Authentication response 134 SACK (Ack+1, Arund=32768), DownlinkNASTransport, Security mode command 258 SACK (Ack+1, Arund=15834), UplinkNASTransport, Security mode complete, Re				
108 2022-11-18 16:48:50.085789	10.205.67.204 10.220.67		142 SACK (Ack=1, Arwnd=10564), OpinnkNASTransport, Security mode complete, Re 142 SACK (Ack=2, Arwnd=32768), DownlinkNASTransport, Security mode command				
4							
<pre>&gt; Ethernet II, Src: ExtremeN.36:58:06 &gt; 882.10 Virtual LAN, PRI 0, DEI 0, &gt; 100 Seream Control Transmission Protocol &gt; Stream Control Transmission Protocol &gt; NGAPICation Protocol (Downlinkkas &gt; NGAPI-PDU: initiatingNessage (0) &gt; initiatingNessage (0) &gt; initiatingNessage procedureCode: id-Downlink criticality: ignore (1) &gt; value &gt; DownlinkkasTransport &gt; value &gt; Item 0: id-AMF &gt; Item 1: id-RAS. &gt; ProtocolIE- id: id- &gt; Item 1: id-RAS. &gt; ProtocolIE- id: id- critical &gt; value &gt; Value &gt; Value &gt; Value &gt; Value &gt; Value &gt; Value &gt; Value &gt; Value &gt; Vitem 2: id-RAS. &gt; Value &gt; V</pre>	<pre>v initiatingWessage procedureCode: id-DownlinkWASTransport (4) criticality: ignore (1) v value v DownlinkWASTransport v protocolIEs: 3 items v protocolIEs: 3 items v Item 0: id-AWF-UE-WGAP-ID &gt; ProtocolIE-Field &gt; Item 1: id-RAW-UE-WGAP-ID v Item 2: id-NAS-PDU v ProtocolIE-Field i id : id-NAS-PDU (38) criticality: reject (0)</pre>						
<pre>&gt; Non-Access-Stratum 505 (MAS)PDU &gt; Plain NAS 505 Message Extended protocol discriminator: 56 mobility management messages (126) 0000 = Spare Half Octet: 0  0000 = Security header type: Plain NAS message, not security protected (0) Message type: Authentication request (0x56) 0000 = Spare Half Octet: 0 &gt; NAS key set identifier - ngKSI  0.0. = Type of security context flag (TSC): Native security context (for KSIAMF)  000 = NAS key set identifier: 0 &gt; ABBA Length: 2 ABBA Contents: 0000 &gt; Authentication Parameter RAND - 56 authentication challenge Element ID: 0x21 RAND value: 019525fd0186fee995ce5364418139C &gt; Authentication Parameter AUTN (UMTS and EPS authentication challenge) - 56 authentication challenge Element ID: 0x20 Length: 10 AUTN value: a36da007152900073e82fd23f53b9dd SQN xor AX: a36da007152900073e82fd23f53b9dd MG: 737e82fd23f53b0dd</pre>							

*Figure 10: AMF/Core Authentication Request* 

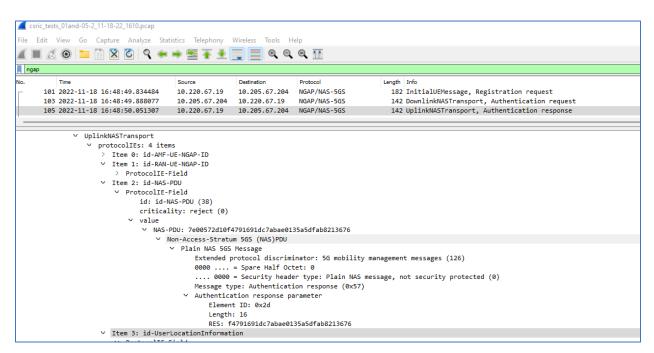


Figure 11: UE Authentication Response

<b>_</b> c	csric_tests_01and-05-2_11-18-22_1610.pcap								
File	ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help								
	( ■ 2 @ > 1 X 0 < + + ≤ 7 ± ] = <								
ng ng	ngap								
No.	Time	Source	Destination	Protocol	Length Info				
Г	101 2022-11-18 16:48:49.834484	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	182 InitialUEMessage, Registration request				
	103 2022-11-18 16:48:49.888077	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	142 DownlinkNASTransport, Authentication request				
	105 2022-11-18 16:48:50.051307		10.205.67.204		142 UplinkNASTransport, Authentication response				
	106 2022-11-18 16:48:50.074457	10.205.67.204		NGAP/NAS-5GS	134 SACK (Ack=1, Arwnd=32768) , DownlinkNASTransport, Security mode command				
	107 2022-11-18 16:48:50.085769		10.205.67.204	NGAP/NAS-5GS/NAS-5GS	258 SACK (Ack=1, Arwnd=16384) , UplinkNASTransport, Security mode complete, Registration request				
	108 2022-11-18 16:48:50.091301	10.205.67.204		NGAP/NAS-5GS	142 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command				
	109 2022-11-18 16:48:50.100630			NGAP/NAS-5GS	158 SACK (Ack=2, Arwnd=16384) , UplinkNASTransport, Security mode complete				
	113 2022-11-18 16:48:50.461164	10.205.67.204	10.220.67.19	NGAP	182 InitialContextSetupRequest				
_									
		lity: reject (0)							
	✓ value								
		PDU: 7e039e116b380		0/010/001360102					
		Non-Access-Stratum ✓ Security protec							
				inator: 5G mobility man	anoment marraner (126)				
			Spare Half Oct		agemente messages (120)				
					ected with new 5GS security context (3)				
			hentication co						
		Sequence nur							
		✓ Plain NAS 5GS M							
		Extended pro	otocol discrim	inator: 5G mobility man	agement messages (126)				
			Spare Half Oct						
		0000 =	Security heade	er type: Plain NAS mess	age, not security protected (0)				
		Message type	e: Security mod	de command (0x5d)					
		✓ NAS security	y algorithms						
					A0 (null ciphering algorithm) (0)				
				tegrity protection algo	rithm: 128-5G-IA2 (2)				
			Spare Half Oct						
		∨ NAS key set							
					C): Native security context (for KSIAMF)				
				t identifier: 0					
				Replayed UE security ca	padliltles				
		✓ IMEISV reque							
			. = Element ID						
			. = Spare bit(		(4)				
		✓ Additional		uest: IMEISV requested	(1)				
		- Additional :	so security in	ormación					

Figure 12: Core Ciphering Algorithm in use – NULL ciphering

sric_tests_01and-05-2_11-18-22_1610.pcap							
Edit View Go Capture Analyze Sta	atistics Telephony Wireless Tools	Help					
🖉 🕲 🚞 🖹 🕱 🙆 🧣							
P							
Time	Source Destination	Protocol	Length Info				
101 2022-11-18 16:48:49.834484	10.220.67.19 10.205.67.204		182 InitialUEMessage, Registration request				
103 2022-11-18 16:48:49.888077	10.205.67.204 10.220.67.19	NGAP/NAS-5GS	142 DownlinkNASTransport, Authentication request				
105 2022-11-18 16:48:50.051307	10.220.67.19 10.205.67.204		142 UplinkNASTransport, Authentication response				
106 2022-11-18 16:48:50.074457	10.205.67.204 10.220.67.19		134 SACK (Ack=1, Arwnd=32768) , DownlinkNASTransport, Security mode command				
107 2022-11-18 16:48:50.085769	10.220.67.19 10.205.67.204						
108 2022-11-18 16:48:50.091301	10.205.67.204 10.220.67.19	NGAP/NAS-5GS	142 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command				
109 2022-11-18 16:48:50.100630		NGAP/NAS-5GS	158 SACK (Ack=2, Arwnd=16384) , UplinkNASTransport, Security mode complete				
113 2022-11-18 16:48:50.461164	10.205.67.204 10.220.67.19	NGAP	182 InitialContextSetupRequest				
115 2022-11-18 16:48:50.517237 116 2022-11-18 16:48:50.517261	10.220.67.19 10.205.67.204 10.220.67.19 10.205.67.204		94 InitialContextSetupResponse				
116 2022-11-18 16:48:50.51/261	10.220.67.19 10.205.67.204	NGAP	914 UERadioCapabilityInfoIndication				
✓ Item 2: id-NAS-	DDU						
V Item 2: id-NAS- V ProtocolIE-							
	NAS-PDU (38)						
	lity: reject (0)						
value	iity. (eject (0)						
	-PDU: 7e048be1ccbb007e005e770009	3515371501217124f171005	f7=004171003601134010f0_				
	Non-Access-Stratum 5GS (NAS)PDU						
	Security protected NAS 5GS m	055000					
-	Extended protocol discrim		nagement messages (126)				
	0000 = Spare Half O						
			tected and ciphered with new 5GS security context (4)				
	Message authentication co	ode: 0x8be1ccbb					
	Sequence number: 0						
	V Plain NAS 5GS Message						
	Extended protocol discrim		nagement messages (126)				
	0000 = Spare Half O						
			sage, not security protected (0)				
	Message type: Security mo	ode complete (0x5e)					
	✓ 5GS mobile identity						
	Element ID: 0x77						
	Length: 9						
		indication: Even number	of identity digits				
	101 = Type of i						
	IMEISV: 3517351101217	421					
	<ul> <li>VAS message container</li> <li>Element ID: 0x71</li> </ul>						
	Length: 95						
	<ul> <li>Non-Access-Stratum 56</li> </ul>						
	<ul> <li>Non-Access-Stratum 50</li> <li>Plain NAS 5GS Mest</li> </ul>						
			obility management messages (126)				
		pare Half Octet: 0	MOTIF, MOUNDEMENT MESSABES (150)				
			ain NAS message, not security protected (0)				
		Registration request (					
	✓ 5GS registrati		····,				
			(FOR): No follow-on request pending				
0 = Follow-On Request bit (FOR): No follow-on request pending							
	001 = 5GS registration type: initial registration (1)						
	✓ NAS key set id		· Initial registration (1)				

*Figure 13: Core Ciphering Algorithm in use –Uplink NAS Transport NULL ciphering* 

sric_tests_01and-05-2_11-18-22_1610.pcap			
Edit View Go Capture Analyze Sta	atistics Telephony Wireless Tools	Help	
🖉 🛛 🚞 🖹 🗙 🖉 👄	🔺 🔍 🛣 🕹 🥅 🔲 📵	Q Q II	
		- <b>、</b> - <b>、</b> <u></u>	
IP			
Time	Source Destination	Protocol	Length Info
106 2022-11-18 16:48:50.074457	10.205.67.204 10.220.67.1		134 SACK (Ack=1, Arwnd=32768) , DownlinkNASTransport, Security mode command
107 2022-11-18 16:48:50.085769	10.220.67.19 10.205.67.2		
108 2022-11-18 16:48:50.091301	10.205.67.204 10.220.67.1	9 NGAP/NAS-5GS	142 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command
∨ value			
	-UE-NGAP-ID: 16790000		
✓ Item 2: id-NAS			
ProtocolIE			
	NAS-PDU (38)		
critica V value	lity: reject (0)		
	-PDU: 7e03c2da75b1017e005d0200	a/fa7afa7a=157a236a1aa19a	11 F 878- 848
	Non-Access-Stratum 5GS (NAS)P		410/00040
	Y Security protected NAS 569		
_		iminator: 5G mobility ma	nagement messages (126)
	0000 = Spare Half		
	0011 = Security h	ader type: Integrity pro	tected with new 5GS security context (3)
	Message authentication	code: 0xc2da75b1	
	Sequence number: 1		
	<ul> <li>Plain NAS 5GS Message</li> </ul>		
		riminator: 5G mobility ma	nagement messages (126)
	0000 = Spare Half		
			sage, not security protected (0)
	Message type: Security		
	✓ NAS security algorithm		
			EAO (null ciphering algorithm) (0)
		integrity protection al	gorithm: 128-5G-IA2 (2)
	0000 = Spare Half ✓ NAS key set identifier		
			TSC): Native security context (for KSIAMF)
	000 = NAS key		Set were seen by concert (for KSIS)
	> UE security capability		anahilities
	✓ IMEISV request		
	1110 = Element	ID: Øxe-	
	0 = Spare	it(s): 0x00	
		request: IMEISV requester	i (1)
	✓ NAS security algorithm		
	Element ID: 0x57		
	0 = Spare	it(s): 0x00	
	.000 = Type of	ciphering algorithm: EP	5 encryption algorithm EEA0 (null ciphering algorithm) (0)
	0 = Spare		
	010 T		zorithm: EPS integrity algorithm 128-EIA2 (2)

Figure 14: Core Ciphering Algorithm in use – Downlink NAS Transport NULL ciphering

### Part 2: Using NEA2 Encryption

In the second part of the experiment, we changed the core setting to use NEA2, the 128-NEA2 cipher algorithm as shown in Figure 8 above. As above, the core and UE exchange an authentication request and response (Figure 15 and Figure 16). Figure 17 shows the downlink message indicating the NEA2 cipher algorithm is to be used. Subsequently, all information transmitted is encrypted, as indicated by the inability of the messages to be deciphered in Figure 18 and Figure 19.

csric_tests_01_prt2_11-18-22_1710.pcap				- 0
File Edit View Go Capture Analyze Statistics	Telephony Wireless Tools	Help		
🖉 🔲 🖉 🕲 🚞 🗂 🕱 🖉 🔶 🗯	🛎 春 🛓 📃 📃 🔍 e			
ngap				X 🗆
No. Time	Source	Destination	Protocol	Length Info
137 2022-11-18 17:17:40.193924	10.220.67.19	10.205.67.204	NGAP/NAS-5GS/NAS-5GS	210 InitialUEMessage, Registration request, Registration request
138 2022-11-18 17:17:40.196040	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	118 SACK (Ack=0, Arwnd=32768) , DownlinkNASTransport, Identity request
140 2022-11-18 17:17:40.308451	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	186 UplinkNASTransport, Identity response
142 2022-11-18 17:17:40.365217	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	142 DownlinkNASTransport, Authentication request
144 2022-11-18 17:17:40.428006	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	150 UplinkNASTransport, Authentication response
145 2022-11-18 17:17:40.439472	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	134 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command
✓ Item 1: id-RAN-UE-NO > ProtocolIE-Field				
✓ Item 2: id-NAS-PDU				
ProtocolIE-Field				
id: id-NAS-PD	DU (38)			
criticality:	reject (0)			
∨ value				
	7e0056010200002197fc0a6877	54137cc2419aa008cc5c73	201027845dbc938b80004980	
	ccess-Stratum 5GS (NAS)PDU			
v P]	ain NAS 5GS Message			
	Extended protocol discrim		anagement messages (126)	
	0000 = Spare Half Oc			
			ssage, not security protected	d (0)
	Message type: Authenticat 0000 = Spare Half O			
	NAS key set identifier -			
-			(TSC): Native security context	t (for KSTAME)
	001 = NAS key s		(15c). Macive security context	
,	ABBA			
	Authentication Parameter	RAND - 5G authenticat	ion challenge	
	Element ID: 0x21		5	
	RAND value: 97fc0a687	764137cc2419aa008cc5c	73	
	Authentication Parameter	AUTN (UMTS and EPS au	thentication challenge) - 5G	authentication challenge
	Element ID: 0x20			
	Length: 16			
	<ul> <li>AUTN value: 27845dbc9</li> </ul>	38b80004980e604760cc4	e4	
	SQN xor AK: 27845	lbc938b		
	AMF: 8000			

Figure 15: NEA2 AMF/CORE Authentication Request

man	noint com/nersonal/analki lima eall/	BV/AUTS/ED//ADAGHU/			ELIACHMENTS%ZELIAST%ZELA%ZELA IX. 167 SZ 🗩 💶 💶 🔹 🚥
	csric_tests_01_prt2_11-18-22_1710.pcap				
File	Edit View Go Capture Analyze S	tatistics Telephony	Wireless Tools H	elp	
	🔳 🖉 🛞 🚞 🗋 🗙 🏹 🍕	• 🔿 😫 🕌 🛓	<b>_ @</b> Q	e !!!	
	ngap				
No.	Time	Source	Destination	Protocol	Length Info
	137 2022-11-18 17:17:40.193924	10.220.67.19	10.205.67.204	NGAP/NAS-5GS/NAS-5GS	210 InitialUEMessage, Registration request, Registration request
	138 2022-11-18 17:17:40.196040	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	118 SACK (Ack=0, Arwnd=32768) , DownlinkNASTransport, Identity request
	140 2022-11-18 17:17:40.308451	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	186 UplinkNASTransport, Identity response
	142 2022-11-18 17:17:40.365217	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	142 DownlinkNASTransport, Authentication request
	144 2022-11-18 17:17:40.428006	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	150 UplinkNASTransport, Authentication response
	145 2022-11-18 17:17:40.439472	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	134 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command
	146 2022-11-18 17:17:40.448703	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	222 SACK (Ack=2, Arwnd=16384) , UplinkNASTransport
< -					
	✓ ProtocolIE	-Field			
	id: id	-NAS-PDU (38)			
	critic	ality: reject (0)			
	∨ value				
	✓ NA5	5-PDU: 7e012929a64	4c107e00572d10311d	c4200b607182669ad560873	cde9f
	v	Non-Access-Strat	um 5GS (NAS)PDU		
		✓ Security pro	tected NAS 5GS me	ssage	
		Extended	protocol discrimi	nator: 5G mobility manag	gement messages (126)
			= Spare Half Oct		
				r type: Integrity protec	ted (1)
			uthentication cod	e: 0x2929a64c	
			number: 16		
		✓ Plain NAS 56			
				nator: 5G mobility manag	gement messages (126)
1			= Spare Half Oct		ze, not security protected (0)
					ge, not security protected (0)
			ation response pa	on response (0x57)	
			nt ID: 0x2d	i dile cei	
		Lengt			
			311cc4200b6071826	59ad560873cde9f	
	✓ Item 3: id-Us	erLocationInforma			
	✓ ProtocolIE				
1		-UserLocationInfo	rmation (121)		
		ality: ignore (1)			
	✓ value	, <u>,</u> , (-)			

Figure 16: NEA2 AMF/UE Authentication Response

csric_tests_01_prt2_11-18-22_1710.pcap	
le Edit View Go Capture Analyze St	atistics Telephony Wireless Tools Help
ngap	
Time 137 2022-11-18 17:17:40.193924 138 2022-11-18 17:17:40.196940 140 2022-11-18 17:17:40.365217 142 2022-11-18 17:17:40.365217 144 2022-11-18 17:17:40.428066 145 2022-11-18 17:17:40.439472 146 2022-11-18 17:17:40.448703	10.205.67.204         10.220.67.19         NGAP/NAS-565         142 DownlinkNASTransport, Authentication request           10.220.67.19         10.205.67.204         NGAP/NAS-565         150 UplinkNASTransport, Authentication response
critica v value RAN V Item 2: id-NAS V ProtocollE id: id- critica v value v NAS	RAW-UE-NGAP-ID (85) ality: reject (0) I-UE-NGAP-ID: 16790010 -PDU
	<pre>&gt; Security protected NAS 565 message Extended protocol discriminator: 56 mobility management messages (126) 0000 = Spare Half Octet: 0  0011 = Security header type: Integrity protected with new 565 security context (3) Message authentication code: 0x7d273240 Sequence number: 0 &gt; Plain NAS 565 Message Extended protocol discriminator: 56 mobility management messages (126) 0000 = Spare Half Octet: 0  0000 = Security header type: Plain NAS message, not security protected (0) Message type: Security mode command (0x5d) &gt; NAS security algorithms 0010 = Type of citohering algorithm: 128-56-E42 (2)  0010 = Type of integrity protection algorithm: 128-56-E42 (2) 0000 = Spare Half Octet: 0 &gt; NAS key set identifier - ngKSI  001 = NAS key set identifier: 1 &gt; UE security capability - Replayed UE security capabilities</pre>

Figure 17: NEA2 Ciphering Command

🚄 C5	sric_tests_01_prt2_11-18-22_1710.pcap				
File	Edit View Go Capture Analyze St	tatistics Telephony	Wireless Tools H	elp	
	🔳 🖉 💿 🚞 🛅 🕱 🍯 🔍 🔶	• 🔿 😫 🕌 🛓		€.	
nga	ap				
No.	Time	Source	Destination	Protocol	Length Info
	142 2022-11-18 17:17:40.365217	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	142 DownlinkNASTransport, Authentication request
	144 2022-11-18 17:17:40.428006	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	150 UplinkNASTransport, Authentication response
	145 2022-11-18 17:17:40.439472	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	134 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command
	146 2022-11-18 17:17:40.448703	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	222 SACK (Ack=2, Arwnd=16384) , UplinkNASTransport
	147 2022-11-18 17:17:40.455974	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	142 SACK (Ack=3, Arwnd=32768) , DownlinkNASTransport, Security mode command
	148 2022-11-18 17:17:40.468290	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	158 SACK (Ack=3, Arwnd=16384) , UplinkNASTransport
	150 2022-11-18 17:17:40.665721	10.205.67.204	10.220.67.19	NGAP	182 InitialContextSetupRequest
	151 2022-11-18 17:17:40.688484	10.220.67.19	10.205.67.204	NGAP	94 InitialContextSetupResponse
	✓ value				
		-UE-NGAP-ID: 1679	00010		
	V Item 2: id-NAS				
	ProtocolIE				
		-NAS-PDU (38)			
		ality: reject (0)			
	✓ value				
				e6cd687e4d†72e2066b8	8126f1de88b7c6b0f9898529cc
	v	Non-Access-Strat			
			tected NAS 5GS me		
					management messages (126)
			= Spare Half Oct		
			<pre>uthentication cod</pre>		protected and ciphered with new 5GS security context (4)
			number: 0	ie: 0x6/50450/	
		<ul> <li>Plain NAS 56</li> </ul>			
				inator: Unknown (49)	
			5GS PD 49 (Unkno		
					5GS PD 49 (Unknown)]
			lot a NAS 5GS PD 4		ses to is (similarly)
			everity level: En		
			iroup: Protocol]		
	>	Data (84 bytes)			
		erlocationInforma	tion		

Figure 18: NEA2 Uplink NAS Transport Ciphering – Uplink Transport Data is encrypted

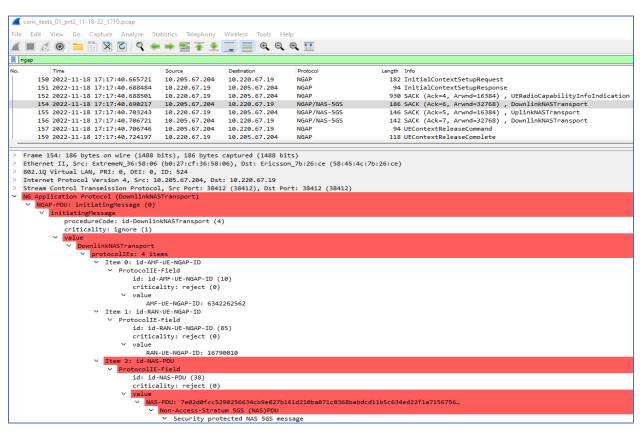


Figure 19: NEA2 Downlink NAS Transport Ciphering – Downlink Transport Data is encrypted

## Success Criteria:

Only NAS messages without user identities (e.g. SUPI, IMEI, etc) are exchanged between smartphone and AMF prior to establishing an encrypted channel. These NAS messages may contain temporary identifiers (TMSI, GUTI, etc.).

After establishment of the encrypted channel, all NAS messages are encrypted, enabling user identity information to be safely exchanged. If the encrypted channel is disabled, messages containing user identities are exchanged between the UE and AMF without encryption.

#### Results

Condition	Status
Only non-user information is observable prior to NAS encryption	Only SUCI is
	transmitted
After NAS encryption, all NAS messages are encrypted	Messages are
	encrypted with NEA2
If the encrypted channel is disabled, messages containing user	Message details are
identities are exchanged between UE and AMF without encryption	visible with NEA0
Overall Test	Success

# Test Case 2: CSRIC 7 WG 3 – RRC Signaling Confidentiality

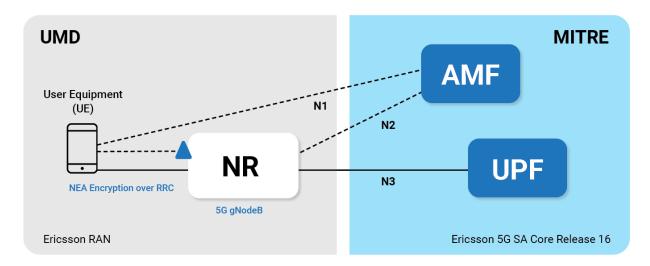


Figure 20: Test Case SA-02 Configuration

# Test Case ID: TC-SA-02

# Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the RRC signaling confidentiality, but optional for service providers to use. Given this standards requirement, CSRIC VII recommends protection of the RRC-signaling confidentiality. Only non-user identity related information shall be conveyed prior to security context being established.

This test involves first demonstrating the visibility of identity-related data when no encryption (NULL scheme) is used and then subsequently demonstrating the concealment of that data when RRC encryption is enabled.

Used	Test Point	Description and Use
	TP1-S	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
Х	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
	TP7	CNOM tool accessing DMC messages
	TP8	Applications running on application server in MITRE facility

# Test points used:

This test has two parts: 1) with NEA0 (no encryption) and 2) with NEA2 activated to encrypt RRC signaling. Figure 21 shows the command line interface setting the RRC encryption on the RAN to use NULL (NEA0) as the first priority.

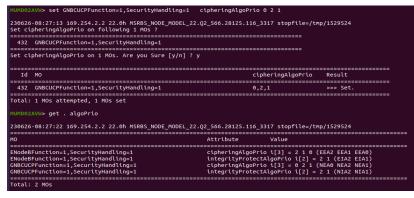
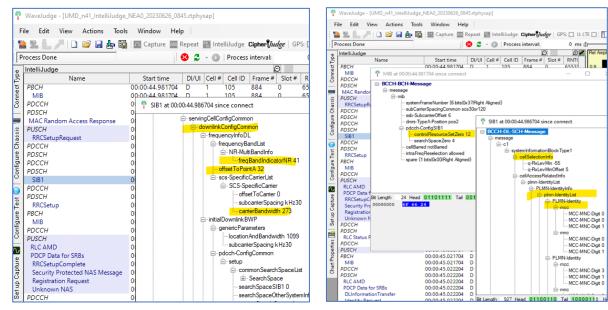


Figure 21: Setting RAN RRC encryption to NEA0



*Figure 22: WaveJudge/IntelliJudge capture of N41 specifications* 

Figure 23: WaveJudge/IntelliJudge capture of PLMN information

Figure 22 and Figure 23 show the UE attach process as captured by the WaveJudge/IntelliJudge tool. Figure 24 and Figure 25 show WaveJudge captures of messages processed with the NEA0 (NULL) algorithm. Because the ciphering algorithm in use is NEA0, all the "security protected" messages can be read in clear text.

Т	WaveJudge - [UMD_n41_IntelliJud		Window	Help	1					
Fil	le Edit View Actions To	ools	window		1.					
	🗶 📗 🥕 🗋 🔛 😓	Cip	ner Judge	GPS: [	🗆 U: L1		- 🖽 -	📠 🕂	$\equiv \sim$	🚼 🖷
Pr	rocess Done			1 😒	2 -	O P	rocess int	terval:		0 ms
л	Capture 🔤 Repeat 🔐 IntelliJu	dge	m	s Trig	gers »	Powe	er >>			
	IntelliJudge									
	Name		Start ti		DI/UI	Cell #	Cell ID	Frame #	Slot #	RNT
	RRCSetup		00:00:44.9		D	i	105	885	0	2007
	MIB		00:00:45.0	01704	D	1	105	886	0	6553
- 1	RLC AMD		00:00:45.0		U	1	105	886	4	2007
1	PDCP Data for SRBs RRCSetupComplete		00:00:45.0		U U	1	105 105	886 886	4 4	2007
	Security Protected NAS Messag		00:00:45.0		Ŭ	1	105	886	4	2007
1	Registration Request		00:00:45.0		Ū	1	105	886	4	2007
'n	Unknown NAS		00:00:45.0	03704	U	1	105	886	4	2007
1	RLC Status PDU		00:00:45.0		D	1	105	886	10	2007
	MIB RLC AMD		00:00:45.0		D	1	105 105	888 888	0	6553 2007
-	PDCP Data for SRBs		00:00:45.0		D	1	105	888	1	2007
Г	RRCSetupRequest at 00:00:44.9				-			_		×
-										
	i ⊂ c1 i mcSetup Request mcSetup Request i mcSetup Request i mcSe	alue {39   Cause m	io-Signalling		light Alig	ned}				
	i mc Setup Request i mc Setup Request i ue-Identity i andom Va i spare {1 bits 0	alue (39 l Cause m 0x00 Righ	io-Signalling nt Aligned}							7 7 7
	rrcSetup Request     rrcSetup Request     rrcSetup Request     ···· ue-Identity     ······ random Va     ····· spare {1 bits[0     Security Protected NAS Mes	alue (39   Cause m 0x00 Righ	o-Signalling nt Aligned} 00:00:45.00							7. 7. 7. 7.
	rrcSetup Request     rrcSetup Request     rrcSetup Request     ····e-Identity     ·····r andomVa     ······spare {1 bits 0     Security Protected NAS Mess     Security Protected NAS Mess	alue {39   Cause m 0x00 Righ ssage at essage	no-Signalling nt Aligned} 00:00:45.00							7. 7. 7. 7.
		alue (39) Cause m 0x00 Righ ssage at essage agement	no-Signalling nt Aligned} 00:00:45.00	03704 sir	nce con	nect	Octet Len	gth		7. 7. 7. 7.
	in rc Setup Request     in Setup Request     in rc Setup Request     in random Va     in random Va     in random Va     in spare {1 bits[0]     Security Protected NAS Mes     in EPD 7 => 5GS mobility man     in Protocol Discriminator 14 =>     in Reserved OK	alue {39   Cause m (x00 Righ ssage at essage agement > Reserv	no-Signalling nt Aligned} 00:00:45.00 t messages ed For Exter	03704 sir	nce con	nect	Octet Len	gth		7 7 7
	rrcSetup Request     rrcSetup Request     rrcSetup Request     rrcSetup Request     readom/s     rrandom/s     spare {1 bits 0     Security Protected NAS Mes     FPD 7 => 5GS mobility man     Protocol Discriminator 14 =>     Reserved OK     Security Header Type 1 =>	alue {39   Cause m 0x00 Righ ssage at essage agement > Reserv	no-Signalling nt Aligned} 00:00:45.00 t messages ed For Exter protected	03704 sir	nce con	nect	Octet Len	gth		7 7 7
	- mc Setup Request     - mc Setup Request     - ue-Identity     - ue-Identity     - ue-Identity     - stablishment     - spare {1 bits[0     ** Security Protected NAS Mes     EPD 7 => 5GS mobility man     Protocol Discriminator 14 =>     Reserved OK     Security Header Type 1 =>	alue {39   Cause m 0x00 Rights ssage at essage agement > Reserv Integrity ode 0x66	no-Signalling nt Aligned} 00:00:45.00 t messages ed For Exter protected 67B1A6	03704 sir	nce con	nect To One (				7. 7. 7. 7.
Bi	····rcSetupRequest     ·····rcSetupRequest     ·································	alue {39   Cause m 0x00 Righ ssage at agement > Reserv Integrity de 0x66	o-Signalling nt Aligned} 00:00:45.00 t messages ed For Exter protected 67B1A6 gistration F	D3704 sin	The PD	nect To One (				7. 7. 7. 7.
	····rcSetupRequest     ·····rcSetupRequest     ·································	alue {39 Cause m x00 Righ ssage at agement > Reserv Integrity de 0x66 m Re	no-Signalling nt Aligned} 00:00:45.00 t messages ed For Exter protected 67B1A6	D3704 sin Insion Of Request	The PD at 00:00	nect To One ( :45.0037	704 since	connect		7 7 7
Bindro da too	····rcSetupRequest     ·····rcSetupRequest     ·································	alue {39   Cause m \x00 Right ssage at essage agement Reserv Integrity de 0x66 \frac{1}{2} Reserves Integrity de 0x66	io-Signalling tt Aligned} 00:00:45:00 tt messages ed For Exter protected 67B1A6 gistration gistration EPD 7 => 5 Protocol Dis	03704 sin nsion Of Request Request GS mobi scriminato	The PD at 00:00	To One ( :45.0037	704 since	connect		
Bi	····rcSetupRequest     ·····rcSetupRequest     ·································	alue {39   Cause m \x00 Right ssage at essage agement Reserv Integrity de 0x66 \frac{1}{2} Reserves Integrity de 0x66	o-Signalling tt Aligned) 00:00:45:00 tt messages ed For Exter protected 67B1A6 gistration F gistration F Bistration S Protocol Dia Reserved C	D3704 sin nsion Of Request Request GGS mobi scriminato DK	The PD at 00:00 t ity mana or 14 =>	nect To One ( 2:45.003) igement ( Reserve	704 since messages d For Exte	connect ension Of T	he PD To	× One Or
Bi	····rcSetupRequest     ·····rcSetupRequest     ·································	alue (39) Cause m x00 Right ssage at essage agement Reserv Integrity de 0x66 <sup>®</sup> Re	o-Signalling t Aligned} 00:00:45.00 t messages ed For Exter protected 67B1A6 gistration F gistration EPD 7 => 5 Protocol Dis Reserved C Security He	03704 sin nsion Of Request GS mobi scriminato JK ader Typ	The PD at 00:00 t ity mana or 14 => ve 0 => F	nect To One ( 45.003) Igement Reserve	704 since messages d For Exte 6 message	connect ension Of T	he PD To	× One O
Bi	····rcSetupRequest     ·····rcSetupRequest     ·································	alue (39) Cause m x00 Right sage at essage agement > Reserv Integrity ide 0x66 Re - Re - Re - Re	o-Signalling tt Aligned) 00:00:45:00 tt messages ed For Exter protected <u>67B1A6</u> gistration F gistration F Protocol Dis Reserved C Security He Message Id ngKSI	D3704 sin nsion Of Request GS mobi scriminat OK ader Typ lentity 65	The PD at 00:00 t ity mana or 14 => re 0 => F => Regi	nect To One ( 45.003) Igement Reserve	704 since messages d For Exte 6 message	connect ension Of T	he PD To	× One O
Bi	····rcSetupRequest     ·····rcSetupRequest     ·································	alue (39) Cause m x00 Right sage at essage agement > Reserv Integrity ide 0x66 Re - Re - Re - Re	o-Signalling t Aligned) 00:00:45.00 t messages ed For Exter protected 6781A6 gistration F gistration F Protocol Dia Reserved C Security He Message I Message I 5GS Regist	D3704 sin nsion Of Request Request GS mobi scriminato DK ader Typ lentity 65 ration Ty	The PD at 00:00 t ity mana or 14 => re 0 => F egi e	nect To One ( :45.0037 Igement Reserve Plain NAS stration I	704 since messages d For Exte 6 message Request	connect ension Of T	he PD To	× One O
Bi	····rcSetupRequest     ·····rcSetupRequest     ·································	alue (39) Cause m x00 Right sage at essage agement > Reserv Integrity ide 0x66 Re - Re - Re - Re	o-Signalling tt Aligned} 00:00:45:00 t messages ed For Exter protected 67B1A6 gistration F gistration EPD 7 => 5 Protocol Dii Reserved C Security He Message Id ngKSI 5GS Regist 	D3704 sin nsion Of Request Request GS mobi scriminato X ader Typ lentity 65 ration Ty on Reque	The PD at 00:00 t ity mana or 14 => e 0 => F => Regi est Pend	nect To One ( :45.003) igement i Reserve Plain NAS istration i ing 1 =>	704 since messages d For Exte 6 message Request	connect ension Of T	he PD To	× One O
Bi	····rcSetupRequest     ·····rcSetupRequest     ·································	alue (39) Cause m 2001Right ssage at essage agement Reserv Integrity de 0x66 TRe P Re	o-Signalling t Aligned) 00:00:45.00 t messages ed For Exter protected 6781A6 gistration F gistration F Protocol Dia Reserved C Security He Message I Message I 5GS Regist	D3704 sin nsion Of Request Request GS mobi scriminato K ader Typ ientity 65 ration Ty on Reque => Initial	The PD at 00:00 t ity mana or 14 => e 0 => F => Regi est Pend	nect To One ( :45.003) igement i Reserve Plain NAS istration i ing 1 =>	704 since messages d For Exte 6 message Request	connect ension Of T	he PD To	× One O
Bindro da too	inc Setup Request     inc space {1 bits 0     Security Protected NAS Mes     Security Header Type 1 =>     Message Authentication Co     SEQUENCE_NUMBER 8     Registration Request     Bit Length 576 Head 011111 0000000 7E 01 66 67 B1	alue (39) Cause m 2001Right sage at essage agement > Reserv Integrity de 0x66 Re - Re - Re - Re - Re	o-Signalling tt Aligned} 00:00:45:00 tt messages ed For Exter protected 67B1A6 gistration F gistration EPD 7 => 5 Protocol Dia Reserved C Security He Message Id ngKSI 5GS Regist SGS Regist UE Security 1 5GS Mobile	D3704 sin nsion Of Request GS mobi scriminate OK ader Typ lentity of 5 mage 1 pon Reque => Initial Identity	The PD at 00:00 t ity mana or 14 => e 0 => F => Registra Registra	nect To One ( :45.003) igement i Reserve Plain NAS istration i ing 1 =>	704 since messages d For Exte 6 message Request	connect ension Of T	he PD To	× One O
	inc Setup Request     inc Setup Request     inc Setup Request     inc Setup Request     inc and on Value Address     inc Security Protected NAS Mes     Security Protected NAS Mes     Protocol Discriminator 14 =>     Reserved OK     Security Header Type 1 =>     Message Authentication Co     SEQUENCE_NUMBER 8     Registration Request Bit Length 576 Head 011111 0000000 7E 01 66 67 B1 00000010 10 FF 00 9D BC	alue (39) Cause m 2001Right sage at essage agement > Reserv Integrity de 0x66 Re - Re - Re - Re - Re	t Aligned) 00:00:45:00 t messages ed For Exter protected 67B1A6 gistration F gistration EPD 7 => 5 Protocol Dia Reserved C Security He Message Id ngKSI 5GS Regist 	D3704 sin histori Of Request Request GS mobil scriminato X ader Typ lentity 65 ration Typ on Reque >> Initial I dentity I dentity I dentity	The PD at 00:00 t ity mana or 14 => e 0 => F => Registra Registra	nect To One ( :45.003) igement i Reserve Plain NAS istration i ing 1 =>	704 since messages d For Exte 6 message Request	connect ension Of T	he PD To	× One O
	<ul> <li>inc Setup Request</li> <li>setablishment</li> <li>spare {1 bits 0</li> <li>Security Protected NAS Mester</li> <li>inc Setup Protected NAS Mester</li> <li>inc Security Protected NAS Mester</li> <li>inc Security Protected NAS Mester</li> <li>inc Security Header Type 1 =&gt;</li> <li>inc Registration Request</li> <li>Bit Length 576 Head 011111</li> <li>0000000 7E 01 66 67 B1</li> <li>0000001 10 FF 00 9D E5</li> </ul>	alue (39) Cause m 2001Right sage at essage agement > Reserv Integrity de 0x66 Re - Re - Re - Re - Re	o-Signalling tt Aligned} 00:00:45:00 tt messages ed For Exter protected 67B1A6 gistration F gistration EPD 7 => 5 Protocol Dia Reserved C Security He Message Id ngKSI 5GS Regist SGS Regist UE Security 1 5GS Mobile	D3704 sin nsion Of Request Request GS mobil GS mobil Scriminato NK Scriminato Scr	The PD at 00:00 t ity mana or 14 => e 0 => F => Registra Registra	nect To One ( :45.003) igement i Reserve Plain NAS istration i ing 1 =>	704 since messages d For Exte 6 message Request	connect ension Of T	he PD To	× One Or

WaveJudge - [UMD\_n41\_IntelliJudge\_NEA0\_20230626\_0845.rtphysap]

Figure 24: Unencrypted RRC messages

爷	WaveJudg	e - [UMD	_n41_Intell	ibuuge_i	_								
F	ile Edit	View	Actions	Tools	Window	Help							
1.5	8	210	💕 🖬 i	🍌 词 (	Cipher	GPS:	🗆 1): C			· · · · · · · · · · · · · · · · · · ·	<b>I</b>	<del>11</del>	
E P	rocess Don	<u> </u>		_			-		Process in			0 ms @	
1	🗖 Capture 🏧 Repeat 🐘 IntelliJudge 🛛 ms						Triggers >> Power >>						
Ð	IntelliJudg	je											
Connect Type		Nouelo	ame		Start 1		DI/UI	Cell #	Cell ID	Frame #	Slot #	RNTI	
ect		tion Reg			00:00:45.		ŭ	1	105	907	14	20074 -	
u u		/ModeCo			00:00:45.		Ď	1	105	935	12	20074 -	
0	UECapa	bilityEng	uiry		00:00:45.	497704	D	1	105	935	12	20074 -	
-	Security	/ModeCo	mplete		00:00:45.	508704	U	1	105	936	14	20074 -	
	UECapa	bilityInfo	rmation		00:00:45.	514071	U	1	105	937	4	20074	
18.56		mationTr			00:00:45.		D	1	105	938	6	20074 -	
ਤੱ			ed NAS Me	ssage	00:00:45.		D	1	105	938	6	20074 -	
9		ation Acc			00:00:45.		D	1	105	938	6	20074 -	
figr		mationTr	anster ed NAS Me		00:00:45.		U	1	105 105	939 939	4 4	20074 -	
	Security		a NAS Me	ssage	00:00:45.	533704							
Į,	Pagister	tion Con	mlata	-	00.00.45	522704							
📃 🚽 Configure Chassis		Message	mand at 00	):00:45.49	00:00:45.	onni 🌴	Securi	ty Prol	ected N	939 S Message AS Messa	ge , MA	CError:	
Ŷ	SecurityM DL-DCCH message	odeComi Message securityMo - rrc-Tra - critica	odeComman InsactionIde Extensions curityMode( ⊖- securityCo ⊡- securityCo	id entifier 0 Command onfigSMC ityAlgorithr <b>pheringAlg</b>	7704 since co	onn 🐐	Securi Securi EPI Prot Res Sec Met	ty Prot ty Prot D 7 => 5 tocol Di served ( sage A QUENC	ected NA GS mobilit scriminator DK eader Type	S Message AS Message y managem 14 => Res 2 => Integ on Code 0x R 1	at 00:00: ge , MAA ent messa erved For ity protect	20074 - 45.524704 CError: ages Extension C	
Ŷ	SecurityM DI-DCCH message d-c1 d- message d- d- d- d- d- d- d- d- d- d-	e security Mo e critica crica critica crica critica critica critica critica critica critica cr	mand at 00 decomman insactionIde Extensions iccurityMode( - securityCode - securityCode	id entifier 0 Command onfigSMC ttyAlgorithm pheringAlg tegrityProt 00:45.524	nConfig gonthm nea0 Algorithm nia2		Securi Securi EPI Prot Res Sec Met	ty Prot ty Prot D 7 => 5 tocol Di served ( sage A QUENC	ected NA ected NA 5GS mobilit scriminator DK eader Type uthenticat E_NUMBE	S Message AS Message y managem 14 => Res 2 => Integ on Code 0x R 1	at 00:00: ge , MAA ent messa erved For ity protect	20074 - 45.524704 CError: ages Extension (	

Figure 25: Decipherable RRC messages when using NEA0

For the second part of the test, we set NEA2 as the first priority for RRC encryption for the RAN, as shown in Figure 26. Figure 27 and Figure 28 show WaveJudge windows indicating that, because the ciphering algorithm in use is NEA2, all the RRC and upper layer are security protected and the contents cannot be deciphered.

Set cipheringAlgoPrio on following 1 MOs ?		file=/tmp/695942 
433 GNBCUCPFunction=1,SecurityHandling=1		
Set cipheringAlgoPrio on 1 MOs. Are you Sure	[y/n] ? y	===
Id MO	cipheringAl	goPrio Result
\$netconf_pid = 696610		
433 GNBCUCPFunction=1,SecurityHandling=1	2,1,0	>>> Set.
Total: 1 MOs attempted, 1 MOs set		
MUMD02AVW> get . algoprio		
230622-10:50:23 169.254.2.2 22.0h MSRBS_NODE	_MODEL_22.Q2_566.28125.116_3317 stop	file=/tmp/695942
мо	Attribute Value	
ENodeBFunction=1,SecurityHandling=1	cipheringAlgoPrio i[3] =	
ENodeBFunction=1.SecurityHandling=1	integrityProtectAlgoPrio	

*Figure 26: Setting RAN RRC encryption to NEA2* 

Ŷ	WaveJudge -	[UMD_n41_Inte	elliJudge_N	EA2_2023062	5_0810.rt	tphysap	o]		
F	ile Edit V	iew Actions	; Tools	Window	Help				
E No	×	4 🗅 😂 🖬	📥 🗐 o	Cipher Judge	GPS: [	1 U: LT	EDI	<b>FH</b> -	<b>m</b> +
E P	rocess Done							rocess int	
1	Capture m	Repeat 🐘 In	telliJudge	m	Trigo		Powe	er >>	
_	IntelliJudge							1	
Connect Type		Name		Start ti	me	DI/UI	Cell #	Cell ID	Frame
់ថ្ល	ULInformat	ionTransfer		00:01:18.6	57735	U	1	105	573
E.		otected NAS M	lessage	00:01:18.6		U	1	105	573
8		tion Response		00:01:18.6		U	1	105	573
		ionTransfer		00:01:18.6		D	1	105	576
		otected NAS M	lessage	00:01:18.6		D	1	105	576
221		ode Command ionTransfer		00:01:18.6		DU	1	105 105	576 577
Ę.		otected NAS M	lassaga	00:01:18.6		ŭ	1	105	577
Configure Chassis	Unknown		lessage	00:01:18.6		ŭ	1	105	577
B		deCommand		00:01:18.9		D	1	105	605
۳Ę.		ionTransfer		00:01:18.9		D	1	105	605
		deComplete		00:01:18.9		Ū	1	105	606
	DCCH-RRC			00:01:18.9	92735	U	1	105	607
t.	DCCH-RRC			00:01:19.0	64235	D	1	105	614
ë.	SecurityMo	deComplete		00:01:19.0	72735	U	1	105	615
ure	T SecurityMe	odeCommand	at 00:01:18	.971235 since	connec	t			_
Chart Properties 🚯 Set un Capture 🛃 Configure Jest 📀	·	= secu	sions ModeComma unityConfigSI securityAlgo inciphering integrityI t 00:01:18.9	and MC rithmConfig gAlgorithm nea: ProtAlgorithm ni 73735 since c	a2				
Char		dllnformation Tra mrc-Transac critical Exter	tion Identifier sions ation Transfe NonCritical E	er Extension {0 bits		RRC m	essage		
	SecurityMo UL-DCCH-	odeComplete a	at 00:01:18.9	987735 since o	onnect				_
	message ⊨∵c1		onIdentifier	D					

Figure 27: Protected RRC Messages

养	WaveJudg	o - FLIMD									
· ·	ile Edit	View	Actions	Tools	Window						
F	ie Edit					Help					
: 12	i 🗶 🔜	P 1	📂 🔛	😓 🗓	Cipher Judge	GPS:	🗆 U:			- <b>m</b> -	- 1
i P	rocess Don	e				1 🛛	2	- 🔘	Process in	terval:	
1	Capture	nn Repea	at 🔐 Inte	elliJudge	n	ns   Trig	gers >	> Po	wer >>		
e e	IntelliJudg										
Connect Type		Na	ame		Start 1	time	DI/L	JI Cell	# Cell ID	Frame	#
De L		mationTra			00:01:18.		U	1	105	577	- 4
l S			d NAS Me	essage	00:01:18.		U	1	105	577	4
	Unknow	vn NAS /ModeCor	mmand		00:01:18.		D	1	105	605	4
		mationTra			00:01:18.		D	i	105	605	6
2019		ModeCor			00:01:18.	987735	Ū	1	105	606	1
Configure Chassis	DCCH-F				00:01:18.		U	1	105	607	4
2	DCCH-F				00:01:19.		D	1	105	614	7
l g		ModeCor	mplete		00:01:19.		U	1	105 105	615 633	4
Б.	DCCH-F				00:01:19.		D	1	105	678	1
<u> </u>	DCCH-F				00:01:19.		ŭ	- i -	105	679	- i
$\odot$			ess Respo	nse	00:01:55.		Ď	i i	105	166	ō
88 D	CCH-RRC a				nest						
Ē		geClassExt	Error in s	subfield							
	·· message	geClassExt xtra Bytes	Error in s tension , Data Unde	subfield erflow: Ext	tra bytes at end	d of RRC	messa	ge			
* C	Message Message Padding/E CCH-RRC L-DCCH-N Message	geClassExt at 00:01:1 dessage	Error in s tension , Data Unde 9.064235 : , Error in ktension	subfield erflow: Ext since cor subfield	tra bytes at end						
* I	- message - message - Padding/E DCCH-RRC - DCCH-RRC - message - message	geClassExt at 00:01:1 dessage ageClassEx Extra Bytes	Error in s tension , DataUnd 9.064235 : , Error in dension s , DataUnd	enflow: Ext since con subfield derflow: Ext at 00:01:	tra bytes at end nnect xtra bytes at en	id of RR(	C messa				
* C	- message message Padding/E CCCH-RRC message mess	geClassExt xtra Bytes at 00:01:1 lessage , ageClassE Extra Bytes rityMode( CCH-Mes sssage c1 secu 	Error in a tension , Data Undo 9.064235 : , Error in dension , Data Undo Complete ssage , El mityModeCo rc-Transac priticalExter L. orticalExter	aubfield erflow: Ext since cor subfield defflow: E at 00:01: mor in su complete tionIdentifi nsions Statensions	tra bytes at end nnect ktra bytes at en 19.072735 sin abfield	d of RR(	C messa ect	age		_	[
↑         □           ↑         □           □         □	I- message I- message I- Padding/1 DOCCH-RCC I- DOCCH-RCC I- DOCCH-RCC I- DOCCH-RCC I- Ressage I- Ressage	geClassExt txtra Bytes at 00:01:1 lessage geClassE txtra Bytes rityMode(C CCH-Mess ssage - c1 - c1 - cc - cc	Error in a tension , Data Undo 9.064235 : , Error in dension , Data Undo Complete ssage , El mityModeCo rc-Transac priticalExter L. orticalExter	aubfield erflow: Ext since cor subfield derflow: E at 00:01: mor in su pomplete tionIdentif sions Extensions Data Under	tra bytes at end nnect ktra bytes at en 19.072735 sin ibfield ier 0 Future flow: Extra byte	d of RR(	C messa ect	age			
3it Len 000000 000000	Inessage Inessage Padding/E CCH-RRC IL-DCCH-N Inessage Iness	geClassExt xtra Bytes at 00:01:1 lessage ageClassE Extra Bytes rityMode( CCH-Mes ssage - c1 - secu - secu - c1 - secu - c1 - secu - c1 - secu - secu - c1 - secu - s	Error in s tension , Data Undo 9.064235 ; Error in dension s , Data Undo Complete asage , Er antty ModeCo criticalExter ham criticalExter ham criticalExter a Bytes , E D1:19.7177 ge , Error	subfield erflow: Ext since cor subfield deflow: E at 00:01: mor in su pomplete tion/dentification Stensions DataUnder 35 since of in subfield	tra bytes at eno nnect ktra bytes at en 19.072735 sin abfield ier 0 iFuture filow: Extra byte connect	d of RR( ce conn es at end	C messa ect	sge C messa	ige		

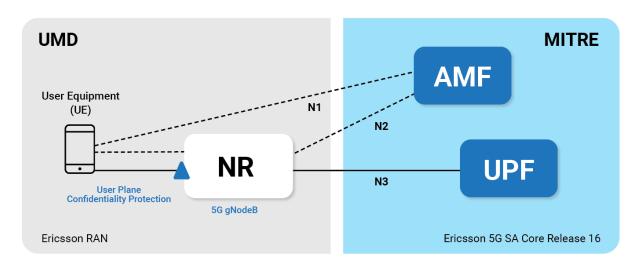
Figure 28: Protected RRC Messages

# Success Criteria:

RRC messages are observable over the RF channel when RRC encryption is disabled, and RRC messages are no longer observable when RRC encryption is enabled.

# Results

Condition	Status
RRC messages are observable over the RF channel when RRC	Contents of RRC messages
encryption is disabled (through use of NEA0 algorithm)	are fully decipherable by
	WaveJudge
RRC messages are no longer observable when RRC	WaveJudge shows contents of
encryption is enabled (through use of NEA2 algorithm)	encrypted messages as "Extra
	bytes at end of RRC message"
Overall Test	Success



# Test Case 3: CSRIC 7 WG 3 – Access Stratum User Plane Confidentiality

Figure 29: Test Case SA-03 Configuration

# Test Case ID: TC-SA-03

#### Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the user plane confidentiality, but optional for service providers to use. Given this standards requirement, CSRIC VII recommends user plane confidentiality protection over the access stratum be done at PDCP layer.

This test involves demonstrating that when confidentiality protection for the user plane is applied at the PDCP layer, no layers below PDCP are confidentiality-protected. User data sent via the UPF may be confidentiality protected.

This test also involves implementing and confirming user plane confidentiality protection over the access stratum at the PDCP layer. Layers below PDCP are not confidentiality-protected.

# Test points used:

Used	Test Point	Description and Use
	TP1-S	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
Х	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
	TP7	CNOM tool accessing DMC messages
	TP8	Applications running on application server in MITRE facility

We were unable to capture user plane messages on the WaveJudge and, as a result, were unable to verify over-the-air encryption of user plane data.

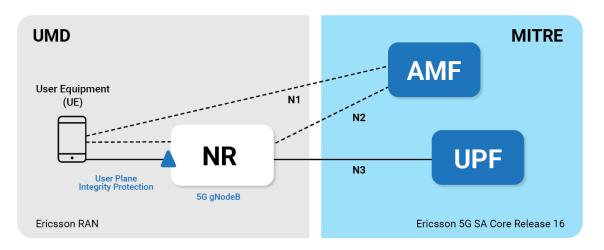
#### Success Criteria:

Once encrypted channel is established, user plane data will not be observable in the recorded data.

Confidentiality protection for the user plane is applied at the PDCP layer via 128-bit NEA algorithms.

#### Results

Condition	Status		
When encryption is disabled, all UP data will be observable	Unable to capture user plane		
	messages with WaveJudge		
When the encrypted channel is established, UP data will not	Unable to capture user plane		
be observable in the recorded data	messages with WaveJudge		
Overall Test	Limited by Test Capability		



# Test Case 4: CSRIC 7 WG 3 – Access Stratum User Plane Integrity

# Test Case ID: TC-SA-04 Description:

3GPP TS 33.501 requires UE to support integrity protection and replay protection of user data between the UE and the gNB, but the data rates at which it is supported are different between releases 15 and 16, and it is optional for service providers to use this feature.

CSRIC VII recommends that device OEMs and network infrastructure vendors support the Release 16 full rate capability, along with 128-NIA3 as defined in Annex D of 3GPP TS 33.501, and for operators to implement according to the service requirement. CSRIC VII recommends that user data integrity is mandatory for Release 16 U.S. deployments.

The Packet Data Convergence Protocol, as specified in TS 38.323 as between the UE and the NG-RAN, is responsible for user plane data integrity protection.

Figure 30: Test Case SA-04 Configuration

# Test points used:

Used	Test Point	Description and Use
	TP1-S	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
Х	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
	TP7	CNOM tool accessing DMC messages
	TP8	Applications running on application server in MITRE facility

As with TC-SA-03, the WaveJudge/IntelliJudge was unable to capture user plane messages. As a result, we were unable to confirm over-the-air integrity protection. However, the PDU Establishment message, as shown in Figure 31, does indicate the intent to apply integrity protection at the full rate.

10.205.67.153 - Remote Desktop Connection

: 🐘 🎥 🗽 🥕 🗋 🧀 🍰 🔚 🔚 🖾 Capture 🥅 Repeat 🎆 IntelliJudge Cipher (Judge   GPS: 🗌 U: LTE 🗌 🛐 🖽 🗸 🎬							
cess Done	1	8 💈	- 0	Process	interval:		0 ms ①
ntelliJudge					Θ	£≮	
Name	Start time	DI/UI	Cell #	Cell ID	Frame #	Slot #	
Name Security Protected NAS Message Registration Complete DLInformationTransfer Security Protected NAS Message Configuration Update Command ULInformationTransfer Security Protected NAS Message Uplink NAS Transport PDU Session Establishment Req RRCSetupRequest RRCSEtupRe	00:00:45.533704 00:00:45.533704 00:00:45.533704 00:00:45.545204 00:00:45.545204 00:00:45.728704 00:00:45.728704 00:00:45.728704 00:00:45.728704 00:00:45.728704 00:00:45.728704 U Session Establishn U Session Establishn U Session Establishn U Session Establishn DU Session ID 1 Procedure Transaction Message Identity 193 Integrity Protection Ma Maxmum data rate PDU Session Type IEI 9 Reserved OK Value 1 => IPv4 SGSM Capability IEI 40 Length 1 bytes Reserved OK Multi-homed IPv6	U U D D U U U U U U U U U U U U U U U U	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	105 105 105 105 105 105 105 105 105 105	Frame # 939 939 940 940 958 958 958 958 958 041 728704 sin 728704 sin rotect gity protect	Slot #           4           4           7           7           14           14           14           14           14           14           15           PD To One           st           tion for uplin	: Octet Length k 255 => Full data rate
	IntelliJudge         Name         Security Protected NAS Message         Registration Complete         DLInformationTransfer         Security Protected NAS Message         Configuration Update Command         ULInformationTransfer         Security Protected NAS Message         Uplink NAS Transport         PDU Session Establishment Req.         RRCSetupRequest         RRCSetupRequest	IntelliJudge     Name     Start time       Security Protected NAS Message     00:00:45:533704       Registration Complete     00:00:45:533704       DLInformationTransfer     00:00:45:545204       Configuration Update Command     00:00:45:545204       ULInformationTransfer     00:00:45:545204       ULInformationTransfer     00:00:45:545204       ULInformationTransfer     00:00:45:728704       Security Protected NAS Message     00:00:45:728704       UDU Session Establishment Req     00:00:45:728704       PDU Session Establishment Req     00:00:45:728704       RRCSetupRequest     RRCSetupRequest       RRCSetupRequest     PDU Session Establishment Req       RRCSetupRequest     PDU Session ID 1       Procedure Transactor     Message Identity 193:       PUU Session ID 1     Protocol Discriminator       PUU Session ID 1     Protocol Discriminator       PUU Session ID 1     Protocol Discriminator       McSetupRequest     Maximum data rate       RRCSetupRequest     Maximum data rate       RRCSetupRequest     PU Session Type       RRCSetupRequest     PSGM Capability       RRCSetupRequest     RRCSetupRequest       RRCSetupRequest     RRCSetupRequest       RRCSetupRequest     RRCSetupRequest       RRCSetupRequest     R	IntelliJudge       Name       Start time       DI/UI         Security Protected NAS Message       00:00:45:533704       U         Registration Complete       00:00:45:533704       U         DLInformationTransfer       00:00:45:545204       D         Security Protected NAS Message       00:00:45:545204       D         Configuration Update Command       00:00:45:545204       D         ULInformationTransfer       00:00:45:545204       D         UUInformationTransfer       00:00:45:728704       U         Uplink NAS Transport       00:00:45:728704       U         PDU Session Establishment Req       00:00:45:728704       U         RCSetupRequest       PDU Session Establishment Req       PDU Session Istablishment Req         RCSetupRequest       PRCSetupRequest       PDU Session Type       IEI 9         RCSetupRequest       POU Session Type       IEI 9       Reserved OK         RCSetupRequest       RCSetupRequest       PO	Image: Start time       D//U       Cell #         Security Protected NAS Message       00:00:45:533704       1         DLInformation Transfer       00:00:45:545204       1         Security Protected NAS Message       00:00:45:545204       1         Configuration Update Command       00:00:45:545204       1         ULInformation Transfer       00:00:45:545204       1         ULInformation Transfer       00:00:45:728704       1         Uplink NAS Transport       00:00:45:728704       1         PDU Session Establishment Request       RRCSetupRequest       PDU Session Establishment Request at         RRCSetupRequest       PDU Session Establishment Request at       PDU Session Establishment Request at         PDU Session Establishment Request       PDU Session Istablishment Request at       PDU Session Istablishment Request at         RRCSetupRequest       PDU Session Istablishment Request at       PDU Session Istablishment Request at         RRCSetupRequest       PDU Session Istablishment Request at       PDU Session Istablishment Request         RRCSetupRequest       RRCSetupRequest       Maximum data rate per UE for user         RRCSetupRequest       Maximum data rate per UE for user       Maximum data rate per UE for user         RRCSetupRequest       PDU Session Type       -IEI 9       -IEI 9 <t< td=""><td>Intellijudge       Name       Start time       DI/UI       Cell #       Cell ID         Security Protected NAS Message       00:00:45:533704       U       1       105         Registration Complete       00:00:45:533704       U       1       105         DLInformationTransfer       00:00:45:545204       D       1       105         Security Protected NAS Message       00:00:45:545204       D       1       105         Configuration Update Command       00:00:45:545204       D       1       105         ULInformationTransfer       00:00:45:545204       D       1       105         Security Protected NAS Message       00:00:45:728704       U       1       105         Uplink NAS Transport       00:00:45:728704       U       1       105         PDU Session Establishment Request       RRCSetupRequest       PDU Session Establishment Request at 00:00:45:       1       105         RRCSetupRequest       PDU Session Establishment Request       PDU Session Ib 1       1       105         RRCSetupRequest       PDU Session Ib 1       Protocol Discriminator 14 =&gt; Reserved For Extens       Procedure Transaction Identifier 7         Message Identity 193 =&gt; PDU Session Type       IE 19       Maximum data rate per UE for userplane inte      <t< td=""><td>IntelliJudge       Image: Start time       D//UI       Cell ID       Frame #         Security Protected NAS Message       00:00:45.533704       0       1       105       939         Registration Complete       00:00:45.533704       0       1       105       939         DLInformationTransfer       00:00:45.545204       D       1       105       940         Security Protected NAS Message       00:00:45.545204       D       1       105       940         Configuration Update Command       00:00:45.728704       U       1       105       958         OUInformationTransfer       00:00:45.728704       U       1       105       958         PDU Session Establishment Request       00:00:45.728704       U       1       105       958         PDU Session Establishment Request       00:00:45.728704       U       1       105       958         PDU Session Establishment Request       PDU Session Establishment Request       00:00:45.728704       U       1       105       958         RRCSetupRequest       RRCSetupRequest       PDU Session Establishment Request       POU Session Establishment Request       PDU Session ID 1       Procedure Transaction Identifier 7       Message Identity 193 =&gt; PDU Session Establishment Request       PDU Session</td><td>IntelliJudge       Image: Start time       D//UI       Process interval:         IntelliJudge       Start time       D//UI       Cell #       Cell ID       Frame #       Slot #         Security Protected NAS Message       00:00:45.533704       U       1       105       939       4         DLInformationTransfer       00:00:45.545204       D       1       105       940       7         Security Protected NAS Message       00:00:45.545204       D       1       105       940       7         Configuration Update Command       00:00:45.545204       D       1       105       940       7         ULInformationTransfer       00:00:45.728704       U       1       105       958       14         PDU Session Establishment Reque.       00:00:45.728704       U       1       105       958       14         PDU Session Establishment Request       PDU Session ID 1       PDU Se</td></t<></td></t<>	Intellijudge       Name       Start time       DI/UI       Cell #       Cell ID         Security Protected NAS Message       00:00:45:533704       U       1       105         Registration Complete       00:00:45:533704       U       1       105         DLInformationTransfer       00:00:45:545204       D       1       105         Security Protected NAS Message       00:00:45:545204       D       1       105         Configuration Update Command       00:00:45:545204       D       1       105         ULInformationTransfer       00:00:45:545204       D       1       105         Security Protected NAS Message       00:00:45:728704       U       1       105         Uplink NAS Transport       00:00:45:728704       U       1       105         PDU Session Establishment Request       RRCSetupRequest       PDU Session Establishment Request at 00:00:45:       1       105         RRCSetupRequest       PDU Session Establishment Request       PDU Session Ib 1       1       105         RRCSetupRequest       PDU Session Ib 1       Protocol Discriminator 14 => Reserved For Extens       Procedure Transaction Identifier 7         Message Identity 193 => PDU Session Type       IE 19       Maximum data rate per UE for userplane inte <t< td=""><td>IntelliJudge       Image: Start time       D//UI       Cell ID       Frame #         Security Protected NAS Message       00:00:45.533704       0       1       105       939         Registration Complete       00:00:45.533704       0       1       105       939         DLInformationTransfer       00:00:45.545204       D       1       105       940         Security Protected NAS Message       00:00:45.545204       D       1       105       940         Configuration Update Command       00:00:45.728704       U       1       105       958         OUInformationTransfer       00:00:45.728704       U       1       105       958         PDU Session Establishment Request       00:00:45.728704       U       1       105       958         PDU Session Establishment Request       00:00:45.728704       U       1       105       958         PDU Session Establishment Request       PDU Session Establishment Request       00:00:45.728704       U       1       105       958         RRCSetupRequest       RRCSetupRequest       PDU Session Establishment Request       POU Session Establishment Request       PDU Session ID 1       Procedure Transaction Identifier 7       Message Identity 193 =&gt; PDU Session Establishment Request       PDU Session</td><td>IntelliJudge       Image: Start time       D//UI       Process interval:         IntelliJudge       Start time       D//UI       Cell #       Cell ID       Frame #       Slot #         Security Protected NAS Message       00:00:45.533704       U       1       105       939       4         DLInformationTransfer       00:00:45.545204       D       1       105       940       7         Security Protected NAS Message       00:00:45.545204       D       1       105       940       7         Configuration Update Command       00:00:45.545204       D       1       105       940       7         ULInformationTransfer       00:00:45.728704       U       1       105       958       14         PDU Session Establishment Reque.       00:00:45.728704       U       1       105       958       14         PDU Session Establishment Request       PDU Session ID 1       PDU Se</td></t<>	IntelliJudge       Image: Start time       D//UI       Cell ID       Frame #         Security Protected NAS Message       00:00:45.533704       0       1       105       939         Registration Complete       00:00:45.533704       0       1       105       939         DLInformationTransfer       00:00:45.545204       D       1       105       940         Security Protected NAS Message       00:00:45.545204       D       1       105       940         Configuration Update Command       00:00:45.728704       U       1       105       958         OUInformationTransfer       00:00:45.728704       U       1       105       958         PDU Session Establishment Request       00:00:45.728704       U       1       105       958         PDU Session Establishment Request       00:00:45.728704       U       1       105       958         PDU Session Establishment Request       PDU Session Establishment Request       00:00:45.728704       U       1       105       958         RRCSetupRequest       RRCSetupRequest       PDU Session Establishment Request       POU Session Establishment Request       PDU Session ID 1       Procedure Transaction Identifier 7       Message Identity 193 => PDU Session Establishment Request       PDU Session	IntelliJudge       Image: Start time       D//UI       Process interval:         IntelliJudge       Start time       D//UI       Cell #       Cell ID       Frame #       Slot #         Security Protected NAS Message       00:00:45.533704       U       1       105       939       4         DLInformationTransfer       00:00:45.545204       D       1       105       940       7         Security Protected NAS Message       00:00:45.545204       D       1       105       940       7         Configuration Update Command       00:00:45.545204       D       1       105       940       7         ULInformationTransfer       00:00:45.728704       U       1       105       958       14         PDU Session Establishment Reque.       00:00:45.728704       U       1       105       958       14         PDU Session Establishment Request       PDU Session ID 1       PDU Se

Figure 31: WaveJudge capture of PDU Establishment message

#### Success Criteria:

Integrity protection for the user plane is applied full-rate at the PDCP layer.

Examine data collected by the RF monitoring tool for the user plane messages. Confirm the integrity check fields are populated.

# Results

Condition	Status
Integrity protection for the user plane is applied full-rate at	PDU Establishment message
the PDCP layer	indicates integrity protection
	applied at full rate
Integrity check fields are populated	Unable to capture and read
	user plane messages over the
	air with WaveJudge
Overall Test	Limited by Test Capability

# Test Case 5: CSRIC 7 WG 3 – SUPI/SUCI Privacy Enabled

Test Case ID: TC-SA-05-1

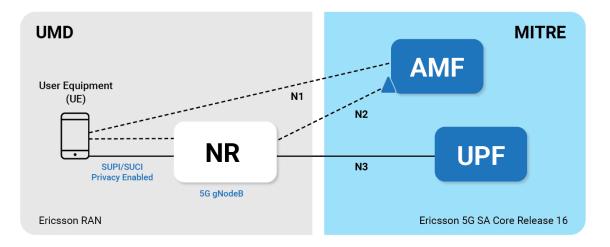
#### Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the SUPI/IMSI privacy; however, 3GPP allows for some exceptions where the Subscription Concealed Identifier (SUCI) may use the null scheme (i.e., the identity is not protected).

CSRIC VII recommends that devices and networks in the U.S. use IMSI privacy (SUCI) and not use the null scheme, except when the UE is requesting emergency services.

It is recommended that no other exceptions allowed by 3GPP in Release 16 (for null scheme SUCI) be used by devices or networks in the U.S. This may result in roaming 5G devices configured by operators from outside the U.S. being unable to connect to 5G SA networks, but that they use 4G LTE networks instead.

To avoid identifying a handset by its Subscription Permanent Identifier (SUPI), 5G uses the subscription concealed identifier (SUCI) to encrypt the SUPI to exchange identity information between the UE and 5G NR. SUPI/SUCI privacy is used for all services, except emergency services and non-authenticated roaming emergency calls.



#### Figure 32: Test Case SA-05 Configuration

We used logs from CSRIC Test TC-SA-01 above, with highest priority set for NEA0 (null algorithm).

# Test points used:

Used	Test Point	Description and Use
	TP1-SW	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
Х	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
	TP7	CNOM tool accessing DMC messages
	TP8	Applications running on application server in MITRE facility

Figure 33 shows the initial UE registration message in which the type of identity is SUCI. Figure 34 shows the uplink NAS transport message with registration request that also provides the type of identity as SUCI. Lastly, Figure 35 shows the downlink NAS transport message indicating the encryption algorithm to use is NEA0.

Edit View Go Capture Analyze Statistics Telephony Wireless Tools H	Help	
= 1 🖉 🕒 🗋 🕅 🖉 🤇 🗣 🗯 🕾 📜 📃 🔍 Q, Q, M		
ap		
Time Source Destination Protocol	Length Info	
101 2022-11-18 16:48:49 10.220.67 10.205.67 NGAP/NAS-565	182 InitialUEMessage, Registration request	
103 2022-11-18 16:48:49 10.205.67 10.220.67 NGAP/NAS-5GS	142 DownlinkNASTransport, Authentication request	
105 2022-11-18 16:48:50 10.220.67 10.205.67 NGAP/NAS-5GS	142 UplinkNASTransport, Authentication response	
106 2022-11-18 16:48:50 10.205.67 10.220.67 NGAP/NAS-5GS	134 SACK (Ack=1, Arwnd=32768) , DownlinkNASTransport, Security mode	
107 2022-11-18 16:48:50 10.220.67 10.205.67 NGAP/NAS-5GS/N.		
108 2022-11-18 16:48:50 10.205.67 10.220.67 NGAP/NAS-5GS	142 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode	
109 2022-11-18 16:48:50 10.220.67 10.205.67 NGAP/NAS-5GS	158 SACK (Ack=2, Arwnd=16384) , UplinkNASTransport, Security mode co	mplete
113 2022-11-18 16:48:50 10.205.67 10.220.67 NGAP	182 InitialContextSetupRequest	
115 2022-11-18 16:48:50 10.220.67 10.205.67 NGAP	94 InitialContextSetupResponse	
116 2022-11-18 16:48:50 10.220.67 10.205.67 NGAP	914 UERadioCapabilityInfoIndication	
118 2022-11-18 16:48:50 10.205.67 10.220.67 NGAP/NAS-5GS	186 SACK (Ack=5, Arwnd=32768), DownlinkNASTransport, Registration a	ccept
.111 = NAS key set ide		b0 27 cf 3e d4 06 58
✓ 56S mobile identity		08 00 45 a0 00 a4 00 0
Length: 54		43 13 0a cd 43 cc 96 0
0 = Spare: 0	003	5c 76 00 03 00 83 02
.000 = SUPI format: IM	NST (0) 0040	00 3c 00 0f 40 6f 00 0
0 = Spare: 0	005	31 f0 00 26 00 43 42
001 = Type of identit		0 10 f0 ff 02 0c 03 78
Mobile Country Code (MCC):	00/1	72 2f d7 a3 50 8a ad 2 b7 81 cc 7e 36 5b 22
Mobile Network Code (MWC):		47 d0 a3 2e 04 f0 70
Routing indicator: 0		10 01 86 a2 12 d0 13
		00 5a 40 01 18 00
Home network public key ide		
Home network public key ide	i7f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc7e365b22f8a0	
Home network public key ide V Scheme output: 037819cded0d		
Home network public key ide V Scheme output: 037819cded0d	17f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc7e365b22f8a0	
Home network public key ide ~ Scheme output: 037819cded0d ECC ephemeral public key	i7f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc7e365b22f8a0_ r: 037819cded0d7f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc;	
Home network public key ide ~ Scheme output: 0378196de000 ECC ephemeral public key Ciphertext: 22f8a0614b	i7f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc7e365b22f8a0_ r: 037819cded0d7f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc;	

Figure 33: UE with profile B – source core-side R6K

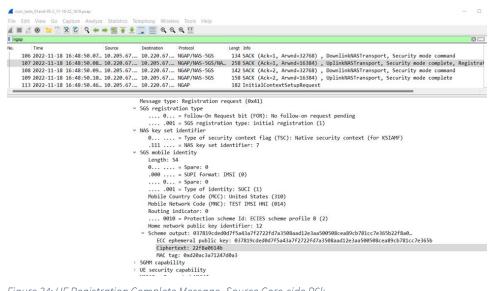


Figure 34: UE Registration Complete Message- Source Core-side R6k

csric_tests_01and-05-2_11-18-22_1610.pcap		-
e Edit View Go Capture Analyze	Statistics Telephony Wireless Tools Help	
🔳 🥼 😑 🚞 🖹 🕅 🍳 🗭	+ 🛯 🖡 🛓 🔽 🔳 @ @ @ II	
ngap		X
107 2022-11-18 16:48:50.08 108 2022-11-18 16:48:50.09	Source         Destination         Protocol         Lengt Info           10.205.67         10.220.67         NGAP/NAS-5GS         134 SACK (Ack=1, Arwind=32768), DownlinkNASTransport, Security mode command           10.220.67         10.205.67         NGAP/NAS-5GS         134 SACK (Ack=1, Arwind=32768), DownlinkNASTransport, Security mode complete, Reg           10.220.67         10.220.67         NGAP/NAS-5GS         142 SACK (Ack=2, Arwind=32768), DownlinkNASTransport, Security mode complete           10.220.67         10.205.67         NGAP/NAS-5GS         125 SACK (Ack=2, Arwind=32768), DownlinkNASTransport, Security mode complete	gist
	Extended protocol discriminator: 56 mobility management messages (126) 0000 = Spare Half Octet: 0 0000 = Security Mode command (0x5d) MKS security algorithms 0000 = Type of ciphering algorithm: 56-EA0 (null ciphering algorithm) (0) 0010 = Type of integrity protection algorithm: 128-56-EA2 (2) 0000 = Type of security context flag (TSC): Native security context (for KSIANF) 000 = MKS key set identifier: 0 V MKS key set identifier: 0 0 UE security capability - Replayed UE security capabilities V IESV request 1110 = Element ID: 0xe- 01 = JMESV request: IMESV requested (1) V MKS security algorithms - Selected EPS NAS security algorithms Element ID: 0x57 0	

Figure 35: NULL scheme in use - Source Core-side R6K

## Success Criteria:

Successful registration with encrypted SUPI.

#### Results

Condition	Status
Use of SUCI by UE in registration process	Success
Successful registration	Success
Overall Test	Success

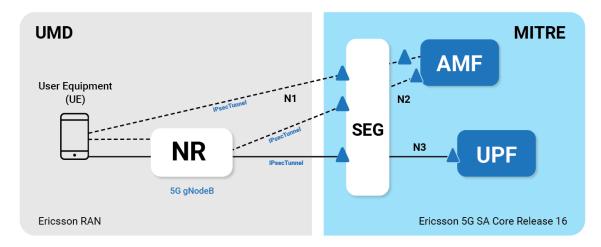
## Test Case 6: CSRIC 7 WG 3 – IPsec on Transport Links

#### Test Case ID: TC-SA-06

#### Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor support for) network security protection such as IPsec, but optional for service providers to use. Given this standards requirement, CSRIC VII recommends the use of IPsec or use of a tunneling technology for transport (e.g., VPN tunnels) for protection of network security.

This test involves demonstrating that when IPsec is used for confidentiality and integrity protection of user plane and signaling on the N1, N2, and N3 interfaces across the transport link, UP and CP traffic cannot be captured, modified, or injected with new packets.



#### Figure 36: Test Case SA-06 Configuration

# Test points used:

Used	Test Point	Description and Use
	TP1-SW	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
	TP2	WaveJudge interface
Х	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
Х	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
Х	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
Х	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
	TP7	CNOM tool accessing DMC messages
	TP8	Applications running on application server in MITRE facility

Similar to the previous tests, Network Slice 2 and UE2 with profile B were used for this test. The UE used for Slice 2 was a Sierra Wireless Modem, which is connected and controlled by a laptop outside the Faraday Cage. IPsec for for Slice 2 and control traffic was turned on/off as and when required.

This test has two parts, attempting to capture, modify, and inject user and control plane traffic: 1) without an IPsec tunnel and 2) with an IPsec tunnel.

Part 1: Traffic Modification without Enabled IPsec Tunnel between BBU and Core-Side R6K For the first part of the test, we ensured that the IPsec tunnel for the transport channel between the RAN and the core was off.

The UE was then restarted and attached to the 5G core, as shown in Figure 37. The larger window in the figure shows the contents of an initial context setup request message captured on the untrusted transport between the RAN and core. The inset figure shows a message within the core regarding the registration of the UE with IMSI used for this test. Figure 38 shows logs of both control plane and user plane messages after UE registration and ping started to the DN server (192.168.59.146). These packets are clearly visible on the transport channel when the IPsec tunnel is down and traffic is unencrypted.

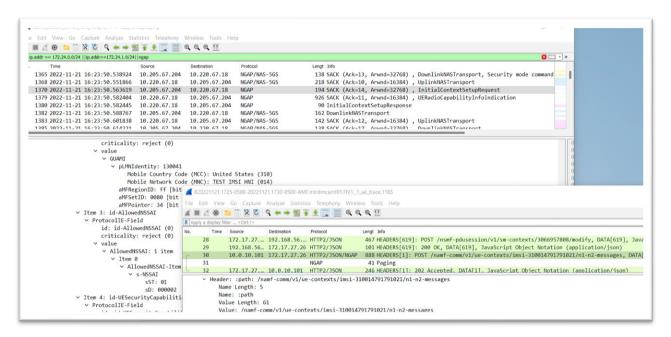


Figure 37: Packet captures at RAN-side switch and at the core showing UE registration over unencrypted transport

File Edit	ring from SLOT 2 Port 2	re Analyze Statistic	s Telephony Wireless T	fools Help	- 0
		\$			
Current	filter: ((!(eth.src == b4:	0c:25:e0:80:10)) && !(ip.s	rc == 128.8.46.80)) && !(eth.s	rc == 00:07:7d:d3:61:ed)	× 🖘 .
o.	Time	Source	Destination	Protocol	Length Info
12090	17:43:48.297457	10.220.67.18	10.205.67.204	SCTP	126 HEARTBEAT
12103	17:43:48.977029	10.220.67.18	10.205.67.204	NGAP/NAS-5GS/NAS	166 InitialUEMessage, Service request
12105	17:43:49.006529	10.220.67.18	10.205.67.204	NGAP	106 SACK (Ack=36, Arwnd=16384) , InitialContextSetupRespon
12109	17:43:49.062630	10.220.67.18	10.205.67.204	SCTP	62 SACK (Ack=38, Arwnd=16384)
12113	17:43:49.091145	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=336/20481, ttl=128
12114	17:43:49.092655	10.220.67.18	10.205.67.204	NGAP	110 PDUSessionResourceSetupResponse
12125	17:43:49.506190	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=337/20737, ttl=128
12144	17:43:50.497694	10.220.67.18	10.205.67.205	SCTP	126 HEARTBEAT
12148	17:43:50.526156	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=338/20993, tt1=128
12171	17:43:51.531162	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=339/21249, ttl=128
12189	17:43:52.571127	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=340/21505, tt1=128
12191	17:43:52.697440	10.220.67.18	10.205.67.204	SCTP	126 HEARTBEAT
12209	17:43:53.571175	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=341/21761, ttl=128
12228	17:43:54.591132	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=342/22017, ttl=128
12232	17:43:54.897701	10.220.67.18	10.205.67.205	SCTP	126 HEARTBEAT
10046	17.42.55 611007	173 34 1 3	100 160 50 146	GTD ATCHON	110 Echa (ning) naquast id_000001 cas_342/2022 ++1-120

Figure 38: Ping messages captured on the untrusted transport link between the RAN and core

Subsequently, we used TP4, a laptop connected to the transport channel, to capture user plane traffic, modify that traffic, and inject it into the transport channel. The data captured was saved to a file (ping\_111822.pcap), and we stopped pings from the UE. The modified data was injected using a laptop connected to the transport channel at the RAN-side switch (TP4), as shown in Figure 39Figure 39. To enhance the injection, the captured traffic is looped and replayed as quickly as possible using the loop and topspeed commands. Logs for the injected traffic are captured on the outgoing interface for the inject laptop (Figure 40), on the outgoing core-side R6K interface (Figure 41Figure 41), and in the ping responses displayed at the laptop connected to the UE (Figure 42).

F	daniel@daniel-Latitude-5520: ~/csric
Failed packets: 0	
Truncated packets: 0	
Retried packets (ENOBUFS): 0	
Retried packets (EAGAIN): 0	
daniel@daniel-Latitude-5520:~/csric\$ sudo tcpreplay	topspeed -i enp0s31f6 ping_111822.pcap
Actual: 122 packets (15456 bytes) sent in 0.000350 se	econds
Rated: 44160000.0 Bps, 353.28 Mbps, 348571.42 pps	
Statistics for network device: enp0s31f6	
Successful packets: 122	
Failed packets: 0	
Truncated packets: 0	
Retried packets (ENOBUFS): 0	
Retried packets (EAGAIN): 0	
daniel@daniel-Latitude-5520:~/csric\$ sudo tcpreplay	topspeed -i enp0s31f6 ping_111822.pcap
Actual: 122 packets (15456 bytes) sent in 0.000378 se	econds
Rated: 408888888.8 Bps, 327.11 Mbps, 322751.32 pps	
Statistics for network device: enp0s31f6	
Successful packets: 122	
Failed packets: 0	
Truncated packets: 0	
Retried packets (ENOBUFS): 0	
Retried packets (EAGAIN): 0	
daniel@daniel-Latitude-5520: <mark>~/csric\$ sudo tcpreplay</mark> ·	
Actual: 122 packets (15456 bytes) sent in 0.000379 se	econds
Rated: 40781002.6 Bps, 326.24 Mbps, 321899.73 pps	
Statistics for network device: enp0s31f6	
Successful packets: 122	
Failed packets: 0	
Truncated packets: 0	
Retried packets (ENOBUFS): 0	
Retried packets (EAGAIN): 0	
daniel@daniel-Latitude-5520:~/csric\$	

Figure 39: Injecting Unencrypted Captured Traffic – TP4 Laptop

ply.	a display filter <ctrl-></ctrl->						
	Time	Source	Destination		Length Info		
	1 2022-11-21 16:29:40.041038	172.24.1.2	192.168.59.146	ICMP	60 Echo (ping) request	id=0x0001, seq=222/56832,	
		192.168.59.146	172.24.1.2	ICMP	60 Echo (ping) reply	id=0x0001, seq=222/56832,	
		172.24.1.2	192.168.59.146	ICMP	60 Echo (ping) request	id=0x0001, seq=223/57088,	and the second
	4 2022-11-21 16:29:41.090242		172.24.1.2	ICMP	60 Echo (ping) reply	id=0x0001, seq=223/57088,	
	5 2022-11-21 16:29:42.083563		192.168.59.146	ICMP	60 Echo (ping) request	id=0x0001, seq=224/57344,	
		192.168.59.146	172.24.1.2	ICMP	60 Echo (ping) reply	id=0x0001, seq=224/57344,	
	7 2022-11-21 16:29:43.103313		192.168.59.146	ICMP	60 Echo (ping) request	id=0x0001, seq=225/57600,	
	8 2022-11-21 16:29:43.190640	192.168.59.146	172.24.1.2	ICMP	60 Echo (ping) reply	id=0x0001, seq=225/57600,	
	9 2022-11-21 16:29:44.122083		192.168.59.146	ICMP	60 Echo (ping) request	id=0x0001, seq=226/57856,	
	10 2022-11-21 16:29:44.153991		172.24.1.2	ICMP	60 Echo (ping) reply	id=0x0001, seq=226/57856,	
		172.24.1.2	192.168.59.146	ICMP	60 Echo (ping) request	id=0x0001, seq=227/58112,	
	12 2022-11-21 16:29:45.169746	102 160 50 146	172.24.1.2	ICMP	60 Echo (ping) reply	id=0x0001, seg=227/58112,	++1-61 (nonuact in 11)

Figure 40: Injected outgoing traffic - Inject Laptop

 Time	Source	Destination	Protocol	Length Info	
13 2022-11-21 17:33:19.098502	10.220.67.18	10.205.67.205	SCTP	130 HEARTBEAT	
14 2022-11-21 17:33:19.098679	10.205.67.205	10.220.67.18	SCTP	130 HEARTBEAT ACK	
15 2022-11-21 17:33:21.194222	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=227/58112, ttl=128 (no response	found!
16 2022-11-21 17:33:21.194227	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=228/58368, ttl=128 (no response	
17 2022-11-21 17:33:21.194229	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=229/58624, ttl=128 (no response	found!
18 2022-11-21 17:33:21.194230	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=230/58880, ttl=128 (no response	found!
19 2022-11-21 17:33:21.194232	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=231/59136, ttl=128 (no response	found!
20 2022-11-21 17:33:21.194235	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=232/59392, ttl=128 (no response	found!
21 2022-11-21 17:33:21.194236	172.24.1.2	192.168.59.146		122 Echo (ping) request id=0x0001, seq=233/59648, ttl=128 (no response	
22 2022-11-21 17:33:21.194247	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=234/59904, ttl=128 (no response	
23 2022-11-21 17:33:21.194249	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=235/60160, ttl=128 (no response	
24 2022-11-21 17:33:21.194251	172.24.1.2	192.168.59.146		122 Echo (ping) request id=0x0001, seq=236/60416, ttl=128 (no response	
25 2022-11-21 17:33:21.194253	172.24.1.2	192.168.59.146		122 Echo (ping) request id=0x0001, seq=237/60672, ttl=128 (no response	found!
	172.24.1.2	239.255.255.250	GTD (CCDD)		
26 2022-11-21 17:33:21.194280 27 2022-11-21 17:33:21.194282	172.24.1.2	192.168.59.146		265 M-SEARCH * HTTP/1.1 122 Echo (ping) request id=0x0001, seq=238/60928, ttl=128 (no response	

*Figure 41: Injected received traffic at core-side R6K* 

	i 🖉 🐵 📁 🖺 🗙 🙆 🔍 🖛 🖷			• III							
Apply	/ a display filter <ctrl-></ctrl->										
<b>.</b>	Time	Source	Destination	Protocol	Length	Info					
	1 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=233/59648,	ttl=61
	2 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=234/59904,	ttl=61
	3 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=235/60160,	ttl=61
	4 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP			(ping)		id=0x0001,	seq=236/60416,	ttl=61
	5 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=237/60672,	ttl=61
	6 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=238/60928,	ttl=61
	7 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=239/61184,	ttl=61
	8 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=240/61440,	ttl=61
	9 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP			(ping)		id=0x0001,	seq=241/61696,	ttl=61
	10 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=242/61952,	ttl=61
	11 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=243/62208,	ttl=61
	12 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=244/62464,	ttl=61
	13 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=245/62720,	ttl=61
	14 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=246/62976,	ttl=61
	15 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=247/63232,	ttl=61
	16 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=248/63488,	ttl=61
	17 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=249/63744,	ttl=61
	18 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=250/64000,	ttl=61
	19 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo	(ping)	reply	id=0x0001,	seq=251/64256,	ttl=61
	20 2022-11-21 17:33:21.630998	192.168.59.146		ICMP			(ping)			seq=252/64512,	
	01 0000 11 01 17.00.01 C00000	100 100 50 140	170 04 1 0	TCHO	~~	P	/>	1	11 0.0001	252/04200	++1 64

Figure 42: Injected traffic received at UE laptop

## Part 2: Traffic Modification with Enabled IPsec Tunnel between BBU and Core-Side R6K

In the second part of the experiment, we turned on IPsec. As above, from the UE laptop, we issued continuous ping messages and captured packets on both the UE and the core-side R6K. Figure 44 shows packet captures of ping traffic outside the tunnel: at the UE and on the egress of the core-side R6K. These messages were not visible on the transport channel, only appearing as ESP packets. The encrypted packets were captured on the transport channel using the laptop connected to TP4. The messages were then modified and injected into the transport channel as shown in Figure 43.

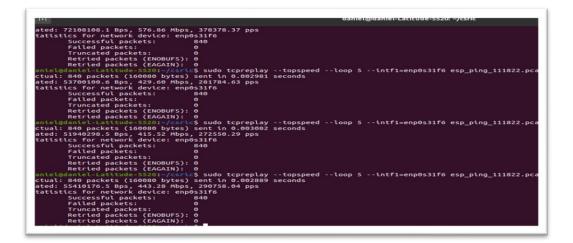


Figure 43: Injecting Encrypted Captured Traffic – TP4 Laptop

# Test Results for 5G STB – CSRIC-Inspired SA Use Cases

_								- × ·	
	CSRIC_test06-prt2_ipsec_UE2-laptop_11-21-22_1800.pcapng						_ 1		
File	e Edit View Go Capture Analyze Statistics Telep	phony Wireless Tools	Help						
	i 🔳 🖉 🐵 🚞 🛅 🗙 🎑 🔍 🖛 🌧 🚞 7	F 🗶 📃 🔲 🔍							
	Icmp						×		
٥.	Time	Source	Destination	Protocol	Length Info				
	121 2022-11-21 18:02:19.122127	172.24.1.3	192.168.59.146	ICMP	60 Echo (ping)	request :	id=0x0001, s	eq=	
	122 2022-11-21 18:02:19.158019	192.168.59.146	172.24.1.3	ICMP	60 Echo (ping)	reply	id=0x0001, s	eq-	
	123 2022-11-21 18:02:20.141664	172.24.1.3	192.168.59.146	ICMP	60 Echo (ping)	request	id=0x0001, s	eq=	
	124 2022-11-21 18:02:20.172928	192.168.59.146	172.24.1.3	ICMP	60 Echo (ping)	reply	id=0x0001, s	eq=	
	125 2022-11-21 18:02:21.150127	172.24.1.3	192.168.59.146	ICMP	60 Echo (ping)	request	id=0x0001, s	eq=	
	126 2022-11-21 18:02:21.167039	192.168.59.146	172.24.1.3	ICMP	60 Echo (ping)	reply	id=0x0001, s	eq=	
	127 2022-11-21 18:02:22.169475	172.24.1.3	192.168.59.146	ICMP	60 Echo (ping)		id=0x0001, s	eq-	
	128 2022-11-21 18:02:22 198250	192 168 59 146	172 24 1 3	TCMP	60 Echo (ping)	renly	d=avaaa1 s	eas	
	129 20  sric_test_06_prt2_mitreR6K_11-21-22_1800.	.pcap							
	130 20 File Edit View Go Capture Analyze	Statistics Telephony	Wireless Tools Help						
	131 20								
	132 28 📶 🔳 🙇 💿 🚞 📄 🔀 🙆 🤇								
-	gtp								$\times \rightarrow$
	Frame 1: 6 No. Time	Source	e Dest	ination	Protocol Leng	th Info			
	Raw packet 5 2022-11-21 18:01:14.30921	172.	24.1.3 192	.168.59.146	GTP <ic 1<="" td=""><td>22 Echo (pi</td><td>ing) request</td><td>id=0x000</td><td>1, seq-</td></ic>	22 Echo (pi	ing) request	id=0x000	1, seq-
	Internet F 6 2022-11-21 18:01:14.30961	L6 192.	168.59.146 172	.24.1.3	GTP <ic 1<="" td=""><td>22 Echo (pi</td><td>ing) reply</td><td>id=0×000</td><td>1, seq=</td></ic>	22 Echo (pi	ing) reply	id=0×000	1, seq=
	Internet 0 7 2022-11-21 18:01:15.32919	94 172.	24.1.3 192	.168.59.146	GTP <ic 1<="" td=""><td>22 Echo (pi</td><td>ing) request</td><td>id=0x000</td><td>1, seq-</td></ic>	22 Echo (pi	ing) request	id=0x000	1, seq-
	8 2022-11-21 18:01:15.32944	16 192.	168.59.146 172	.24.1.3	GTP <ic 1<="" th=""><th>22 Echo (pi</th><th>ing) reply</th><th>id=0x000</th><th>1, seq=</th></ic>	22 Echo (pi	ing) reply	id=0x000	1, seq=
	11 2022-11-21 18:01:16.34908	30 172.	24.1.3 192	.168.59.146	GTP <ic 1<="" th=""><th>22 Echo (pi</th><th>ing) request</th><th>id=0x000</th><th>1, seq-</th></ic>	22 Echo (pi	ing) request	id=0x000	1, seq-
	12 2022-11-21 18:01:16.34933			.24.1.3		22 Echo (pi		id=0x000	
	13 2022-11-21 18:01:17.35915			.168.59.146			ing) request		
	14 2022-11-21 18:01:17.35942			.24.1.3		22 Echo (pi		id=0x000	
	17 2022-11-21 18:01:18.37404			.168.59.146			ing) request		
	18 2022-11-21 18:01:18.37429			.24.1.3		22 Echo (pi		id=0x000	
	19 2022-11-21 18:01:19.39479	99 172.	24.1.3 192	.168.59.146	GTP <ic 1<="" td=""><td>22 Echo (pi</td><td>ing) request</td><td>id=0x000</td><td>1, seq=</td></ic>	22 Echo (pi	ing) request	id=0x000	1, seq=

Figure 44: Ping traffic from UE laptop and egress of core-side R6K

The logs for injected packets were captured from the outgoing interface of the inject laptop at TP4 as shown in Figure 45. As observed, only ESP packets were captured. To distinguish between the actual ESP packets flowing through the encrypted tunnel from the modified injected ESP packets, we used the loop and topspeed commands to attempt to inject a high volume of ESP packets (2,490 packets) as quickly as possible.

Edit View Go Capture Analyze Statistics	lelephony Wireless lool	s Help				
🔳 🖉 🕲 🚞 🛅 🔀 🌀 🔍 🖛 🔿	🛎 T 🛓 📃 🔍 🔍	୍ ର୍ 🎹				
sp						$\times \rightarrow$
Time	Source	Destination	Protocol	Length Info		
7 2022-11-21 18:13:26.762299107	10.220.67.18	10.205.67.200	ESP	186 ESP	(SPI=0xc3308779)	
8 2022-11-21 18:13:26.762310383	10.205.67.200	10.220.67.18	ESP	186 ESP	(SPI=0x1d2c0196)	
9 2022-11-21 18:13:26.762313377	10.220.67.18	10.205.67.200	ESP	202 ESP	(SPI=0xc3308779)	
10 2022-11-21 18:13:26.762316162	10.205.67.200	10.220.67.18	ESP	202 ESP	(SPI=0x1d2c0196)	
11 2022-11-21 18:13:26.762318909	10.220.67.18	10.205.67.200	ESP	186 ESP	(SPI=0xc3308779)	
12 2022-11-21 18:13:26.762321653	10.205.67.200	10.220.67.18	ESP	186 ESP	(SPI=0x1d2c0196)	
13 2022-11-21 18:13:26.762324272	10.220.67.18	10.205.67.200	ESP	186 ESP	(SPI=0xc3308779)	
14 2022-11-21 18:13:26.762326880	10.205.67.200	10.220.67.18	ESP	186 ESP	(SPI=0x1d2c0196)	
15 2022-11-21 18:13:26.762329431	10.220.67.18	10.205.67.200	ESP	202 ESP	(SPI=0xc3308779)	
16 2022-11-21 18:13:26.762332472	10.205.67.200	10.220.67.18	ESP	202 ESP	(SPI=0x1d2c0196)	
17 2022-11-21 18:13:26.762335136	10.220.67.18	10.205.67.200	ESP	186 ESP	(SPI=0xc3308779)	
18 2022-11-21 18:13:26.762337900	10.205.67.200	10.220.67.18	ESP	186 ESP	(SPI=0x1d2c0196)	
Identification: 0x0073 (115) > 000 = Flags: 0x0 0 0000 0000 0000 = Fragment Offset Time to live: 63	: 0					
Protocol: Encap Security Payload (50)						
Header Checksum: 0xde06 [validation d	isabledl					
[Header checksum status: Unverified]	isabica]					
Source Address: 10.220.67.18						
Destination Address: 10.205.67.200						
Encapsulating Security Payload						
ESP SPI: 0xc3308779 (3274737529)						
ESP Sequence: 711						



As shown in Figure 46, none of the injected packets or their decrypted version makes through to the UE or MITRE R6K during the test. Once the IPsec tunnel is established, traffic to and from the UE to the 5G core is encrypted, and it's not possible to see the contents of the messages. Even though it is possible to capture ESP packets, their contents are encrypted and unreadable, and when packets are modified and injected, they are dropped from either end of the tunnel end-points.

ly a display filter <ctrl-></ctrl->						
Time	Source	Destination	Protocol	Length Info		
1 2022-11-21 18:14:38.031828	172.24.1.3	239.255.255.2			H * HTTP/1.1	
2 2022-11-21 18:14:39.037248	172.24.1.3	239.255.255.2			H * HTTP/1.1	
3 2022-11-21 18:14:40.055848 4 2022-11-21 18:14:41.063101	172.24.1.3	239.255.255.2			Η * HTTP/1.1 Η * HTTP/1.1	
+ 2022-11-21 18.14.41.005101	172.24.1.3	239.233.233.	500 550F	205 IN-SEAR		-
csric_test_06_prt2_mitreR6K_11-21-22						-
File Edit View Go Capture And			Help			
Apply a display filter <ctrl-></ctrl->						
No. Time	So	urce	Destination	Protocol	Length Info	
88 2022-11-21 18:14:17.1	38663 10	.205.67.205	10.220.67.19	SCTP	130 HEARTBEAT ACK	
89 2022-11-21 18:14:19.3	37937 10	.220.67.19	10.205.67.204	SCTP	130 HEARTBEAT	
90 2022-11-21 18:14:19.3	38159 10	.205.67.204	10.220.67.19	SCTP	130 HEARTBEAT_ACK	
91 2022-11-21 18:14:20.0	55801 10	.205.67.204	10.220.67.19	SCTP	130 HEARTBEAT	
92 2022-11-21 18:14:20.0	59818 10	.220.67.19	10.205.67.204	SCTP	130 HEARTBEAT_ACK	
93 2022-11-21 18:14:21.5	38194 10	.220.67.19	10.205.67.205	SCTP	130 HEARTBEAT	
94 2022-11-21 18:14:21.5	38325 10	.205.67.205	10.220.67.19	SCTP	130 HEARTBEAT_ACK	
95 2022-11-21 18:14:23.3	38373 10	.220.67.19	10.205.67.204	SCTP	130 HEARTBEAT	
96 2022-11-21 18:14:23.3	38505 10	.205.67.204	10.220.67.19	SCTP	130 HEARTBEAT_ACK	
97 2022-11-21 18:14:25.9	37918 10	.220.67.19	10.205.67.205	SCTP	130 HEARTBEAT	
98 2022-11-21 18:14:25.9	38083 10	.205.67.205	10.220.67.19	SCTP	130 HEARTBEAT_ACK	
99 2022-11-21 18:14:28.1	.38967 10	.220.67.19	10.205.67.204	SCTP	130 HEARTBEAT	
100 2022-11-21 18:14:28.1	.39047 10	.205.67.204	10.220.67.19	SCTP	130 HEARTBEAT_ACK	
CSRIC 101 2022-11-21 18:14:30.3	38173 10	.220.67.19	10.205.67.205	SCTP	130 HEARTBEAT	
102 2022-11-21 18:14:30.3	38392 10	.205.67.205	10.220.67.19	SCTP	130 HEARTBEAT_ACK	
103 2022-11-21 18:14:32.5		.220.67.19	10.205.67.204	SCTP	130 HEARTBEAT	
104 2022-11-21 18:14:32.5	38732 10	.205.67.204	10.220.67.19	SCTP	130 HEARTBEAT_ACK	
105 2022-11-21 18:14:34.3		.220.67.19	10.205.67.205	SCTP	130 HEARTBEAT	
106 2022-11-21 18:14:34.7	38320 10	.205.67.205	10.220.67.19	SCTP	130 HEARTBEAT_ACK	
		captured (1040 bi				

Figure 46: Observed Packets at UE and MITRE R6K after Injecting Packets on Encrypted Transport Channel

## Success Criteria:

- 1. Unable to eavesdrop on UP and CP traffic across the transport link
- 2. Unable to modify UP and CP traffic across the transport link
- 3. Unable to inject UP and CP traffic across the transport link

## Results

Condition	Status
Unable to eavesdrop on UP and CP traffic across	Success
the encrypted transport link	
Unable to modify UP and CP traffic across the	Success
encrypted transport link	
Unable to inject UP and CP traffic across the	Success
encrypted transport link	
Overall Test	Success

# Test Case 7: CSRIC 7 WG 3 – Transport Layer Security for SBA Interfaces

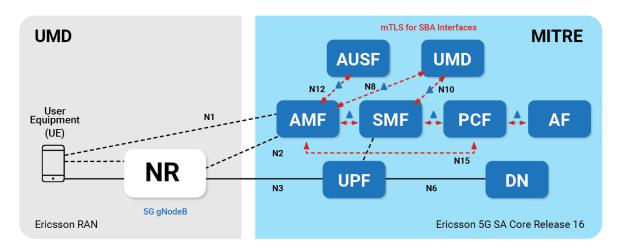
Test Case ID: TC-SA-07

### Description:

3GPP TS 33.501 specifies mandatory (e.g. requires vendor support for) transport layer security, but optional for service providers to use.

Given this standards requirement, CSRIC VII recommends the application of TLS for SBA interfaces and tunneling technology for transport when not using the SBA.

This test involves demonstrating that when TLS is used to provide protection for SBA interfaces in the 5G core, data packets cannot be captured, modified, or injected on the SBA interface.



*Figure 47: Test Case SA-07 Configuration* 

# Test points used:

Used	Test Point	Description and Use
	TP1	Laptop connected to Sierra Wireless card and/or software-defined radio (SDR); Wireshark captures packets originating at and destined to UE laptop; other tools access SDR controls and data
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can be configured to capture packets outside the tunnel (i.e., before IPsec encryption or after IPsec decryption) or inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
Х	TP7	CNOM tool accessing DMC messages, Ericsson transparent TCP proxy tool
	TP8	Applications running on application server in MITRE facility

This test case is comprised of two parts. For Part 1, the 5G core SBA network function (NF) interfaces are not configured with mutual transport layer security (mTLS)—rather, they utilize HTTP2. In Part 2, the 5G core SBA interfaces are configured with mTLS. Table 3 lists the mapped IP addresses used by the various NFs used for the SBA interfaces. Due the nature of the 5G core setup, some NFs (e.g., AMF) communicated on multiple IP addresses.

AMF	NRF	AUSF	UDM	SMF	TCP Proxy
172.17.152.165	192.168.56.143	192.168.56.138	192.168.56.137	192.168.56.129	172.17.208.251
172.17.95.197	192.168.56.143			192.168.56.131	
172.17.27.33					
172.17.152.146					
172.17.13.136					

#### Table 3: Network Function IP Addresses

For modification and insertion of traffic on the SBA interfaces, we used an Ericsson-provided TCP Layer Proxy Tool. The Proxy Tool was inserted between the various NFs and had the ability to intercept messages from producer (NRF) and its client, as shown in

## Figure 48.



Figure 48: TCP Layer Proxy Setup

As shown in Figure 49, services requests (e.g., the GET operation) are made through the TCP Proxy Tool, where in this figure we have highlighted the AMF (172.17.152.146) requesting services from the TCP Proxy (172.17.208.251) using port 8080.

stream eq 4					
Time	Source	Destination		Source Port Destinat L	
99 125.593716	172.17.152.146	172.17.208.251	HTTP2	43137 8080	124 Magic, SETTINGS[0], WINDOW_UPDATE[0]
100 125.593721	172.17.208.251	172.17.152.146	TCP	8080 43137	72 8080 → 43137 [ACK] Seq=1 Ack=53 Win=62720 Len=0 TSval=973056555 TSecr=710274034
119 125.594785	172.17.208.251	172.17.152.146	HTTP2	8080 43137	127 SETTINGS[0], SETTINGS[0], WINDOW_UPDATE[0]
121 125.594852	172.17.152.146	172.17.208.251	TCP	43137 8080	72 43137 → 8080 [ACK] Seq=53 Ack=56 Win=62720 Len=0 TSval=710274036 TSecr=973056556
124 125.594928	172.17.152.146	172.17.208.251	HTTP2	43137 8080	81 SETTINGS[0]
125 125.594931	172.17.208.251	172.17.152.146	TCP	8080 43137	72 8080 → 43137 [ACK] Seq=56 Ack=62 Win=62720 Len=0 TSval=973056556 TSecr=710274036
149 125.622963	172.17.152.146	172.17.208.251	HTTP2	43137 8080	188 HEADERS[1]: GET /nnrf-disc/v1/nf-instances?service-names=nudm-uecm&target-nf-type=UDM&requester-nf-type
150 125.622974	172.17.208.251	172.17.152.146	TCP	8080 43137	72 8080 → 43137 [ACK] Seq=56 Ack=178 Win=62720 Len=0 TSval=973056584 TSecr=710274064
155 125.625225	172.17.208.251	172.17.152.146	HTTP2/JSON	8080 43137	1463 HEADERS[1]: 200 OK, DATA[1], JavaScript Object Notation (application/json)
156 125.625302	172.17.152.146	172.17.208.251	TCP	43137 8080	72 43137 → 8080 [ACK] Seq=178 Ack=1447 Win=61440 Len=0 TSval=710274066 TSecr=973056587
183 167.836927	172.17.152.146	172.17.208.251	HTTP2	43137 8080	173 HEADERS[3]: GET /nnrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-typ
184 167.836944	172.17.208.251	172.17.152.146	TCP	8080 43137	72 8080 → 43137 [ACK] Seq=1447 Ack=279 Win=62720 Len=0 TSval=973098798 TSecr=710316278
189 167.839393	172.17.208.251	172.17.152.146	HTTP2/JSON	8080 43137	1223 HEADERS[3]: 200 OK, DATA[3], JavaScript Object Notation (application/json)
fUnescape	ed: http] ation: Indexed Head	er Field			
Represent Index: 6 ∨ Header: :pat Name Leng	th: 5	instances?service-name	s=nudm-uecm&ta	rget-nf-type=UDM&	requester-nf-type=AMF&supi=imsi-310014791791001
Represent Index: 6 Ƴ Header: :pat	th: 5	instances?service-name	es=nudm-uecm&ta	rget-nf-type=UDM&	requester-nt-type=AWF&supi=imsi-310014791791001
Represent Index: 6 ∨ Header: :pat Name Leng	th: 5 th	instances?service-name	es=nudm-uecm&ta	rget-nf-type=UDM&	requester-nf-type=AMPäsupi=imsi-310014791791001
Represent					

Figure 49: Wireshark Capture of TCP Layer Proxy Communication with Network Functions

# Part 1: Unencrypted SBA Interfaces

Tests for Part 1 were performed on February 27, 2023. There are three subparts to this test: (1) eavesdropping on SBA interfaces, (2) packet modification, and (3) packet injection.

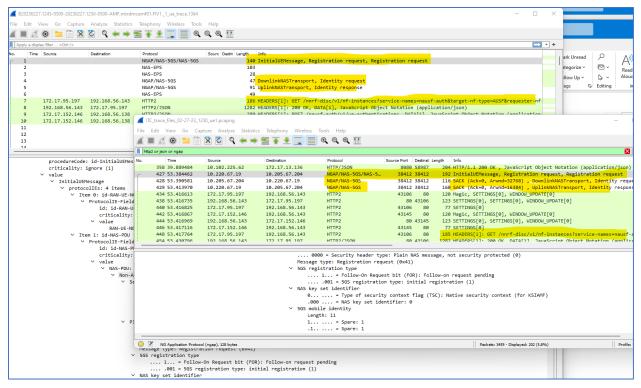
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 /	NCB ~ # gsh get_subscriber -imsi 310014791791001
Subscriber Data	
IMSI	: 310014791791001
Mobile Subscriber ISDN No.	: 7917910001
IMEI	: 004403160428990
Radio Access Technology	: NGRAN
Mobility Management State	: RM-DEREGISTERED CM-IDLE
Time of Registration in AMF	:
Time released	
RAT restrictions	: [EUTRA]
Forbidden areas	: []
Core network type restrictions	: Information not available
RFSP Index in Use	: Information not available
Service area restriction	
Restriction type	: NOT ALLOWED AREAS
TACs	; []
Max num. of TAs	: Information not available
Security Context State	: Security Context without Secure exchange
5GMM Capability	: Information not available
In MICO Mode	: No
CN Assistance Info RRC INACTIVE to NG-RAN	: false
Paging Proceed Flag	
Last Visited Tracking Area [TAI]	
Tracking Area List	
Latest NG-RAN Node List (MCC-MNC-Size-qNBId)	: 001-001-24-100002
TMS VoPS	: Not supported
SMS over NAS Allowed	: false
Subscribed S-NSSAIs	
Default S-NSSAIs	: 1-1
Non Default S-NSSAIs	
Registered S-NSSAIs	:
5G-GUTI	
PLMN Id	310-014
AMF Region Id	255
AMF Set Id	: 2
AMF Pointer	: 13
5G-TMSI	: 3758407710 (#E004C01E)

Figure 50: SA-07 Subscriber details from MITRE 5G Core

Figure 51 shows both the UE trace files and the combined ITC trace files including similar traffic flows with NAS messages and SBA interface messages. In addition, the ITC trace file shows TCP handshakes on the SBA interface: HTTP2 SETTINGs and DATA frame messages.

From these captures, we can clearly read the messages on the SBA interface. Specifically, as shown in Figure 52 and Figure 53, we can eavesdrop on the TCP handshakes and HTTP2 frames messages through, during, and after the UE initial registration process. Looking deeply into HTTP2 HEADER frame messages we see that at Packet 448, the AMF requests AUSF services from NRF through an HTTP2 HEADERS GET frame. These messages expose multiple AMF IP addresses (172.17.152.146, 172.17.95.197, 172.17.27.33, and 172.17.152.165) through the establishment of successful TCP handshakes between other NFs such as NRF (192.168.56.143), SMF (192.168.56.129), AUSF (192.168.56.138), and UDM (192.168.56.137), as well as UE details such as the SUPI (IMSI: 310014790791001), all visible in Figure 53.

## Test Results for 5G STB – CSRIC-Inspired SA Use Cases



*Figure 51: Test Case SA-07 traffic flows for combined ITC and UE trace files* 

📕 ПТС	_trace_files_02-27-23_12	230_ue1.pcapng			
File	Edit View Go Car	oture Analyze Statist	ics Telephony Wireles	s Tools Hel	lp
	1 🖉 🔍 🖿 🗎	🖹 🏹 🔍 🖛 =	• 🛎 🖌 👱 📃 🛛	•	e II
📕 (tcp	.flags.syn==1 and tcp.flags.	ack==1) && !(ip.src == 10.10	12.225.62)		
No.	Time	Source	Destination	Proto: Length	Info
	431 53.416362	192.168.56.143	172.17.95.197	TCP	76 80 → 43106 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=672073434 TSecr=1379474035 WS=256
	570 54.047591	192.168.56.129	172.17.27.33	тср	76 7070 → 43075 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=131081165 TSecr=110021449 WS=256
	461 53.433648	192.168.56.138	172.17.27.33	TCP	76 80 → 43077 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=4251342230 TSecr=144785766 WS=256
	561 54.046910	192.168.56.129	172.17.152.165	TCP	76 7070 → 43049 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=3339134728 TSecr=1907729930 WS=256
	459 53.433593	192.168.56.138	172.17.152.146	TCP	76 80 → 43137 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=658490094 TSecr=2367796144 WS=256
	436 53.416663	192.168.56.143	172.17.152.146	TCP	76 80 → 43145 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=907850761 TSecr=612013779 WS=256
	3295 361.836579	172.17.152.146	10.0.10.115		76 8080 → 49744 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=2422291602 TSecr=1714658740 WS=256
	588 54.261012	172.17.152.165	10.0.10.115	TCP	76 8080 -> 31351 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=3011720040 TSecr=1997809008 WS=256

Figure 52: Test Case SA-07 with no mTLS – AMF and other SBA NFs TCP Handshake, Source combined ITC trace file

🗏 🧕 🖢 🚡 😂 🔍 🔍 🔍 👄 🔿 💆 📃	
stream eq 12	S 🗔 🕤 +
Time Source Destination Protocol	Source Port Destinal Length Info
439 53.416748 172.17.95.197 192.168.56.143 TCP	43106 80 68 43106 → 80 [ACK] Seq=53 Ack=56 Win=62720 Len=0 TSval=1379474036 TSecr=672073435
440 53.416825 172.17.95.197 192.168.56.143 HTTP2	43106 80 77 SETTINGS[0]
441 53.416846 192.168.56.143 172.17.95.197 TCP	80 43106 68 80 → 43106 [ACK] Seq=56 Ack=62 Win=62720 Len=0 TSval=672073435 TSecr=1379474036
448 53.417764 172.17.95.197 192.168.56.143 HTTP2	43106 80 185 HEADERS[1]: GET /nnrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-type=AWF&supi
449 53.417790 192.168.56.143 172.17.95.197 TCP	80 43106 68 80 → 43106 [ACK] Seq=56 ACK=179 Win=62720 Len=0 TSval=672073436 TSecr=1379474037
454 53.430796 192.168.56.143 172.17.95.197 HTTP2/ 455 53.430813 172.17.95.197 192.168.56.143 TCP	
455 53.430813 172.17.95.197 192.168.56.143 TCP	43166 80 66 43166 + 80 [ACK] Seq-179 Ack-1270 Win-61696 Len-0 Tsval-1379474850 TSecn-672073449
Name Length: 5 Name: :path	0000 00 04 00 01 00 06 0e a7 97 be b9 88 00 00 08 00 0010 45 a0 00 a9 ea 63 40 00 40 06 49 fa ac 11 5f c5
Value Length: 119	
Value: /nnrf-disc/v1/nf-instances?service-names=naus	🙀 📶 Wireshark - Follow TCP Stream (tcp.stream eq 12) - ITC_trace_files_02-27-23_1280_ue1.pcapng 🚽 👘 🗧
path: /nnrf-disc/v1/nf-instances?service-names=naus	
Path segment: /nnrf-disc/v1/nf-instances	PRI * HTTP/2.0
Path sub segment: service-names=nausf-auth	SM .
Path sub segment: service-names=nausf-auth Path sub segment: target-nf-type=AUSF	SM
Path sub segment: target-nf-type=AUSF Path sub segment: requester-nf-type=AMF Path sub segment: supi=imsi-310014791791001	
Path sub segment: target-nf-type=AUSF Path sub segment: requester-nf-type=AWF Path sub segment: supi=imsi-310014791791001 [Unescaped: /nnf-disc/v1/nf-instances?service-names	A     A
Path sub segment: target-nf-type-AUSF Path sub segment: requester-nf-type-AUSF Path sub segment: supi-imsi-310014791791001 [Unescaped: /nnf-disc/u/inf-instances?service-names Representation: Literal Header Field with Incrementa	4
Path sub segment: target-nf-type=AUSF Path sub segment: requester-nf-type=AVF Path sub segment: supi-sinsi-1308478/231081 [Unescaped: /unf-disc//u1/nf-instances?service-names Representation: Literal Header Field with Incrementa Index: 4	4
Path sub segment: target-of-type-AUSF Path sub segment: request-of-type-AUSF Path sub segment: supi-imsi-310014791791001 [Unescaped: /unrf-disc/vl/nf-instances?service-names Representation: Literal Header Field with Increments Index: 4 V Header: :method: GET	4
Path sub segment: target-nf-type-MUSF Path sub segment: supi-insi-31004791273001 [Unscaped:/nnrf-disc/suf-insi-31004791273001 [Unscaped:/nnrf-disc-28-evice-names Representation: Literal Header Field with Incrementa Index: 4 V Header: :method: GET Name Length: 7	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUSF Path sub segment: supi-taria: 1300479273001 [Unescaped: /mrf-disc/vl/nf-instances?service-names Representation: Literal Header Field with Incrementa Index: 4 V Header: method: GET Name: method	4         Db.l.1.0", D*, NLTQ*, 124:17(2*,154:17(1*,2*),0",1",
Path sub segment: target-nf-type-MUSF Path sub segment: supi-supi-suppe-MUS Path sub segment: supi-supi-signotAr30230801 [Unscaped:/nnrf-discords-Zervice-names Representation: Literal Header Field with Incrementa Index: 4 V Header: :method: GET Name: :method Value (ength: 3	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUSF Path sub segment: supi-taria: 1300479273001 [Unescaped: /nmrf-disc/v1/nf-instances?service-names Representation: Literal Header Field with Incrementa Index: 4 * Header: :method: GET Name: .method Value Length: 3 Value: GET	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUS Path sub segment: supi-sub-i3004791270001 [Inscaped:/nnrf-dic/v1/nf-instances2ervice-names Representation: Literal Header Field with Incrementa Index: 4 V Header: :method: GET Name: :method Value: uength: 3 Value: GET :method: GET	4
Path sub segment: target-nf-type-MUSF Path sub segment: rugut=rnf-type-MUSF Path sub segment: sup1=sis-130014791273001 [Umscsged:/nnf-intranceSrevice.names Representation: Literal Header Field with Incrementa Index: 4 V Header: smethod: GET Name: Length: 7 Name: unethod Value Length: 3 Value: GET :method: GET [Umscsged: GET]	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUS Path sub segment: supi-smi-310047912701001 [[Inscaped://mrf-discapes?ervice-names Representation: Literal Header Field with Incrementa Index: 4 V Header: :method: GET Name: :method Value: uength: 3 Value: GET :method: GET [Unescaped: GET] Representation: Indexed Header Field	4
Path sub segment: target-nf-type=AUSF Path sub segment: request-nf-type=AUSF Path sub segment: supi-sub-i3004791273001 [Unscaped:/nnf-discloreStervice-mass Representation: Literal Header Field with Incrementa Index: 4 * Header: smethod: GET Name: nethod Value Length: 3 Value: GET : method: GET [Unscaped: GET] [Unscaped: GET] [Unscaped: GET] [Unscaped: GET] [Unscaped: GET] [Unscaped: GET]	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUS Path sub segment: supi-msi-310047912730001 [Unescaped:/mnf-discapes/revice-names Representation: Literal Header Field with Incrementa Index: 4 V Header: method: GET Name: imethod Value: uneght: 3 Value: GET imethod: GET [Unescaped: GET] Representation: Indexed Header Field Index: 2 V Header: isuthority: 192.166.56.143:80	4
Path sub segment: target-nf-type=AUSF Path sub segment: request-nf-type=AUSF Path sub segment: supi-sub-i3004791273001 [Unscsped:/nnf-fictaresStervice-news Representation: Literal Header Field with Incrementa Index: 4 * Header: imethod: GET Name: Length: 7 Name: Length: 7 Name: Length: 3 Value: GET :method: GET [Unscsped: GET] Representation: Indexed Header Field Index: 2 * Header: :muthority: 192.168.55.143:80 Name Length: 10	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUSF Path sub segment: supi-main-13004791273001 [Unescaped:/nnf-discoverService-names Representation: Literal Header Field with Incrementa Index: 4 * Header: :method: GET Name: :method Value: GET :method: GET [Unescaped: GET] Representation: Indexed Header Field Index: 2 * Header::suthority: 192.166.56.143:00 Name: Length: 10 Name: Langth: 10	4
Path sub segment: target-nf-type-AUSF Path sub segment: request-nf-type-AUSF Path sub segment: supi-sub-i300479173001 [Unscaped:/ndr-idscapes/service-names Representation: Literal Header Field with Incrementa Index: 4 V Header: imethod: GET Name: Length: 7 Name: Length: 3 Value: GET :method: GET [Unscaped: GET] Representation: Indexed Header Field Index: 2 V Header: :authority: 192.166.56.143:80 Name: :authority Value: Length: 12	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUS Path sub segment: supi-msi-31004791273001 [Inscsped:/mnf-disc/vl/nf-intances2service-names Representation: Literal Header Field with Incrementa Index: 4 * Header: method Value Length: 7 Name: imethod Value: GET [Inescaped: GET] Representation: Indexed Header Field Index: 2 * Header: mathority: 192.166.55.143:00 Name: Length: 10 Name: Length: 17 Value: Longth: 17 Value: Longth: 17 Value: Longth: 20.168.55.143:00	4
<ul> <li>Path sub segment: target-nf-type-AUSF</li> <li>Path sub segment: ruguiter.nf.type-AUSF</li> <li>Path sub segment: supi-sub-1300473173001</li> <li>[Unscaped: /nnf-files/structure.net</li> <li>Indext 4</li> <li>Header: :method: GET</li> <li>Name Length: 7</li> <li>Name: sethod</li> <li>Value tength: 3</li> <li>Value tength: 3</li> <li>Value tength: 3</li> <li>Value tength: 1</li> <li>Representation: Indexed Header Field</li> <li>Indext: 2</li> <li>Meader: :method: GET</li> <li>Representation: Indexed Header Field</li> <li>Indext: 2</li> <li>Meader: :method: SetT</li> <li>Name :method: SetT</li> <li>Name tength: 10</li> <li>Name :method: SetT</li> <li>Value tength: 12.166.56.143:80</li> <li>Name :mathority</li> <li>Value: 192.168.56.143:80</li> <li>:mathority: 192.168.56.143:80</li> </ul>	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUSF Path sub segment: supi-main-13004791273001 [Unescaped:/nnf-discoverService-names Representation: Literal Header Field with Increments Index: 4 * Header: :method: GET Name: :method Value: GET :method: GET [Unescaped: GET] Representation: Indexed Header Field Index: 2 * Header::suthority: 192.166.55.143:00 Name: Length: 10 Name: Length: 17 Value: Length: 17 Value: Length: 30	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUSF Path sub segment: supi-main-13004791273001 [Inscsped:/mnf-disc/vl/nf-intances2revice-names Representation: Literal Header Field with Incrementa Index: 4 * Header: method Value Length: 7 Name: imethod Value: GET [Inescaped: GET] Representation: Indexed Header Field Index: 2 * Header: isuthority; 192.166.56,143:00 Name: Length: 10 Name: Length: 17 Value: Length: 17 Value: Length: 17 Value: Length: 17 Value: Length: 18 Value Length: 17 Value: Length: 18 Value: Length: 18 Va	4
Path sub segment: target-nf-type-MUSF Path sub segment: request-nf-type-MUSF Path sub segment: supi-mini-l300479173001 [Unescaped:/Inf-fistcares/service-names Representation: Literal Header Field with Incrementa Index: 4 V Header: :method: GET Name Length: 7 Name: neethod Value (eff :method: GET [Unescaped: GET] Representation: Indexed Header Field Index: 2 V Header: :mathority Value (eff): Name: :mathority Value (eff): Name: :mathority Value (eff): Name: :mathority Value (eff): Name: :mathority Value (eff): Name: :mathority Value (eff): 192.168.56.143:80 Name: :mathority Value (eff): 192.168.56.143:80 [Unescaped: 192.168.56.143:80] Representation: Literal Header Field with Incrementa	4

Figure 53: TCP stream showing SBA NFs' communication messages

## Part 1.2: Modifying Traffic on the SBA Interfaces

For this part, we used the TCP Layer Proxy Tool to modify a message from one NF and transmit the modified packet to the client NF.

In Figure 54, the AMF requests SMF service through a GET frame via the TCP Proxy Tool (packet 229), and the tool relays this request to NRF (packet 231). Shown as an inset in the figure is the NRF response to the Proxy Tool containing the SMF IP address of 192.168.56.129 (packet 233).

However, as can be seen in Figure 55, rather than passing the message back to the AMF as-is, the Proxy Tool intercepts the message, modifies the SMF IP address to 192.168.56.131, and posts this modified HEADER frame to the AMF (packet 235). That message is received successfully by the AMF without generating an error.

diagon_with_modification	1.pcap				- 0	×
e Edit View Go Ca	inture Analyze Statisti	ics Telephony Wireless	Tools Help			
		****				
			4 4 4 H			1.
http2 or json	- Hard Street	10000000000			8 - •	+
Time	Source	Destination		surce Port Destinal L		
220 221.245484	172.17.208.251	172.17.13.136	HTTP2/JSON	8080 42471	602 HEADERS[9]: 201 Created, DATA[9], JavaScript Object Notation (application/json)	0
222 221.257736	172.17.152.146	172.17.208.251	HTTP2	43136 8080	172 HEADERS[5]: GET /nnrf-disc/v1/nf-instances?service-names=nudm-uecm&target-nf-type=UDM&requester-nf-type=AMF&supi=imsi-310014791791001	M
224 221.257861 225 221.259831	172.17.208.251 192.168.56.143	192.168.56.143 172.17.208.251	HTTP2 HTTP2/JSON	54794 80	172 HEADERS[5]: GET /nnf-disc/v1/nf-instances?service-names=nudm-uecm&target-nf-type=UDM&requester-nf-type=AMF&supi=imsi-310014791791001 1378 HEADERS[5]: 200 OK, DATA[5], JavaScript Object Notation (application/json)	Zoon
227 221.259930	172.17.208.251	172.17.152.146	HTTP2/JSON	80 54794 8080 43136	1378 HEADENS[3]: 200 UK, DHANES[, JavaScript UBject Notation (application/json) 1378 HEADENS[5]: 200 UK, DATA[5], JavaScript Object Notation (application/json)	1
229 221,731021	172.17.27.33	172.17.208.251	HTTP2/JSON	43072 8080	<pre>is/d maules[j]: zwo uw, Uwink[j], zwascrupt ubject motation (application json) 221 HEADES[j]: Edit // Innfr-disc/ul/nf-instancesiservice-name=smamf-pdusesion&amp;target-nf-type=SNF&amp;requester-nf-type=AMF&amp;snssais=%S6%76%22sst%22%33]</pre>	Zoon
231 221.731175	172.17.208.251	192,168,56,143	HTTP2	54792 80	221 HEADER[3]: GET /mnf-disc/v1/nf-instances/service-names-mamf-pdusesionatalget-mi-type=SMFarequest-mi-type=AMFassais=XS6X705225xt522534	
233 221.733835	192.168.56.143	172.17.208.251	HTTP2/350N	80 54792	222 memory [] ut /mm - usc/szm - ansumcersetvice-mames-man - publication (specimic - gpe-arrain-quester - m - cype-arrain-specimic - m - cype-arrain-specimi	
			Sector Vestorio S	100000000000		
Index: 6						100
✓ Header: :pat	h: /nnrf-disc/v1/nf-	-instances?service-nam	mes=nsmf-pdusessi	on&target-nf-typ	<pre>sest##arequester-nf-type=A#F&amp;snssais=\$58\$78%22sst%22%3A%2C%22sd%22%3A%22000001%22%70%50&amp;dnn=dnn=embb-stb1.mitre.net</pre>	P F
Name Lens						Oue 3
Name: :pa	ath					0
Value Ler	ngth: 185					0
Value: /r	nnrf-disc/v1/nf-inst	ances?service-names=n	smf-pdusession&ta	rget-nf-type=SM	&requester-nf-type=AVF&snssais=X55%78%22sst%22%3A1%2C%22x3d%22%3A%22000001%22%7D%5D&dnn=dnn-embb-stb1.mitre.net	0
ipath: /r	nnrf-disc/v1/nf-inst	ances?service-names=n	smf-pdusession&ta	rget-nf-type=SM	&requester-nf-type=AMF&snssais=%58%78%22sst%22%3A1%2C%22sd%22%3A%22000001%22%70%50&dnn=dnn=embb=stb1.mitre.net	0
Path	segment: /nnrf-disc.	/v1/nf-instances		1		
Path	sub segment: service	e-names=nsmf-pdusessio	n		Wireshark - Packet 233 - diagon_with_modification.pcap -	- 0
Path	sub segment: target	-nf-type=SMF				
Path	sub segment: request	ter-nf-type=AMF			Member: port	
		s=%58%78%225st%22%3A19	%2C%22sd%22%3A%22	00001%22%70%51	<pre>[Path with value: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/port:7070]</pre>	
		n-embb-stb1.mitre.net			[Member with value: port:7070]	
[Unescape	ed: /nnrf-disc/v1/nf	-instances?service-na	mes=nsmf-pdusessi	on&target-nf-t	Number value: 7070	
Represent	tation: Literal Head	ler Field with Increme	ntal Indexing - I	ndexed Name	Key: port	
Index: 4					<pre>[Path: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/port]</pre>	
✓ Header: :met	hod: GET				<ul> <li>Member: ipv4Address</li> </ul>	
Name Leng					<pre>[Path with value: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/ipv4Address:192.168.56.129]</pre>	
Name: :me					[Member with value: ipv4Address:192.168.56.129]	
Value Ler					String value: 192.168.56.129	
Value: GE					Key: ipv4Address	
:method:	GET				<pre>[Path: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/ipv4Address]</pre>	
[Unescape					Key: ipEndPoints	
	tation: Indexed Head	ler Field			<pre>[Path: /nfInstances/[]/nfServices/[]/ipEndPoints]</pre>	
Index: 2					Member: versions	
	hority: 10.108.204.4	47:8080			✓ Array	
Name Leng					• Object	
Name: :au					✓ Member: apiFullVersion	
Value Ler					<pre>[Path with value: /nfInstances/[]/nfServices/[]/versions/[]/apiFullVersion:1.1.2]</pre>	
					[Member with value: apiFullVersion:1.1.2]	
Value: 10						
Value: 10 :authorit	ty: 10.108.204.47:80				String value: 1.1.2	
Value: 10 :authorit [Unescape		[93				

Figure 54: AMF request for SMF services via TCP Proxy Tool

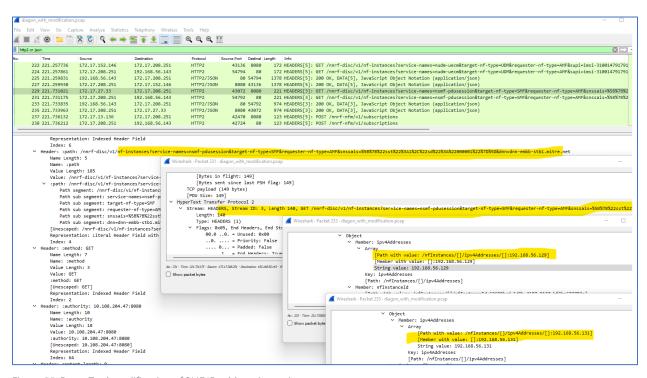


Figure 55: Proxy Tool modification of SMF IP address in service request response

## Part 1.3: Injection of Traffic on the SBA Interface

Similar to Part 1.2 above, in Part 1.3 of the experiment, we again used the TCP Layer Proxy Tool, this time injecting a new packet into the SBA NFs' interface data stream. We attempted to insert additional packets into the data stream as additional TCP/HTTP2 messages.

Figure 56 shows the AMF (172.17.152.146) requesting SMF services from the NRF (192.168.56.143) by way of the TCP Proxy Tool (172.17.208.251), as seen in packets 219 and 220. The NRF replies to the Proxy Tool with the IP address for the SMF (packet 221), which is then passed on to the AMF (packet 223). However, in this instance, we saved the message relayed to the AMF, and inserted that duplicated packet into the SBA interface (packet 225). This message is successfully conveyed to the AMF. Because it is a duplicate packet, the AMF recognizes the extra packet and issues a GOAWAY frame message, telling the Proxy Tool and NRF to initiate a graceful shutdown of the HTTP2 connection.

agon_duplicated_packet.pcap	- 0					
Edit View Go Capture Analyze Statistics Telephony Wireles	ss Tools Help					
I 🖉 🕲 늘 🖹 🗙 🏹 🍳 ሩ 🗭 🖉 🖉 🗐	<b>a a a a</b>					
Time Source Destination	Protocol Source Port Destinal Lenoth Info					
217 185.595130 172.17.208.251 172.17.152.165	HTTP2 8080 43041 89 PING[0]					
219 188.712690 172.17.152.146 172.17.208.251	HTTP2 43137 8080 221 HEADERS[5]: GET /nnrf-disc/v1/nf-instances?service-names=nsmf-pdusession&target-nf-type=SMF&r					
220 188.712827 172.17.208.251 192.168.56.143	HTTP2 46294 80 221 HEADERS[5]; GET /mrf-disc/v1/nf-instances?service-names=nsmf-odusession&target-nf-type=SMR&r					
221 188,714989 192,168,56,143 172,17,208,251	HTTP2/JSON 80 46294971 HEADERS[5]: 200 OK, DATA[5], JavaScript Object Notation (application/json)					
223 188,715076 172,17,208,251 172,17,152,146	HTTP2/JSON 8080 43137 971 HEADERS[5]: 200 OK, DATA[5], JavaScript Object Notation (application/json)					
225 188.715176 172.17.208.251 172.17.152.146	HTTP2/JSON 8080 43137 971 HEADERS[5]: 200 0K, DATA[5], JavaScript-Object Notation (application/json)					
227 188.715483 172.17.152.146 172.17.208.251	HTTP2 43137 8080 89 GOAWAY[0]					
229 188.715536 172.17.208.251 192.168.56.143	HTTP2 46294 80 89 GOAWAY[0]					
235 188.716993 172.17.13.136 172.17.208.251	HTTP2 42464 8080 87 HEADERS[5]: POST /nnrf-nfm/v1/subscriptions					
Path sub segment: dnn=dnn-embb-stb1.mitre.ne						
	names=nsmf-pdusession&target-nf-type=SMF&requester-nf-type=AMF&snssais=[{"sst":1,"sd":"000001"}]&dnn=dnn-embb-stbl.mitre.net]					
	📕 Wireshark - Packet 223 - diagon_duplicated_packet.pcap — 🗆					
	Key: port					
	<pre>[Path: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/port]</pre>					
	Member: ipv4Address					
	<pre>[Path with value: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/ipv4Address:192.168.56.129]</pre>					
	[Member with value: ipv4Address:192.168.56.129]					
	String value: 192.168.56.129					
	Key: ipv4Address					
	🖉 Wireshark - Packet 225 - diagon_duplicated_packet.pcap —					
	- S. American -					
	Member: ipv4Address					
	<ul> <li>rember: 1pv4Address</li> <li>[Path with value: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/ipv4Address:192.168.56.129]</li> </ul>					
	[Path with Value: /htintsances/[]/https://acast.jpina/coints/[]/ipv4Address:192.168.56.129] [Member with value: ipv4Address:192.168.56.129]					
	[member with value: 1pv+nduress:192.108.50.129] String value: 192.168.56.129					
	Key: ipv4Address					
Representation: Indexed Header Field	<pre>representation and the second a</pre>					
35       188.716093       172.17.18.136       172.17.208.251         Path sub segment: dnn=dnn=membs-stbl.mitre.         [Unescaped: /nn=f-disc/vl/nf-instances?service       Representation: Literal Header Field with Incr         Index: 4        Header: imethod: GET         Name: imethod       Value: Length: 7         Name: imethod       Value: GET         imethod: GET       [Unescaped: GET]         Representation: Indexed Header Field       Index: 2         / Header: authority: 10.108.204.47:8080       Name: isuthority         Value: GET       :authority: 10.108.204.47:8080         Name: isuthority: 10.108.204.47:8080       :authority: 10.108.204.47:8080         Value: 10.108.204.47:8080       [Unescaped: 10.108.204.47:8080]         Representation: Indexed Header Field       Index: 65         Value: 10.108.204.47:8080       [Wnescaped: 10.108.204.47:8080]         Representation: Indexed Header Field       Index: 65         / Header: content-length: 0       Name: content-length: 1         Name: content-length: 1       1	Key: ipEndPoints					
Header: content-length: 0	<pre>rej. ipinicults [Path: /nfinstances/[]/nfServices/[]/ipEndPoints]</pre>					
	Member: versions					
	~ Array					
	v Object					
Value: 0	Wember: apiFullVersion					
content-length: 0	[Path with value: /nfInstances/[]/nfServices/[]/versions/[]/apiFullVersion:1.1.2]					
[Unescaped: 0]	[Member with value: apjfull/version:1.1.2]					
Representation: Indexed Header Field	String value: 1.1.2					
	Key: apfullversion					
Index: 64						

*Figure 56: Inserting duplicate message on the SBA interface* 

# Part 2: mTLS on the SBA Interface

For the second part of the test, we repeated the same basic tests as Part 1 of this test after configuring mTLS on the 5G core SBA interface. With mTLS, each network function mutually authenticates with the others to form encrypted connections among them. These latter tests were conducted on June 1, 2023, and also used the TCP Layer Proxy Tool.

# Part 2.1: Inability to Eavesdrop on the SBA Interfaces

For this experiment, we focused on the traffic between the SMF (192.168.56.129), NRF (192.168.56.143), and AMF (172.17.27.33). As shown in Figure 57, two SBA interfaces at IPs 172.17.27.33 (AMF) and 192.168.56.129 (SMF) perform TLS handshake, including the Client Hello, Server Hello, and Key Exchanges and Verifications (packets 14664-14673). Thereafter, upon successful key exchange, the mTLS tunnel is established between the two network functions. All traffic between them is subsequently encrypted, and we can no longer see or tell the underlying messages, as seen in Figure 58 in which the Application Data is shown as encrypted and undecipherable by Wireshark.

CSRIC_7b-and-mTLS_t2_combined-itc-trace-files_06 e Edit View Go Capture Analyze Statistics					- 0
II d 🕲 📁 🗎 🕅 🙆 🔍 🔶 🗮 🖗 🤅	• <b>] 0 0 0</b>				
addr ==192.168.56.129					+
Time Source	Destination	Protocol	Source I	Destinatic	Length Info
14661 11:49:03.68 <mark>5935 172.17.27.33</mark>	192.168.56.129	TCP	43074	7070	
14662 11:49:03.686101 192.168.56.129	172.17.27.33	TCP		43074	
14663 11:49:03.686120 172.17.27.33	192.168.56.129	TCP	43074	7070	
14664 11:49:03.686992 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	
14665 11:49:03.687061 192.168.56.129	172.17.27.33	TCP		43074	· · · · · · · · · · · · · · · · · · ·
14668 11:49:03.702449 192.168.56.129	172.17.27.33	TLSv1.2		43074	
14669 11:49:03.702465 172.17.27.33	192.168.56.129	TCP	43074	7070	
14671 11:49:03.721675 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	
14672 11:49:03.721771 192.168.56.129	172.17.27.33	TCP		43074	
14673 11:49:03.725476 192.168.56.129	172.17.27.33	TLSv1.2		43074	
14674 11:49:03.725483 172.17.27.33	192.168.56.129	TCP	43074	7070	
14675 11:49:03.725827 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	
14676 11:49:03.725890 192.168.56.129	172.17.27.33	TCP		43074	
14677 11:49:03.725936 192.168.56.129	172.17.27.33	TLSv1.2		43074	
14678 11:49:03.725940 172.17.27.33	192.168.56.129	TCP	43074	7070	
14679 11:49:03.726036 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	
14680 11:49:03.726084 192.168.56.129	172.17.27.33	тср	7070	43074	4 68 7070 → 43074 [ACK] Seq=2524 Ack=2606 Win=60416 Len=0 TSval=1432070426 TSecr=
rame 14664: 291 bytes on wire (2328 b:	its) 201 bytes ca	ntured (232	R hits) o	n inter	rface unknown, id 0 0000 00 04 00 01 00 06 0e 54 57 fc 23 a6 00 00 08 00
inux cooked capture v1	103), 201 bytes eu		, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	ii ilicci	0010 45 a0 01 13 f0 6c 40 00 40 06 88 7c ac 11 1b 21
nternet Protocol Version 4, Src: 172.3	17 27 33 Dst · 192	168 56 129			0020 c0 a8 38 81 a8 42 1b 9e 70 27 e3 af 43 31 46 74
ransmission Control Protocol, Src Port			• 1 Ack·	1 Len	0030 80 18 00 f5 c1 61 00 00 01 01 08 0a ea 38 dd 45
ransport Layer Security		. ////0, 504	. <b>1</b> , <i>n</i> ex.	1, 100	0040 55 5b a8 +2 16 03 03 00 da 01 00 00 d6 03 03 64
TLSv1.2 Record Laver: Handshake Prot	ocol: Client Hello	n			0050 78 bd ef 99 e7 ad d7 78 ae e6 20 95 39 50 9f e7
Content Type: Handshake (22)	court criterie merre	-			0060 f6 c2 0d 85 f9 f6 71 09 27 0e 70 76 88 cd 7f 00
Version: TLS 1.2 (0x0303)					0070 00 06 00 ff c0 30 c0 2f 01 00 00 a7 00 00 03 6
Length: 218					0080 00 34 00 00 31 6d 74 72 64 6d 63 73 6d 66 30 31 0090 2e 73 6d 66 2e 64 6d 63 2e 6d 6e 63 30 31 34 2e
<ul> <li>Handshake Protocol: Client Hello</li> </ul>					00a0 6d 63 63 33 31 30 2e 33 67 70 70 6e 65 74 77 6f
Handshake Type: Client Hello (	1)				00b0 72 6b 2e 6f 72 67 00 0d 00 18 00 16 06 03 06 01
Length: 214	-,				00c0 05 03 05 01 04 03 04 01 03 03 03 01 02 03 02 01
Version: TLS 1.2 (0x0303)					00d0 02 02 33 74 00 00 00 0a 00 3a 00 38 00 0e 00 0d
Random: 6478bdef99e7add778aee6	209539509fe7f6c20d	85f9f671092	70e707688	cd7f	00e0 00 19 00 1c 00 0b 00 0c 00 1b 00 18 00 09 00 0a
Session ID Length: 0					00f0 00 1a 00 16 00 17 00 08 00 06 00 07 00 14 00 15
Cipher Suites Length: 6					0100 00 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0f
> Cipher Suites (3 suites)					0110 00 10 00 11 00 0b 00 02 01 00 00 10 00 05 00 03
Compression Methods Length: 1					0120 02 68 32
> Compression Methods (1 method)					

Figure 57: ITC trace file showing mTLS handshake

		S 4 🗢 🗢 🔤 🏚										1.
p.s	tream == 208											J+
	Time	Source	Destination	Protocol			Length Info					
4	673 11:49:03.7254	76 192.168.56.129	172.17.27.33	TLSv1.2	7070	43074	119 Change Cipher S					
4	4674 11:49:03.7254	83 172.17.27.33	192.168.56.129	TCP	43074	7070	68 43074 → 7070 [A	ACK] Seq=2	187 Ack=2452	Win=60416 Len=	0 TSval=392959524	4 TSecr
4	4675 11:49:03.7258	27 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	149 Application Dat	ta				
4	676 11:49:03.7258	90 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 [A		152 Ack=2568	Win=60416 Len=	0 TSval=143207042	6 TSecr
4	677 11:49:03.7259	36 192.168.56.129	172.17.27.33	TLSv1.2	7070	43074	140 Application Dat	ta				
4	4678 11:49:03.7259	40 172.17.27.33	192.168.56.129	TCP	43074	7070	68 43074 → 7070 [A	ACK] Seq=2	68 Ack=2524	Win=60416 Len=	0 TSval=392959524	4 TSecr
4	4679 11:49:03.7260	36 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	106 Application Dat	ta				
4	680 11:49:03.7260	84 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 [A	ACK] Seq=2	24 Ack=2606	Win=60416 Len=	0 TSval=143207042	6 TSecr
4	4681 11:49:03.7271	48 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	251 Application Dat	ta				
14	682 11:49:03.7272	02 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 [A	ACK] Seq=2	24 Ack=2789	Win=60416 Len=	0 TSval=143207042	7 TSecre
14	4683 11:49:03.7272	42 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	1461 Application Dat	ta				
4	684 11:49:03.7272	85 192.168.56.129	172.17.27.33	ТСР	7070	43074	68 7070 → 43074 [A	ACK1 Sea=2	24 Ack=4182	Win=59136 Len=	0 TSval=143207042	8 TSecr
-												
•a	ame 14683: 1461 by	tes on wire (1168/	8 bits), 1461 bytes	captured (	11688 bit	s) on i	nterface unknown, id				6c dd a9 d6 58	
r	nux cooked capture	e v1									a6 21 81 44 ea	
nt	ernet Protocol V	ersion 4, Src: 172	.17.27.33, Dst: 192	.168.56.129							06 5b 6f e4 fd	
•	ansmission Contro	l Protocol, Src Po	rt: 43074, Dst Port	: 7070, Seq	: 2789, A	ck: 252	4, Len: 1393				d5 74 44 6a 5b	
	ansport Laver Seco	urity			-		-				98 7d 95 d1 32	
ransmission Control Protocol, Src Port: 43074, Dst Port: 7070, Seq: 2789, Ack: 2524, Len: 1393 ransport Laver Security											b5 2b 3d 8d 6d	
											30 25 71 3e 1d bf 77 5f 3a 64	
	Content Type:											
na	Content Type: Version: TLS 1		()								38 db 30 0e 03	

Figure 58: Encrypted SBI traffic with mTLS – source ITC trace file, MITRE 5G Core

## Part 2.2: Modifying Traffic on the SBA Interface

In this part, as in Parts 1.2 and 1.3, we used the TCP Proxy Layer Tool to attempt to modify the traffic stream from the NRF (IP address 192.168.56.143) and transmit the traffic to the SMF (IP address 172.17.208.231). The tool is transparent to the SBA interfaces. Also, because traffic between the SBA NFs is encrypted, and the TCP Proxy Tool actions are transparent, the ITC trace files do not show any interactions for the TCP Proxy Tool service or HTTP pod IPs as illustrated in Figure 59, where no messages appear when filtering on the relevant IP addresses. The logs from these IPs are only visible from the logs taken by the Proxy Tool.

	SRIC_7b-and-mTLS	t2_combined	d-itc-trace-files_06	-01-23_1100a	m.pcapng				_		×
File	Edit View Go	Capture An	alvze Statistics	Telephony	Wireless Tools Help						
	I 🖉 🕲 🚞 🛅	× 2 9	* * * * * *								
ip.a	ip.addr==172.17.208.231    ip.addr==10.108.204.47    ip.addr==172.17.208.251								*		Hex Va
No.	Time	Source	Destination	Protocol	Source Destination Length	info					_
-											
0 2	CSRIC_7b-and-m	TLS_t2_combine	ed-itc-trace-files_06-0	1-23_1100am.p	capng		Pa	ckets: 72224 * Displayed: 0 (0.0%)	Pr	ofile: STB	Profile

Figure 59: TCP Proxy Tool actions are transparent, source ITC trace file

Because data flowing through the TCP Proxy Tool is encrypted, the tool cannot identify what type of message any given packet corresponds to. Consequently, for data modification, the TCP Proxy Tool randomly selected packets to modify. The modification changed the last byte of data

to 0x00 for the selected packet. An example output of the Proxy Tool is shown in Figure 60. The figure also shows how the receiving node disconnects the TLS/TCP traffic stream when the modified packet is received. Subsequently, a new TCP client traffic connection is initiated, starting a new TLS stream in order to complete the failed operation. Figure 61, Figure 62, and Figure 63 show additional cases of the TCP Proxy Tool modifying encrypted packets. Every time the tool modifies the data, a TCP reset (RST) is sent, closing the connection between the sender and the recipient device, and informing the sender to create another connection and resend the traffic.

root@diagon-d4df7fdb-mctv9:/app# python diagon_with_modification2.py
('172.17.208.231', 64802) has connected
Modifying data ('172.17.208.231', 64802)!
Original data: b'\x17\x03\x00\x1a\x95\xee\xea\x81\x82\xf1\x06(\x11\xc9N\x07e\x9b\xb5W\xca\xf5\x16\x01\x95\xf9\xba\xf3(\xf8'
Modified data: b'\x17\x03\x03\x00\x1a\x95\xee\xea\x81\x82\xf1\x06(\x11\xc9N\x07e\x9b\xb5W\xca\xf5\x16\x01\x95\xf9\ <mark>xba\xf3(\x00'</mark>
('172.17.208.231', 648 <mark>02) has disconnected</mark>
('172.17.208.231', 65338) has connected
('172.17.208.231', 64582) has connected
('172.17.208.231', 64737) has connected
('172.17.208.231', 64587) has connected
Modifying data ('192.168.56.143', 443)!
Original data: b'\x16\x03\x00\x00\x00\x00\x00\x00\x03\x03\x82\x86\xfa\xc2[\xe3\xb3\xef\x08Fh\x1f\xf1\xcf\x8e!\x18B!-aqY4\x0e\x02\x83\r\xec\xcd] \xfa\x9a./\xc4
\xae\xb79\xb8\xab\xb4\xd6\xe6\xd4\xb6\xf3\xfb\xbc\x1e\xb8\xcc\xe1\x0c\xe2TV:rF\xfe\x9b\x13\x00\x00\x00\x00\x00\x00\x1d\x00 \x1aVhvN\xb3\x19\xa8\x0b\x01
\xa0\xe5\x99\x8e\$*\x18\xc4\xbd\xf8\xc4\xf9\xfc\xee\xfe\x8a\xfb\x98]<\x9db\x00+\x00\x02\x03\x04\x14\x03\x03\x00\x01\x17\x03\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x04\x14\x03\x03\x04\x04\x04\x04\x04\x04\x04\x04\x14\x03\x03\x03\x04\x04\x04\x04\x04\x04\x04\x04\x04\x04

Figure 60: Traffic modification using TCP Proxy Tool

A MARINE THE STATE OF				
Mitre_diagon-pod-trace_continuous.pcapng.gz				
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help				
◢ ■ ∅ ⊗ 늘 🗅 🗙 🖏 ९ 🗢 ⇒ 🛎 🐺 🖢 🔲 ९ ९ ९ ୩ 🗉				
tcp.port == 64802	X 🗆 🔹 +			
No. Time Source Destination Protocol Source Destination	Length Info			
3513 12:25:28.363922 172.17.208.231 172.17.208.251 TCP 64802 8080				
→ 3514 12:25:28.363939 172.17.208.251 172.17.208.251 TCP 8080 64802				
4793 12:25:51.593440 172.17.208.231 172.17.208.251 TCP 64802 8080				
4794 12:25:51.593457 172.17.208.251 172.17.208.231 TCP 8080 64802				
6653 12:26:28.783482 172.17.208.231 172.17.208.251 TCP 64802 8080				
6654 12:26:28.783498 172.17.208.251 172.17.208.231 TCP 8080 64802				
7043 12:26:35.243500 172.17.208.231 172.17.208.251 TCP 64802 8080				
7044 12:26:35.243516 172.17.208.251 172.17.208.231 TCP 8080 64802				
7045 12:26:35.243540 172.17.208.231 172.17.208.251 TCP 64802 8080				
7049 12:26:35.244110 172.17.208.231 172.17.208.251 TCP 64802 8080				
7050 12:26:35.244118 172.17.208.251 172.17.208.231 TCP 8080 64802				
7055 12:26:35.245709 172.17.208.251 172.17.208.231 TCP 8080 64802				
	Wireshark - Packet 3514 - Mitre diagon-pod-trace continuous.pcapng.gz			
> Frame 3513: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on inter				
Linux cooked capture v2	> Frame 3514: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0			
> Internet Protocol Version 4, Src: 172.17.208.231, Dst: 172.17.208.251	> frame Ssis: ou bytes on wire (400 bits), ou bytes captured (400 bits) on interface -, id o			
Transmission Control Protocol, Src Port: 64802, Dst Port: 8080, Seq: 0, Len: 0	<ul> <li>Entroy cooked capture v2</li> <li>Internet Protocol Version 4, Src: 172.17.208.251, Dst: 172.17.208.231</li> </ul>			
Source Port: 64802	<ul> <li>Transmission Control Protocol, Src Port: 8060, Dst Port: 64802, Seq: 1, Ack: 1, Len: 0</li> </ul>			
Destination Port: 8080	Source Port: 8080			
[Stream index: 1072]	Destination Port: 64802			
[Conversation completeness: Incomplete (37)]	Stream index: 1072			
[TCP Segment Len: 0]	[Conversation completeness: Incomplete (37)]			
Sequence Number: 0 (relative sequence number)	[TCP Segment Len: 0]			
Sequence Number (raw): 1407823150	Sequence Number: 1 (relative sequence number)			
[Next Sequence Number: 1 (relative sequence number)]	Sequence Number (raw): 0			
Acknowledgment Number: 0	[Next Sequence Number: 1 (relative sequence number)]			
Acknowledgment number (raw): 0	Acknowledgment Number: 1 (relative ack number)			
1010 = Header Length: 40 bytes (10)	Acknowledgment number (raw): 1407823151			
Flags: 0x002 (SYN)	0101 = Header Length: 20 bytes (5)			
Window: 62720	> Flags: 0x014 (RST, ACK)			
[Calculated window size: 62720]	Hindow: A			

Figure 61: TCP packet reset after data is modified, source TCP Proxy Tool logs

Modifying data ('172.17.208.231', 64737)
Original data: b'\x17\x03\x03\x00\x13#\xd3\xb1N\x1b\xaf=ua?\x00MNm~\x82\xaf5\xa7'
M <mark>odlfied data: b`\x</mark> 17\x03\x03\x00\x13#\xd3\xb1N\x1b\xaf=ua?\x00MNm~\x82\xafS\x00'
('172.17.208.231', 64737) has disconnected
Modifying data ('192.168.56.143', 443)
Original data: b \x17\x03\x03\x03\x04\x9b/ <s\x9d\xx9b td="" xs\x40\xe9\xc1\x89\xd5n\xb0\xf0\xf9"\xea\x05zh\n\xb0\x01\xfbp\xc4\xae\xd6\xde\xe3\rla\xc05\xe5\xa1\xbc\n\x91<=""></s\x9d\xx9b>
\xac\xaf\xcb\xde\xf4\x14\xc3\xe1b\x10\xa9?\xae\x898scY\$8\x93.\xa10K\x1d \xe2\xa7#\xde\xba\x9f6\xd50\xd4I@\xd9sZ\xd6\xc1\x89T\x94\xb5b\x17\\"0\xe0\x1a\x16\xfc
\xca\x9df\xfa\xce\xfd\xb1\xb3*4D\xb1 >\xb5\x04\xcc<\x85\x1e6\xd1cQhh\x0e\xf0;\xaa\n&7\x1c\xf5\xe6:\xb1\x02\x06\x9&\r\x95\x8a\xaa\x88B\x16@J\x01\ <mark>x05\x98</mark>
Modified data: b'\x17\x03\x03\x03\x04\x9b/ <s\x9dul\xd0\xeey~\xc1\x89\xd5n\xb0\xf9"\xea\x05zh\n\xb0\x01\xfbp\xc4\xae\xd6\xde\xe3\rla\xc05\xe5\xa1\xbc\n\x91< td=""></s\x9dul\xd0\xeey~\xc1\x89\xd5n\xb0\xf9"\xea\x05zh\n\xb0\x01\xfbp\xc4\xae\xd6\xde\xe3\rla\xc05\xe5\xa1\xbc\n\x91<>
\xac\xaf\xcb\xde\xf4\x14\xc3\xe1b\x10\xa9?\xae\x898scY\$8\x93.\xa10K\x1d \xe2\xa7#\xde\xba\x9f6\xd50\xd4I@\xd9sZ\xd6\xc1\x89T\x94\xb5b\x17\\"0\xe0\x1a\x16\xfc
\xca\x9df\xfa\xce\xfd\xb1\xbas*4D\xb1 >\xb5\x04\xcc<\x85\x1e6\xd1cQhh\x0e\xf0;\xaa\n&7\x1c\xf5\xe6:\xb1\x02\x06\x9c&\r\x95\x8a\xaa\x88\x1e@J\x01\
('172.17.208.231', 65487) has disconnected
('172.17.208.231', 65192) has connected
Modifying data ('172.17.208.231', 65192)
Original data: b'\x17\x03\x00\x1a\xa5\xcdU^\xd1cu\xe6\xb8q\xd5MXq\x9b\xb9\x90\x16\xe6a\x960\x1e\xb6xe'
Modified data: b'\x17\x03\x00\x1a\xa5\xcdU^\xd1cu\xe6\xb8q\xd5MXq\x9b\xb9\x90\x16\xe6a\x960\x1e\xb6x\x00'
('172.17.208.231', 65192) has disconnected
('172.17.208.231', 64773) has connected
Modifying data ('172.17.208.231', 64773)!
Original data: b'\x17\x03\x00"s\xc3P\xefq\xbcACfj82\xfaK4\x91\t\xe4*\x80jX\xea\x0f,\xdf`\xb9\xfa1\xf4M\xeb\xa1
Modified data: b'\x17\x03\x03\x03\x00"s\xc3P\xefq\xbcACfj82\xfaK4\x91\t\xe4*\x80jX\xea\x0f\\xdf`\xb9\xf01\xf4M\xeb\x00'
('172.17.208.231', 64773) has disconnected

Figure 62: Traffic modification using TCP Proxy Tool

p.stream eq 6917					X - + HexV
Packet list ∨ Narro	w & Wide 🗸 🗌	Case sensitive Hex value	<ul> <li>✓ 7fbac</li> </ul>	a00	Find Cancel
Time	Source	Destination Protocol	Source Port D		
21756 13:39:40.962489	172.17.208.251	192.168.56.143 TCP	53238	443	80 53238 → 443 [SYN] Seq=0 Win=62720 Len=0 MSS=8960 SACK_PERM TSval=193763350
21757 13:39:40.962540	192.168.56.143	172.17.208.251 TCP	443	53238	80 443 → 53238 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSva
21758 13:39:40.962546	172.17.208.251	192.168.56.143 TCP	53238	443	72 53238 → 443 [ACK] Seq=1 Ack=1 Win=62720 Len=0 TSval=1937633508 TSecr=26402
21761 13:39:40.962775	172.17.208.251	192.168.56.143 TLSv1.3	53238	443	428 Client Hello
21762 13:39:40.962797	192.168.56.143	172.17.208.251 TCP	443	53238	72 443 → 53238 [ACK] Seq=1 Ack=357 Win=62464 Len=0 TSval=2640279933 TSecr=193
21763 13:39:40.964069	192.168.56.143	172.17.208.251 TLSv1.3	443	53238	1638 Server Hello, Change Cipher Spec, Application Data
21764 13:39:40.964080	172.17.208.251	192.168.56.143 TCP	53238	443	72 53238 → 443 [ACK] Seq=357 Ack=1567 Win=61184 Len=0 TSval=1937633510 TSecr=
21773 13:39:40.966409	172.17.208.251	192.168.56.143 TLSv1.3	53238	443	2279 Change Cipher Spec, Application Data, Application Data, Application Data
21774 13:39:40.966443	192.168.56.143	172.17.208.251 TCP	443	53238	72 443 → 53238 [ACK] Seq=1567 Ack=2564 Win=60416 Len=0 TSval=2640279937 TSec
21775 13:39:40.966651	172.17.208.251	192.168.56.143 TLSv1.3	53238	443	491 Application Data, Application Data
21776 13:39:40.966668	192.168.56.143	172.17.208.251 TCP	443	53238	72 443 → 53238 [ACK] Seq=1567 Ack=2983 Win=60160 Len=0 TSval=2640279937 TSec
21777 13:39:40.966759	192.168.56.143	172.17.208.251 TLSv1.3	443	53238	96 Application Data
21778 13:39:40.966766	172.17.208.251	192.168.56.143 TCP	53238	443	72 53238 → 443 [ACK] Seq=2983 Ack=1591 Win=61184 Len=0 TSval=1937633512 TSecr
21779 13:39:40.966799 21780 13:39:40.966816	192.168.56.143 192.168.56.143	172.17.208.251 TCP 172.17.208.251 TCP	443	53238 53238	72 443 → 53238 [FIN, ACK] Seq=1591 Ack=2983 Win=60160 Len=0 TSval=2640279937 72 443 → 53238 [RST, ACK] Seq=1592 Ack=2983 Win=60160 Len=0 TSval=2640279937
Length: 1836 Encrypted Application Data: 6722407af30de4049620316baf589520ed4df521de6d [Application Data Protocol: Hypertext Transfer Protocol] 'TLS/1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protoco: Opaque Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 281 Encrypted Application Data: 1c00450ccdae29519c270ad051587ce05fled9bf3c2c [Application Data Protocol: Hypertext Transfer Protocol] 'TLS/1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protococ Opaque Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 69 Encrypted Application Data: 4bbee39ca24612bea1675a3924833bffe5cd2238fag				> > > > > > > > > > > > > > > > > > >	Frame 21773: 2279 bytes on wire (18232 bits), 2279 bytes captured (18232 bits) of Linux cooked capture v.         Linux cooked capture v.         Linux cooked capture v.         Internet Protocol Version 4, Src: 172.17.208.251, Dst: 192.168.56.143         Transmission Control Protocol, Src Port: 53286, Dst Port: 443, Seq: 357, Ack: 15         Source Port: 5328         Destination Port: 443         [Stream index: 6917]         860       16 ea 43 e3 a8 97 98 ce       dd fd 6d 45 0c 7d e8 e2         870       8a 3f 43 e7 6f 75 2a d8 46 f5 d5 60 58 ff 6c d9         880       80 7 cd e1 45 60 d8 97 75 32 e6 56 c9 ea 25 e 43

*Figure 63: TCP packet data modification, source TCP Proxy Tool logs* 

## Part 2.3: Inserting Packets into SBA Traffic Stream

Similar to Part 2.2 above, in Part 2.3 of the experiment we again used the TCP Layer Proxy Tool to try and inject a new packet into the SBA NFs' interface data stream. In this case, the tool was programmed to duplicate packets randomly. Each duplicate packet is then inserted into the traffic stream and transmitted. As shown in Figure 64 and Figure 65, the TCP Proxy Tool duplicates data on the fly. We see from the logs that the TCP stream is disconnected by issuance of a [FIN,ACK] whenever the remote NF notices a duplicate packet.

\xe6\x98\x8a\xe7\'\x93\x98{\xb7\xc8\xafY\x92\xb1\x84\x85\x04i\xa0M\x14\x84\xb5\x11\*\xfb\x9a|\xedQZ\xa6L\xd679\xd52\xc3\xf1\xfc\x95\xf4\x807\xc2\x91]\xce\xa6 \x1c\xd2J\xb9\xda\xa8\xe1\x1c\xd1\x0f@1b\x81-UTqB;\x0c\xc8\xe4P\xe8dx(\xd8\x1b\xf8\xb5\x9aR\xe1\xee\x0e\xa1\xbcQ|F\xa6\xdf\x01Q\x94\xb0\xabGG\xc9\xi \xac]\xe4 Duplicating packet!



b'\x17\x03\x03\x89\x800\x13F\xc7d\xbaT\xd5b\xdd\xb1\x11\x06\x93\x87H\xb7D\x82\xc8A'

b'\x17\x03\x03\x04\x64\xe5\x890\xd6\xa8"\x95xW\x99u\xc6\x99u\xa6\xfb\xd6\xca\x87\xadc\xd9%A\xb0\xba\x93+1\x86N\x87\x04\x80\x13\x96\x14\x94\x8b\xd2\x82\x0 \xab\x04cp\'\xb0\xf7\x021\xd7-\xf0"4\\\xb0\xb9\x93\xf3\xfde\x87\'\xefj\xe7\xae\x13\xc7\x82\xee\xd0\xd5cd \xf0\xc2\x04\xae\xb0\xf10Y\r\x80\x07\xd7\x88 \xa0H\xfb\x19!\xba\x91\xe1^\*h\xfb\xa9\x83\xaf\xb1+\xd9\xcc\xf6gh\'\xce\*S\x11\x19\xe5&\xccY]\xad6@#n\xf2eS\xccW\x95\xcb\xd1\x02\x120\xf8\xf9\xdfp\xe5L\rp \x8C\xd8\xd2\xd8\xd2\xd8\xcc\xa3\xdd.PM\xe6\x93i\xf5\xab\xafn\x11\xe0\xa1\x11\x95\xac\x1d\$s\x66\x14U1@\xb7\x17\x04\x9f\xca\xf9E\xa3\xc2D\x07g#\x81\xe3u\xdc\xc3\xafP \xe4\xa8\x89\x82\xc1\xc7\x88\xf1\xb17\xd4V\xcd\xaf\xb6\x94\xbcp\x04A\x9e-\x13\x9c\xd0\x9d\x14q\xeb\x01wf\x08\xef\xcdS'\xd5\xf2\xfe\xc0\xd4%\xadp\xc3?w\xa6\xac \xa9\xb9\xe1\x8fQ\xbc(\xd0]\x14\x11\x14\x07r\xb9u\x86\xf4\xb3\x06\x1d\x83\x902\xfc\xa9\x90 \x03\xa2\x94\xad ('172.17.208.231', 64878) has disc Original data:

b"\x17\x03\x01\xd7\xc7\xc6\xd1rm\xd2\xc9e\x03(\xe8;(\x82\xe5?\xfcf5\xa5;Z\x88M\x18\x92P\xd8\xd9\x91H\xd7E\x9c\_\xa8i%\x82\xed\x0c\xbb\x9a\xe0\xd2\x89 \xf5bV,\x9e\xeb\x10\x02\xe6\x0b\x14\*xx>\x12\xa0\r\xdf\xb0\x93\xd8\xff\x9d;g\x1b6s\xbcX\xe8\xe3B\tQe\xf9T\xc9n\xbe\xba\x1c\xcd)\x9f\xe2i\xb3\xd5\xfc\xce \x8f\x85\xcf\xed\r\xd0\xd3~RBg\xf3\xab\x92\x8ec\n0\xf34\xae\xb5WB#\xf5\xbfw,\x93\xaa^\xf0m\x82\x90\x9bPt\xa8\xda\x8d\xed\xe6\xa2\xc5\x14\x1bX\xb0\xcb\x98\x08



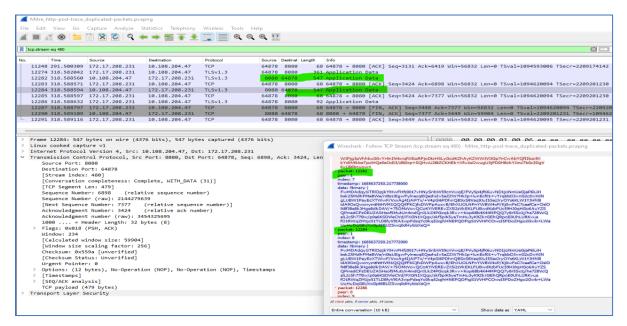


Figure 65: Inserted TCP packets, Wireshark view, source TCP Proxy Tool logs

#### Success Criteria:

- 1. Unable to eavesdrop on the SBA interfaces
- 2. Unable to modify traffic on the SBA interfaces
- 3. Unable to inject messages on the SBA interfaces

Condition	Status
Able to eavesdrop on the SBA interface when mTLS is not implemented	Success: Able to identify IP addresses for AMF, AUSF, NRF, SMF, UDM; as well as IMSI/SUPI
Able to modify traffic on the SBA interface when mTLS is not implemented	Success: Able to intercept message between the NRF and AMF and modify the SMF IP address without producing error
Able to insert traffic on the SBA interface when mTLS is not implemented	Success: Able to insert duplicate packet on SBA interface, which is received successfully by the AMF, causing it to issue a GOAWAY command
Unable to eavesdrop on the SBA interface when mTLS is implemented	Success: After successful TLS handshake, all subsequent data is encrypted and undecipherable
Unable to modify traffic on the SBA interface when mTLS is implemented	Success: After successful TLS handshake, any attempt to modify encrypted traffic results in an error and reset, terminating the connection
Unable to insert traffic on the SBA interface when mTLS is implemented	Success: Inserting duplicate encrypted packet into the SBA interface causes error and disconnection of session between network functions
Overall Test	Success

# Results

# **Conclusions and Next Steps**

This round of testing successfully verified the efficacy of employing security procedures recommended by the CSRIC VII WG3 report, implementing commercial hardware in a commercially-relevant SA configuration.

For each of the seven test cases described here, the tests successfully verified the efficacy of employing security procedures recommended by the CSRIC VII WG3 Report 2 recommendations for securing the 5G standalone network architecture. This verification of the CSRIC recommendations in a commercially-deployed environment is the first of its kind for 5G standalone networks. The test cases focused on confidentiality and integrity at multiple locations in the 5G system, including over-the-air between the UE and the RAN, for NAS signaling, for RRC signaling, over an untrusted backhaul, as well as on the Service-Based Architecture interface.

The first test case demonstrated that the implementation of NEA2 encryption on NAS messages enables user identity to be safely exchanged. With no encryption, as observed when setting the system to use the NULL NEA0 algorithm, messages containing user identities were exchanged between the UE and AMF in a way that message details were visible. However, when the NEA2 encryption algorithm was specified, all NAS messages were encrypted and undecipherable by an observer who does not have the correct encryption key. In addition, only non-user information was observable prior to NAS encryption, and user identity was transmitted via the SUCI.

The second test case considered confidentiality protection for RRC traffic. To test RRC confidentiality, Test Case 2 used an RF network monitoring tool to capture the messages transmitted over the air. First, this test demonstrated the visibility of identity-related data when no encryption (NULL scheme) was used for RRC messages. The captured data showed that the contents of RRC messages were fully decipherable by the RF monitoring tool. Second, the test demonstrated the concealment of the data when RRC encryption was enabled. In that test, the RF monitoring tool indicated the contents of the encrypted messages as "Extra bytes at end of RRC message," implying that there was additional data present in the packets, but the tool was unable to make sense of it.

The fifth test case addressed the CSRIC VII recommendation that devices and networks in the U.S. use IMSI privacy (SUCI) and do not use the NULL scheme, which could expose the IMSI/SUPI to an unauthorized entity. The test run on the 5GSTB demonstrated the use of the SUCI by the UE in the registration process and resulted in a successful registration.

The next test case reported here replicated tests performed previously for the NSA architecture, demonstrating that the implementation of an IPsec tunnel over an untrusted backhaul link prevents eavesdropping on both user plane and control plane traffic, as well as preventing modification and injection of false traffic designed to appear as originating from or destined to a valid UE. As with the NSA tests, use of the IPsec tunnel resulted in all traffic on the untrusted link appearing as encrypted ESP packets with no ability to read the contents. In addition, when attempting to modify and inject traffic into the transport link, the IPsec tunnel prevented all of the injected packets, or decrypted versions of them, from making it out of the tunnel to either the UE or the core-side router.

The final tests performed for this effort addressed security on the SBA interface, illustrating the benefits of mTLS among the multiple network functions. As such, there were two main parts to the test case: highlighting vulnerabilities without encryption; and demonstrating the protection provided by encrypting traffic on the SBA interface using mTLS. For the first part, it was shown that, without encryption, we were able to identify IP addresses for several network functions (AMF, AUSF, NRF, SMF, and UDM) as well as extracting user identity through the IMSI/SUPI. In addition, the tests demonstrated the ability to intercept messages between the NRF and AMF and modify the SMF IP address without producing an error when encryption was not used. It was also possible to insert duplicate packets on the SBA interface, which were received successfully

by the AMF and resulted in a GOAWAY command from the AMF. The second part, with mTLS enabled, encrypted traffic among the network functions. After being able to observe a successful TLS handshake between two network functions, all subsequently exchanged data were encrypted and undecipherable. Furthermore, attempts to modify and inject traffic on the SBA resulted in errors and tearing down the connection between the network functions.

The seven test cases summarized above validate a subset of the CSRIC VII WG3 recommendations. Validation of additional recommendations from WG3 Report 2 are anticipated when the available test tool capabilities are sufficient to run the appropriate tests and capture the required data. Some examples of required capabilities include the ability to alter a message after the integrity check is applied, as well as the ability to capture user plane traffic over the air, in order to demonstrate the efficacy of applying user plane integrity and of access stratum user plane confidentiality.

As new participants and the diversity of test cases grow in tandem, the 5G Security Test Bed will continue contributing to the evolving future of 5G network security, including additional phases of network slicing tests. For future tests, the 5G Security Test Bed is exploring additional aspects of network function security, false base stations, roaming security, and 5G cloud security that arise with use of the Network Exposure Function (NEF), the Application Function (AF), and Multi-access Edge Computing (MEC). The Test Bed is also exploring opportunities to test configurations of Open Radio Access Network (RAN) to verify security recommendations.

For more information, or to participate in the 5G Security Test Bed, please contact Harish Punjabi (hpunjabi@ctia.org; (202) 845 5701), or visit https://5gsecuritytestbed.com/.

# Appendix: Acronyms

3GPP	3rd Generation Partnership Project						
5G STB	5G Security Test Bed						
AMF	Access and Mobility Management Function						
AUSF	Authentication Server Function						
BBU	Baseband Unit						
СИОМ	Core Network Operations Manager						
СР	Control Plane						
CSRIC	Communications Security, Reliability, and Interoperability Council						
CSWG	Cybersecurity Working Group						
DHS	Department of Homeland Security						
DMC	Dual-Mode Core						
eMBB	Enhanced Mobile Broadband						
eNB	e-Node B						
ESP	Encapsulating Security Payload						
FCC	Federal Communications Commission						
IKEv2	Internet Key Exchange Protocol Version 2						
IMEISV	International Mobile Station Equipment Identity Software Version						
IMSI	International Mobile Subscriber Identity						
IPsec	Internet Protocol Security						
ITC	Integrated Traffic Capture						
ITU	International Telecommunications Union						

\_\_\_\_\_

ММЕ	Mobility Management Entity					
mTLS	Mutual Transport Layer Security					
MTP	Mobile Test Platform					
NAS	Non-Access Stratum					
NG-RAN	Next-Generation Radio Access Network					
NIST	National Institute of Standards and Technology					
NR	New Radio					
NRF	Network Repository Function					
NSA	Non-Standalone					
PDCP	Packet Data Convergence Protocol					
RAN	Radio Access Network					
RRC	Radio Resource Control					
SA	Standalone					
SBA	Service-Based Architecture					
SBI	Service-Based Interface					
SDR	Software-Defined Radio					
SEG	Security Gateway					
SUCI	Subscription Concealed Identifier					
SUPI	Subscription Permanent Identifier					
TAC	Technical Advisory Committee					
тс	Test Case					
ТСР	Transmission Control Protocol					
TLS	Transport Layer Security					

ТР	Test Point
TS	Technical Standards
UE	User Equipment
UP	User Plane
UPF	User Plane Function
VPN	Virtual Private Network
WG	Working Group