

# **Securing 5G:** mTLS Security on 5G Network SBI Test Report Q4 2023

# Table of Contents

Introduction
The 5G Security Test Bed Is the Latest Industry Initiative to Advance 5G Security3
The 5G Security Test Bed Uses Real-World Equipment, Validating Real-World Applications4
1.1.1. Real-World Testing4
1.1.2. Real-World Applications4
Background5
5G Security: The Service-Based Architecture, Transport Layer Security, and Zero Trust5
CSRIC VII7
Definition of Test Cases7
Test Results
Introduction8
1.1.3. Core IP Addresses
Test Case 1 – Understand SBI Vulnerabilities10
Test Case 2 – Implement Mutual TLS on SBA Interfaces17
Test Case 3 – Prevent Expired SBI Attach Request21
Test Case 4 – Prevent Unknown VNF Attach Request30
Test Case 5 – Implement Multi-Domain mTLS on SBI37
Conclusions and Next Steps 44
Appendix: Acronyms

# 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. The Test Bed's 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 (NSA) and standalone (SA) 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 use of mutual transport layer security (mTLS) in a 5G core network. 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.

# Background

# 5G Security: The Service-Based Architecture, Transport Layer Security, and Zero Trust

<u>Service-Based Architecture and Mutual Transport Layer Security.</u> One of the novelties of 5G is the introduction of a Service-Based Architecture (SBA) in which core network functionalities are delivered through a set of interconnected Network Functions (NFs), with the possibility of each NF to have access to services from another NF. Transport layer security (TLS) is a powerful encryption tool that can significantly enhance security across 5G SBA interfaces. When TLS is used between two 5G network functions across the SBA interface (SBI), the NFs authenticate each other using Mutual Transport Layer Security (mTLS) to confirm they are valid, then exchange information over the encrypted TLS connection.

The mTLS capabilities tested for in this report can serve as a foundational component of Zero Trust (ZT) on 5G networks.

Zero Trust. Zero Trust is a set of principles that significantly strengthens security on these networks. Zero Trust's core concepts are part of 3GPP's 5G standards, which define network security features for three domains of 5G: network access security, network domain security, and SBA domain security.<sup>1</sup>

Zero Trust principles enhance network security by requiring ongoing verification of users, applications, and associated devices beyond the network's endpoints. When Zero Trust principles are implemented, users, devices, and applications are authenticated at multiple points *within* the network as they access different areas of the network and corresponding network functions. The methods, applications, and components that are implemented to achieve Zero Trust are part of the Zero Trust Architecture (ZTA).

<u>Testing SBA Domain Security as Part of Zero Trust.</u> The U.S. government has recently focused on Zero Trust as a method of network security to address cybersecurity concerns. For example, in a June 2021 Executive Order, President Biden instructed the federal government to "advance toward Zero Trust Architecture" on its networks.<sup>2</sup> The Office of Management and Budget followed up with additional guidance for federal agencies that included requirements to encrypt network traffic.<sup>3</sup> The National Institute of Standards and Technology's (NIST) foundational guidance on Zero Trust, SP 800-207: *Zero Trust Architecture*, also recommends "authenticating all connections and encrypting all traffic" on a network.<sup>4</sup>

The test cases included in this report support SBA domain security and show how 5G specifications and mTLS can work to implement a Zero Trust Architecture.

For more details on how the wireless industry approaches Zero Trust, see CTIA's report on Defining Zero Trust: Industry Approaches and Policy Frameworks for Strong Wireless Network Security.<sup>5</sup>

<sup>&</sup>lt;sup>1</sup> See Jonathan Olsson at. al., Ericsson, Zero trust and 5G – Realizing zero trust in networks, (May 2021) <u>https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g</u>.

<sup>&</sup>lt;sup>2</sup> The White House, Executive Order 14028: Improving the Nation's Cybersecurity, (June 12, 2021), available at <u>https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/</u>.

<sup>&</sup>lt;sup>3</sup> OMB, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, M-22-09, (Jan. 26, 2022), <u>https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf</u>.

<sup>&</sup>lt;sup>4</sup> NIST, SP 800-207, Zero Trust Architecture, at 8 (Aug. 2020),

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

<sup>&</sup>lt;sup>5</sup> See CTIA, Defining Zero Trust: Industry Approaches and Policy Frameworks for Strong Wireless Network Security (Jan. 2023) <u>https://api.ctia.org/wp-content/uploads/2023/01/Defining-Zero-Trust-White-Paper-2023.pdf</u>

Confidential and Proprietary to the 5G Security Test Bed – Not for Disclosure

## **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 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 worked to identify and evaluate optional features in the 3GPP standards that would potentially cause security gaps in 5G if not implemented. CSRIC's Working Group 3 (WG3, "Managing Security Risk in Emerging 5G Implementations") released a March 2021 report, *Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security.*<sup>6</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. Based on its assessment, CSRIC recommended the use of TLS for Service-Based Architecture (SBA) interfaces.

This report addresses testing of the recommendation for the application of TLS for SBA interfaces (also called Service-Based Interfaces, or SBIs).

## **Definition of Test Cases**

Based on guidance from its Technical Advisory Committee and the relevant CSRIC VII WG3 recommendation, the 5G Security Test Bed established and executed five test cases described in this report, as follows:

Confidential and Proprietary to the 5G Security Test Bed – Not for Disclosure

<sup>&</sup>lt;sup>6</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>.

#### 1. Demonstrate Clear SBI Vulnerabilities:

a. <u>5G STB Test Case 1:</u> Show that critical information can be exposed on the 5G core SBA interfaces if data encryption is not implemented.

#### 2. Implement Mutual TLS on SBA Interfaces:

a. <u>5G STB Test Case 2</u>: Demonstrate the capability to encrypt critical user, device, and network information via HTTPS, and to authenticate and authorize both sides of the HTTPS connection through mTLS.

#### 3. Prevent Expired SBI Attach Request:

a. <u>5G STB Test Case 3:</u> Implement mutual TLS and prove that expired credentials on one end will lead to a failed SBI connection. This capability can keep out-of-date functions that may have vulnerabilities from attaching to the network.

#### 4. Prevent Malicious SBI Attach Request:

a. <u>5G STB Test Case 4-:</u> Show that in mutual TLS, invalid credentials on one end will lead to a failed SBI connection. This prevents unwanted functions from joining the network.

#### 5. Implement Multi-Domain mTLS on SBI:

a. <u>5G STB Test Case 5:</u> Demonstrate that a 5G core solution can be implemented securely using different vendors. This ensures mutual TLS sessions can be established across different certificate authorities (CAs).

# **Test Results**

## Introduction

This document presents the test results based on use cases corresponding to mutual TLS implementation on the Service-Based Interface. The 3GPP standards for 5G networks mandate the implementation of security controls for the SBIs on the 5G core but makes the use of them optional. These test cases are intended to validate the recommendations of the CSRIC Working Group 3 requirements for secure 5G deployment.

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. Figure 1 shows the relevant components of the Test Bed, including eight available test points (TPs). 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. The core is configured to support two network slices. The first slice is considered the default enhanced mobile broadband (eMBB) network slice. The second slice emulates a private network and includes the ability to form an IP security (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.

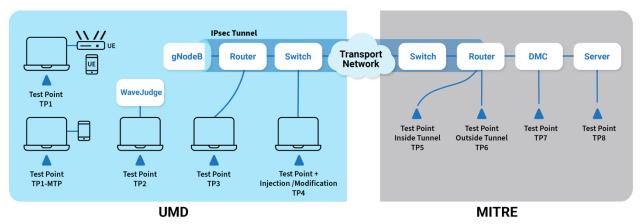


Figure 1:5G STB Lab Component Block Diagram and Test Points

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. For the purposes here, this report refers to the combination of that laptop and the cellular modem as the user equipment, or UE.

Packets are captured at the dual-mode core (TP7) as integrated traffic capture (ITC) traces and UE trace files.

Figure 2 shows the network elements within the Dual-Mode Core, including the network functions as they exchange TLS-encrypted information after mTLS verification. This network configuration was used for test cases 1-4.

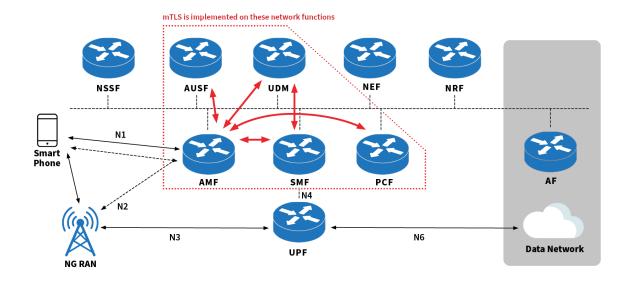


Figure 2: Basic UE Attach and PDU Request on SBI

#### **Core IP Addresses**

Table 1 lists the mapped IP addresses used by the various network functions used for the Service-Based Interfaces. Due the nature of the 5G core setup, some network functions, such as the 5G core Access and Mobility Management Function (AMF), communicated on multiple IP addresses.

#### Table 1: Dual-Mode Core SBI IP Address Assignments

/
8.251
3.251

## Test Case 1 – Understand SBI Vulnerabilities

#### Test Case ID: TC-SBI-01 Description:

This test is designed to determine if data traveling on the 5G core SBI is vulnerable in the event of a data breach.

## **Objectives:**

- As an "unauthorized" user, access and capture the content of the data carried on the SBI:
  - o User information
  - o Device information
  - o Location information
  - o Connection details

Logs were captured at the 5G core using ITC trace and UE trace logs. The UE started in airplane mode with all information about the UE deleted from the core. We then took the UE off airplane mode, successfully connected it to the network, put the UE back in airplane mode, and saved the ITC trace files. All the downloaded ITC trace files were dragged into an open Wireshark window session to merge all those traces into a single packet capture (PCAP) file.

From Figure 3, we see the AMF requesting AUSF (authentication server function) client services through an HTTP2 GET service frame request (packet 7). From the frame details, AMF provides the target PLMN list details for the requested AUSF (target-plmn-

list=[{"mcc":"310","mnc":"014"}]). It is clear from Figure 3 that the producer IP address is 192.168.56.143 at port 80, and therefore this must be the IP address of the 5G core's network repository function (NRF). In addition, the requester has IP address 172.17.152.146, the address of the AMF. In Figure 4, we see the HTTP2 HEADER 200 DATA frame response from the NRF (packet 8) to the AMF, which contains the IP address of the AUSF, 192.168.56.138, along with its status, service name, fully qualified domain name (FQDN), etc.

-				
<b>B</b> 2023	0303.1225-0500-202	30303.1230-0500-AMF.mtro	dmcamf01.FIV11_ue	trace.915
File Edit	View Go Ca	pture Analyze Statistic	s Telephony Wir	eless Tools Help
4 H.	1 @ 🐂 🛅	🕅 🔁 🖉 🛶 📦	🗰 🛣 🕹 🚞	🔲 🔍 🔍 🖽
http2 or	json			
No. T	ime Source	Destination	Protocol	Length Info
<b>7</b>		146 192.168.56.143	HTTP2	236 HEADERS[19]: GET /nnrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-type=AVF&target-plmn-list=%58%78%22mcc%22%3A%22%310%22%3
8		143 172.17.152.146	HTTP2/JSON	1281 HEADERS[19]: 200 OK, DATA[19], JavaScript Object Notation (application/json)
9		146 192.168.56.138	HTTP2/JSON	364 HEADERS[1]: POST /nausf-auth/v1/ue-authentications, DATA[1], JavaScript Object Notation (application/json)
10		146 192.168.56.138 146 192.168.56.138		364 HEADERS[1]: POST /nausf-auth/v1/ue-authentications, DATA[1], JavaScript Object Notation (application/json) 287 HEADERS[3]: PUT /nausf-auth/v1/ue-authentications/cid-eric-sausf-engine-08958bbdc-vc489-20230803127243-144/5g-aka-confirmation, DATA[3], JavaScript Object No
15		138 172.17.152.146		20/ NEADENS[3]: PUI /NBUST-BUENVA/UMM-BUENETLIGENCE/BUENETLIGENCE/BUENEBSSDECK-VC409-20230301/2/43-149/58-8K8-CONTINUETLIG, UAIA[3], JAVASCRIPT UDJECT NO 366 HEADENS[3]: 200 (N, DATA[3], JAVASCRIPT Object Notation (application/ison)
25		146 192.168.56.143		Job HEARCHS[2]]: GOT /nof-j, Jobac ip: Object Hotel application (spin-son) 133 HEARS[2]]: GOT /nnf-disc/vl/nf-instances/service-namesnudm-sdm&target-nf-type=UDM&requester-nf-type=AMF&supi=imsi-310014791791021
26		143 172 17 152 146		1458 HEADERSCRIFT, DAD AN ATAT/IL JavaScrint Object Notation (annicational providence) and a provide a start of the start
	Type: HEADER	5 (1)		
	Flags: 0x05,	End Headers, End Str	ream	
		00 0000 0000 0000 000	01 0011 = Stream	Identifier: 19
	[Pad Length:			
			f6e6e72662d64697	3632f76312f6e662d696e7374616e6365733f7365727669
	[Header Leng			
	[Header Cour Header: :sch			
			instances konuis	e-names=nausf-auth&target-nf-tvpe=AU5F&requester-nf-tvpe=AWF⌖+plm-list=%5F%7F%22mcc%22%3A%22310%22%2C%22%2C%22%3A%22014%22%3D%5D
	Name Len		Instances, servic	enimeseninusi encinaria Becelli etypeninisia edinesten elli etypenini tastenisioni natsintestasinastsitokstastastastastastastastastastastastastas
	Name: :p			
	Value Le			
	Value: /		ances?service-name	res=nausf-auth&target-nf-type=AUSF&requester-nf-type=AVF&target-plmn-list=%58%78%22mcc%22%3A%22310%22%2C%22%nc%22%3A%22014%22%7D%5D
	> :path: /	nrf-disc/v1/nf-insta	ances?service-nam	nes=nausf-auth&target-nf-type=AUSF&requester-nf-type=AMF&target-plmn-list=\$58%78%22mc%22%3A%22310%22%2C%22mnc%22%3A%223014%22%7D%5D
		segment: /nnrf-disc/		
		sub segment: service		h
		sub segment: target-		
		sub segment: request		
				%22mcc%22%34%22310%22%2C%22mcc%22%3A%22014%22%7D%5D
				ce-namesInau <mark>sF-auting-tinf-type-AUSFRequester-inf-type-AVFRtarget-plm-list=[["mcc":"310","mnc":"014"]]]</mark>
	Index: 4	ation: Literal heade	er rield with ind	remental indexing - indexed Name
	Header: :met	hod: GET		
		hority: 192.168.56.14	43:80	
	Name Len			
	Name: :a	thority		
	Value Le			
		2.168.56.143:80		
		y: 192.168.56.143:80		
		d: 192.168.56.143:80		
		ation: Literal Heade	er Field with Ind	remental Indexing - Indexed Name
	Index: 1			
	Header: cont			
L	[Full reques	t UKL: http://192.16	8.56.143:80/nnrt	-disc/v1/nf-instances?service-names-nausf-auth&target-nf-type=AUSF&requester-nf-type=AUF&target-plmn-list=%SB%78%22mcc%22%3A%22310%22%2C%22mnc%22%3A%22014%22%70%50]

Figure 3: Wireshark window showing UE trace with AMF request for AUSF services

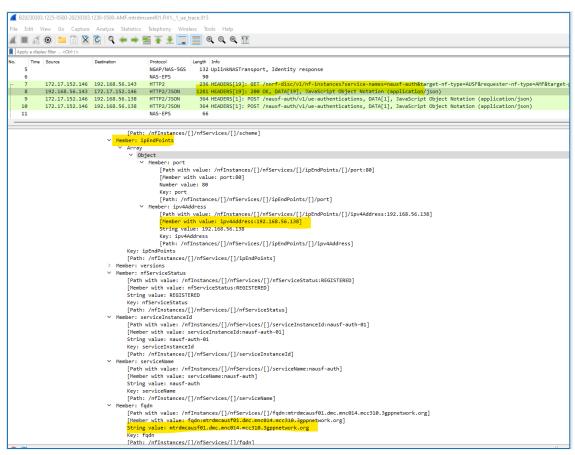


Figure 4: Wireshark window showing UE trace with NRF response to AMF request for AUSF services

Figure 5 shows that after obtaining the AUSF service IP address from the NRF, the AMF begins the UE authentication process through HTTP2 HEADER POST frame messages (packets 9 and 10). The AMF then requests authentication details from the UE (packet 12), and the UE responds with the authentication response parameter through the Uplink NAS (Non Access Stratum) Transport message<sup>7</sup> (packet 13). In addition, Figure 66 shows a message in which the UDM (unified data management) IP address, 192.168.56.137, is exposed (packet 26). Lastly, Figure 7 shows where the AMF requests PDU Establishment from the SMF (session management function), identifying a second AMF IP address, 172.17.27.33, as well as an SMF IP address, 192.168.56.131 (packet 63). These results are summarized in Table 2.

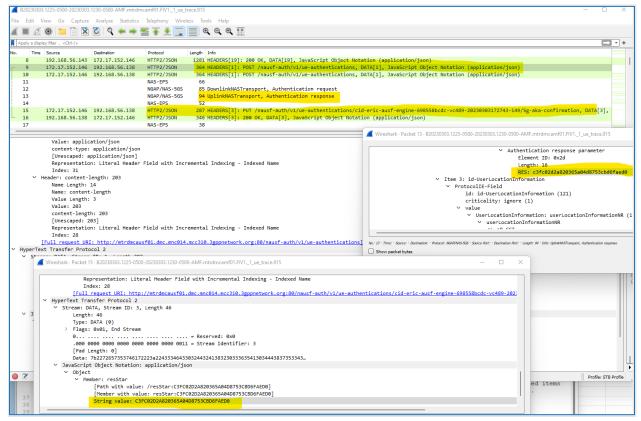


Figure 5: AMF initialization of UE authentication

<sup>&</sup>lt;sup>7</sup> "NAS signaling" carries the user data from the user equipment to the MME through the S1 pathway. Confidential and Proprietary to the 5G Security Test Bed – Not for Disclosure

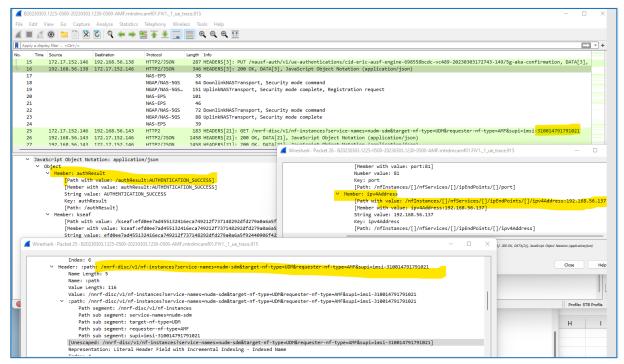


Figure 6: Wireshark window of UE trace showing UDM IP address

	i 🛃 🙆	📄 🗋 🔀 🖸	९ 🗢 🔿 🔮	i 🐔 👱 🛄		Ð,	Q		11						
)	ly a display filter .	<%/>>				89									-
	Time	Source	Destination	Protocol	Length	Info									
	59			NGAP/NAS-5GS	163	Upli	InkNAST	rans	port						
	60			NAS-EPS	113										
	61	172.17.152.146	192.168.56.143	HTTP2	253	HEAD	ERS [25	]: 0	GET /nnr	f-disc	/v1/nf-	instand	ces?servic	e-names=nsmf	-pdu
	62	192.168.56.143	172.17.152.146	HTTP2/JSON	1029	HEAD	ERS [25	]: 2	00 OK,	DATA [2	5], Jav	aScript	t Object N	otation (app	lica
	63	172.17.27.33	192.168.56.131	HTTP2/JSON/	1556	HEAD	DERS [81	]: P	POST /ns	mf-pdu	session	/v1/sm-	-contexts,	DATA[81], J	avaS
	64	192.168.56.131	172.17.27.33	HTTP2/JSON	172	HEAD	ERS [81	]: 2	01 Crea	ted, [	ATA[81]	, Javas	Script Obj	ect Notation	(ap
	65			NGAP	44	UECo	ontextR	elea	seReque	st					
	66			NGAP	40	UECo	ontextR	elea	seComma	nd					
	67			NGAP	61	UECO	ontextR	elea	seCompl	ete					
	68	192.168.57.201	172.17.27.33	HTTP2/JSON/	1164	HEAD	DERS[1]	: P0	ST /nam	f-com	/v1/ue-	-context	ts/imsi-31	001479179102	1/n1
	c0			NCAD		D									
		pt Object Notation: ap	plication/json						4a 43				d 58 37 3		
	V Object				01				71 46				55 36 7a 6 39 44 38 3		
		ber: supi							31 63				6 53 43 0		
		[Path with value: /supi			01				74 65				5 3a 20 6		
		[Member with value: sup	i:imsi-3100147917	91021]	014	40 7	0 70 6	c 69	63 61	74 69	6f 6e	2f 6a 7	73 6f 6e Ø	d pplicati	on/
	5	String value: imsi-3100	14791791021		01				22 73				69 6d 73 6		
		Key: supi							30 31				31 30 32 3		
	1	[Path: /supi]											59 73 76 2 36 36 32 3		
	Mem	ber: pei							70 73				50 50 52 5 59 73 64 6		
ſ		[Path with value: /pei:	imeisv-3517351101	216621]					37 39				c 22 70 6	4 -7917910	021
		[Member with value: pei	:imeisv-351735110	1216621]					73 69				31 2c 22 6		Id"
	5	String value: imeisv-35	17351101216621						22 64				2 2d 73 7		
	ĸ	Key: pei							69 74				2 2c 22 7		
	1	[Path: /pei]							69 22 3a 22				22 3a 31 2 22 7d 2c 2		
	Mem	ber: gpsi							69 6e				a 22 65 6		
	1	[Path with value: /gpsi	:msisdn-791791002	1]					66 30				34 39 37 3		
		[Member with value: gps							30 2d				5 61 38 6		
	S	String value: msisdn-79	17910021						22 67				b 22 70 6		
		Key: gpsi							22 3a				Ba 22 33 3		
		[Path: /gpsi]							6d 6e				34 22 7d 2 30 38 44 2		
		ber: pduSessionId							65 72				4 77 6f 7		
		[Path with value: /pduS	SessionId:11						22 6d				31 30 22 2		
		[Member with value: pdu							22 3a				c 22 72 6		
		Number value: 1	13C3310110.1]						74 54				19 4e 49 5		
		Key: pduSessionId							52 45				c 22 6e 3		
		[Path: /pduSessionId]							67 22 22 6e				4 65 6e 7 2 7d 2c 2		
		ber: dnn							70 65				0 5f 41 4		
		[Path with value: /dnn:	don_ombb_cth2 mit	co notl									0 65 22 3	a CESS","r	atT
		[Member with value: dnr			03	00 2	2 4e 5	2 22	2c 22	75 65	4c 6f	63 61 7	4 69 6f 6	e "NR","ue	Loc
		String value: dnn-embb-		ire.net]		ame (1	556 bytes		Decomo	neend L	eader (288	butes)			_

Figure 7: Wireshark UE trace showing UE PEI: SUPI, IMEISV

Confidential and Proprietary to the 5G Security Test Bed – Not for Disclosure

Network Function	IP Address	Packet
AMF	172.17.152.146 172.17.27.33	Packet 7 Packet 63
AUSF	192.168.56.138	Packet 8
NRF	192.168.56.143	Packet 7
SMF	192.168.56.131	Packet 63
UDM	192.168.56.137	Packet 26

Table 2: Network Function IP Addresses identified in UE Trace

In addition to the NF IP addresses, the unencrypted SBI also exposes UE identifying information. Specifically, Figure 7 shows the PDU Establishment message in which the AMF provides the SMF with the UE SUPI and IMEISV, where the SUPI is the Subscriber Permanent Identifier, equivalent to the International Mobile Subscriber Identity (IMSI), and the IMEISV is the International Mobile Equipment Identity Software Version, or the code that identifies the specific UE's software. We note that the SUPI was also exposed in packet 25, shown in Figure 6 above. Figure 8 shows that same message where the NR Cell ID is also provided in the clear. These results are summarized in Table 3.

• •	•	<b>a</b> B:	20230303.1225-050	0-20230303.1230-(	)500-AM	IF.mtrdr	ncamf	01.FIV1.	1 ue trace	.915.r	cap					
	- <u></u>		0 4 -	= <u> </u>												
		· · · · · · · · · · · · · · · · · · ·		∎ ♥ ≚ 💻		~	~		-						_	۰.
No.	ply a display filter	Source	Destination	Protocol	Length	Info										- +
INO.	59	Source	Destination	NGAP/NAS-5GS			LNACT	ranspor	+							
	60			NAS-EPS	103		NINAJI	anspor	L L							
	61	172.17.152.146	192.168.56.143	HTTP2			RS [25	: GET	/nnrf-disc	c/v1/r	nf-ins	tance	s?service	-names=ns	mf-pdu	
	62	192.168.56.143	172.17.152.146	HTTP2/JSON	1029	HEADE	RS [25	: 200	OK, DATA[2	25], 3	lavaSc	ript	Object No	tation (a	pplica	'
Г	63	172.17.27.33	192.168.56.131	HTTP2/JS0N/	1556	HEADE	RS[81	: POST	/nsmf-pdu	sess	ion/v1	/sm-c	ontexts,	DATA[81],	Javas	5
	64	192.168.56.131	172.17.27.33	HTTP2/JSON					Created, [	DATA [8	31], J	avaSc	ript Obje	ct Notati	on (ap	
	65			NGAP				eleaseR								
	66			NGAP				eleaseC								
	67	100 100 57 001	470 47 07 00	NGAP					omplete				11	04 4704 704	000 (	
	68	192.168.57.201	172.17.27.33	HTTP2/JSON/		HEADE		PUST	/namf-com	n/v1/(	ie-con	texts	/1ms1-310	014/91/91	021/n	
			cation/nrLocation,						0390	Зa	22 30	31 38	36 41 3	2 31 32 4	14 22	7d 7d
		Member: ncgi							03a0				6e 74 6			61 74
		v Object							03b0				22 68 7			2f 5c
		∨ Member: pl	lmnId						03c0 03d0				38 2e 3 61 6c 6			33 3a 73 5c
		v Object							03e0				64 75 7			6f 6e
		Member							03f0	76	31 5c	2f 69	6d 73 6	2d 33	31 30	30 31
			ath with value: /		tion/nc	:gi/plm	nId/m	c:001]	0400				30 32 3			2d 63
			ember with value:	mcc:001]					0410 0420				3 5c 2f 2 39 30 3			
			ring value: 001						0430				2 3a 22 5			49 45
			y: mcc		1	1			0440				49 6e 7			
			ath: /ueLocation/	nrLocation/ncgi/p	) (mnia/m	ICC]			0450				3a 22 4			
		<ul> <li>Member</li> </ul>		uel ecotion (pri eco	+ i = = / = =	ai/n]m	nTd (m		0460				6e 61 6 70 4f 6			3a 66
			ath with value: / ember with value:		11100/00	.g 1/p till	INTO/III	10:001]	0480				22 69 6			
			ring value: 001	muc:001]					0490				65 2c 2			
			v: mnc						04a0				3a 66 6			
			ath: /ueLocation/	nrlocation/negi/r	lmnTd/m	ncl			04b0 04c0				2 61 64 6 5 78 74 6			
		Key: pl			) (IIIIIIU/II	inc]			04C0				5 72 49 6			
		, ,	/ueLocation/nrLoc	ation/ncgi/nlmnTc	1				04e0				61 74 6			
		Member: nr		acton, negt, pennie					04f0				61 6c 7			
			ith value: /ueLoc	ation/nrlocation/	'ncai/nr	CellId	.0186	21201	0500 0510				72 49 6			
			with value: nrCe		neg1/m	cettia	10100/	(LILD]	0510				1 6f 69 4 7 30 64 4			72 6d 53 41
			value: 0186A212D						0530				6e 33 3			74 75
		Key: nr							0540				30 41 6			
		,	/ueLocation/nrLoc	ation/ncgi/nrCell	[bl				0550 0560				0d 0a 4			
		Key: ncgi			-				0560				53 6d 4			43 6f 70 6c
		[Path: /ueLo	cation/nrLocation,	/ncgi]									2f 76 6			
		Key: nrLocation		-					0590	67	6e 61	73 00	0a 0d 0	a 2e 01	13 c1	00 00
		[Path: /ueLocation	n/nrLocation]						05a0	01	00 7b	00 29	80 80 2	L 10 01	00 00	10 81
_	Ke	ey: ueLocation							Fram	ne (1556	6 bytes)	De	compressed	Header (288	bytes)	
0 7	Member with value	ue (json.member_with_value), 1	11 bytes						Packets: 27	6 · Disn	laved: 2	76 (100	.0%)		Profile:	Default
		vuide),								- 0.5p	,					_ staan

Figure 8: Wireshark UE Trace showing NR Cell ID

Table 3: UE identifying information observed on SBI

UE Parameter	Value	Packet
SUPI/IMSI	310014791791021	Packets 25,63
IMEISV	3517351101216621	Packet 63
NR Cell ID	0186A212D	Packet 63

#### Success Criteria:

- 1. Able to eavesdrop on SBA interfaces.
- 2. Able to capture device/user/connection-specific information: specifically SUPI, IMEISV, and NR Cell ID.
- 3. Able to capture network information: specifically AMF, SMF, NRF, and AUSF IP addresses.

Confidential and Proprietary to the 5G Security Test Bed – Not for Disclosure

#### Results

Condition	Status
Able to eavesdrop on SBA interfaces	Success: HTTP2 and other
	messages are decipherable.
Able to capture device/user/connection specific	Success: Identified SUPI, IMEISV,
information, specifically SUPI, IMEISV, and NR Cell ID	and NR Cell ID in PDU
	Establishment message.
Able to capture network information, specifically AMF,	Success: Identified IP addresses
SMF, NRF, and AUSF IP addresses	for AMF, AUSF, NRF, SMF, and
	UDM.
Overall Test	Successfully demonstrated that,
	in the event of a data breach,
	critical information can be
	exposed on the 5G core SBA
	interfaces if data encryption is
	not implemented.

## Test Case 2 – Implement Mutual TLS on SBA Interfaces

#### Test Case ID: TC-SBI-02

#### Description:

Utilizing the same configuration setup as Test Case 1, Test Case 2 is designed to implement mTLS as a requirement for SBI communications. This test case is intended to demonstrate both the authentication/authorization components of mTLS, as well as to verify that mTLS can authenticate and authorize both ends of the HTTPS connection.

#### Objectives:

- Demonstrate the ability to encrypt critical user, device, and network information via HTTPS using mTLS.
- Demonstrate the ability to authenticate/authorize both sides of an HTTPS connection using mTLS.

From both the combined ITC trace files and from the UE trace file, we can get additional details regarding the NFs interactions. In Figure 9, the combined ITC trace file shows the three-way handshake establishment of a TCP session between the SMF and NRF. Subsequently, immediately following establishment of the TCP session, Figure 10 shows the TLS handshake between the SMF and NRF, including the client and server hellos and the key exchange.



Following mTLS establishment, the resulting data streams between the NFs are encrypted (packet 14675, 14679, etc.) and shown only as Application Data in Wireshark rather than exposing the contents of the messages. In addition, Figure 11: illustrates how all traffic traversing other SBI interfaces, e.g., between UDM (192.168.56.137) and AMF (192.168.56.197, 172.17,95.197, and 172.17.27.33), are encrypted and indecipherable.

	1 🖉 🛞 🚞 🕯						
ip.ad	ldr == 192.168.56.129						
	Time	Source	Destination	Protocol	Source De	tinat Length	Info
146	61 1486.223979	172.17.27.33	192.168.56.129	TCP	43074 7	970 7	76 43074 → 7070 [SYN] Seq=0 Win=62720 Len=0 MSS=8960 SACK_PERM TSval=3929595204 TSecr=0 WS=256
146	62 1486.224145	192.168.56.129	172.17.27.33	TCP	7070 43	374 7	76 7070 → 43074 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=1432070386 TSecr=392
	63 1486.224164		192.168.56.129	TCP	43074 7		68 43074 → 7070 [ACK] Seq=1 Ack=1 Win=62720 Len=0 TSval=3929595204 TSecr=1432070386
	64 1486.225036		192.168.56.129	TLSv1.2	43074		91 Client Hello
		192.168.56.129	172.17.27.33	TCP	7070 43		68 7070 → 43074 [ACK] Seq=1 Ack=224 Win=62464 Len=0 TSval=1432070387 TSecr=3929595205
		192.168.56.129	172.17.27.33	TLSv1.2	7070 43		68 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
	69 1486.240509		192.168.56.129	TCP	43074 7		68 43074 → 7070 [ACK] Seq=224 Ack=2401 Win=60416 Len=0 TSval=3929595221 TSecr=1432070403
	71 1486.259719		192.168.56.129	TLSv1.2	43074 7		31 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Mes
		192.168.56.129	172.17.27.33	TCP	7070 43		68 7070 → 43074 [ACK] Seq=2401 Ack=2487 Win=60416 Len=0 TSval=1432070422 TSecr=3929595240
		192.168.56.129	172.17.27.33	TLSv1.2	7070 43		19 Change Cipher Spec, Encrypted Handshake Message
	74 1486.263527		192.168.56.129	TCP	43074		68 43074 → 7070 [ACK] Seq=2487 Ack=2452 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426
	75 1486.263871		192.168.56.129	TLSv1.2	43074		49 Application Data
146	76 1486.263934	192.168.56.129	172.17.27.33	TCP	7070 43		68 7070 → 43074 [ACK] Seq=2452 Ack=2568 Win=60416 Len=0 TSval=1432070426 TSecr=3929595244
146	78 1486.263984		172.17.27.33 192.168.56.129 bits), 76 bytes ca	TLSv1.2 TCP	7070 43 43074 7	970 G	40 Application Data 58 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 
146 Fra Lin	78 1486.263984 mme 14661: 76 by nux cooked captu	172.17.27.33 rtes on wire (608 ure v1	192.168.56.129 bits), 76 bytes ca	TCP	43074 3	970 G	68 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426
146 Fra Lin Int	me 1486.263984 me 14661: 76 by nux cooked captu cernet Protocol	172.17.27.33 rtes on wire (608 ure v1 Version 4, Src: 1	192.168.56.129	TCP aptured (608 192.168.56.	43074 ; bits) on i 129	970 6	58 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426
146 Fra Lin Int	78 1486.263984 mme 14661: 76 by nux cooked captu ernet Protocol msmission Contr Source Port: 4	172.17.27.33 rtes on wire (608 ire v1 Version 4, Src: 1 rol Protocol, Src 3074	192.168.56.129 bits), 76 bytes ca 72.17.27.33, Dst:	TCP aptured (608 192.168.56.	43074 ; bits) on i 129	970 6	68 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426
146 Fra Lin Int	78 1486.263984 mme 14661: 76 by nux cooked captu sernet Protocol insmission Contr Source Port: 4. Destination Po	172.17.27.33 rtes on wire (608 ure v1 Version 4, Src: 1 vol Protocol, Src 3074 rt: 7070	192.168.56.129 bits), 76 bytes ca 72.17.27.33, Dst:	TCP aptured (608 192.168.56.	43074 ; bits) on i 129	970 6	King 2 - 2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432870426      Mineshark- Packet 14676 - CSRIC_7b-and-mTL5_t2_combined-itc-trace-files_06-01-23_1100am.pcapng      Frame 14676: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface unknown, :     Linux cooked capture v1
146 Fra Lin Int	78 1486.263984 mme 14661: 76 by nux cooked captu ternet Protocol insmission Contr Source Port: 4. Destination Poo [Stream index:	172.17.27.33 tes on wire (608 tre v1 Version 4, Src: 1 tol Protocol, Src 3074 rt: 7070 208]	192.168.56.129 bits), 76 bytes ca 72.17.27.33, Dst: Port: 43074, Dst F	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	58 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432870426
146 Fra Lin Int	78 1486.263984 imme 14661: 76 by uux cooked captu isernet Protocol insmission Contr Source Port: 4: Destination Poo [Stream index: [Conversation of the second sec	172.17.27.33 rtes on wire (608 ire v1 Version 4, Src: 1 rol Protocol, Src 3074 rt: 7070 208] completeness: Incc	192.168.56.129 bits), 76 bytes ca 72.17.27.33, Dst:	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	King 2 - 2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426      Mineshark- Packet 14676 - CSRIC_7b-and-mTL5_t2_combined-itc-trace-files_06-01-23_1100am.pcapng      Frame 14676: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface unknown,     Linux cooked capture v1
L46 Fra Lin Int	78 1486.263984 mme 14661: 76 by nux cooked captu cernet Protocol msmission Contr Source Port: 4. Destination Poo [Stream index: [Conversation of [TCP Segment Li	172.17.27.33 tes on wire (608 ire v1 Version 4, Src: 1 tol Protocol, Src 3074 rt: 7070 208] completeness: Incompleteness: Incompletene	192.168.56.129 bits), 76 bytes ca 72.17.27.33, Dst: Port: 43074, Dst F	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 </pre>
146 Fra Lin Int	78 1486.263984 mme 14661: 76 by uux cooked captu uux cooked captu uux cooked captu uux cooked captu uux cooked captu sernet Protocol [Stream index: [Conversation o [TCP Segment Lu Sequence Number	172.17.27.33 ttes on wire (608 ire v1 version 4, Src: 1 ol Protocol, Src 3074 rt: 7070 208] completeness: Inco en: 0] r: 0 (relative	192.168.56.129 bits), 76 bytes ca 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number)	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426</pre>
146 Fra Lin Int	78 1486.263984 mme 14661: 76 by ux cooked captu- cernet Protocol nemission Contr Source Port: 4 Destination Po- [Stream index: [Conversation [TCP Segment L Sequence Numbe	172.17.27.33 tes on wire (608 ire v1 Version 4, Src: 1 val Protocol, Src 3074 rt: 7070 208] completeness: Incc en: 0] r: 0 (relative r (raw): 18816623i	192.168.56.129 bits), 76 bytes ca 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number) 32	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	S8 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 inknown, id 0 Wireshark-Packet 14676 - CSRIC_7b-and-mTL5_t2_combined-itc-trace-files_06-01-23_1100am.pcapng Frame 14676: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface unknown, Linux cooked capture v1 Intermet Protocol Version 4, Src: 192.168.56.129, Dst: 172.17.27.33 Transmission Control Protocol, Src Port: 7070, Dst Port: 43074, Seq: 2452, Ack: 2568, Len: 0 Source Port: 7070 Destination Port: 43074
146 Fra Lin Int	78 1486.263984 mme 14661: 76 by ux cooked captu ernet Protocol nomission Contr Source Port: 4. Destination Poi [Stream index: [Conversation TCP Segment L Sequence Numbe Sequence Numbe	172.17.27.33 tes on wire (608 ire v1 Version 4, Src: 1 vol Protocol, Src 208] completeness: Incr en: 0] r: 0 (relative r (raw): 18816623 Number: 1 (re:	192.168.56.129 bits), 76 bytes ca 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number)	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 inknown, id 0</pre>
L46 Fra Lin Int	mm 1486.263984 mm 14661: 76 by ux cooked capturent Protocol numission Contr Source Port: 4. Destination Port: 4. Destination Port: (Conversation on [TCP Segment L Sequence Numbe [Next Sequence [Next Sequence Acknowledgment	172.17.27.33 ttes on wire (608 re v1 Version 4, Src: 1 01 Protocol, Src 3074 trt: 7070 2083 Completeness: Incc en: 0] r: 0 (relative r (raw): 18816623 Number: 0	192.168.56.129 bits), 76 bytes ca 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number) 32	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432870426</pre>
L46 Fra Lin Int	778 1486.263984 me 14661: 76 by me 14661: 76 by Source Ports 4 Destination Pon Stream Index: [Conversation - ICP Segment L Sequence Numbe [Next Sequence Acknowledgment	172.17.27.33 tes on wire (608 re v1 Version 4, Src: 1 00 Protocol, Src 3074 rt: 7070 208] completeness: Inc. en: 0] r: 0 (relative r (raw): 188166232 Number: 0 number (row): 0	192.168.56.129 bits), 76 bytes ce 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number) 32 lative sequence nu	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 4304 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 inknown, id 0 00.04.09.01.09.06.09.54.5 Wreshark-Packet14676 - CSRC_7b-and-mTL5_t2_combined-itc-trace-files_06-01-23_1100am.pcapng &gt; Frame 14676: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface unknown, &gt; Linux cooked capture v1 &gt; Internet Protocol Version 4, Src: 192.168.56.129, Dst: 172.17.27.33 &gt; Transmission Control Protocol, Src Port: 7070, Dst Port: 43074, Seq: 2452, Ack: 2568, Len: 0 Source Port: 7070 Destination Port: 43074 [Stream index: 2081] [Conversation completeness: Incomplete, DATA (15)] [TCP Segment Len: 0]</pre>
L46 Fra Lin Int	<pre>r78 1486.263984 mme 14661: 76 by www.cooked captu ernet Protocol nmmission Contr Source Port: 4 Destination Poort: 4 Destination Poort: 4 Conversation ITCP Segment L Sequence Numbe Sequence Numbe Sequence Numbe INext Sequence Acknowledgment Acknowledgment Acknowledgment Nath Sequence Numbe Nath Sequence Numbe Next Sequence Nath Nath Nath Nath Nath Nath Nath Nath</pre>	172.17.27.33 ttes on wire (608 re v1 Version 4, Src: 1 vol Protocol, Src 3074 trt: 7070 2083 completeness: Incc m: 0] (relative r (raw): 18816623 Number: 1 (rec Number: 0 number: (raw): 0 State (raw): 40 by (ra	192.168.56.129 bits), 76 bytes ce 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number) 32 lative sequence nu	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 inknown, id 0 000 00 00 00 00 00 00 00 00 00 00 00</pre>
146 Fra Lin Int Tra	778 1486.263984 mme 14661: 76 by uux cooked capturernet Protocol memission Contr Source Port: 4 Destination Po [Stream index: [Conversation - [TCP Segment L Sequence Numbe [Next Sequence Acknowledgment 1010 # He Flags: 0x002 (°	172.17.27.33 ttes on wire (608 re v1 Version 4, Src: 1 vol Protocol, Src 3074 trt: 7070 2083 completeness: Incc m: 0] (relative r (raw): 18816623 Number: 1 (rec Number: 0 number: (raw): 0 State (raw): 40 by (ra	192.168.56.129 bits), 76 bytes ce 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number) 32 lative sequence nu	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 43074 + 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 min.owm, id 0</pre>
146 Fra Lin Int Tra	778 1486.263984 mme 14661: 76 by www.cooked captu ernet Protocol Source Port: 4. Destination Poo Stream index: [Conversation ITCP Segment L. Sequence Numbe Sequence Numbe	172.17.27.33 tes on wire (608 re v1 Version 4, Src: 1 00. Protocol, Src 3074 2081 2081 2081 r: 0 (relative r (raw): 0 Number: 0 Number: 0 Number: 0 Number: 40 by Srt) 40 by Srt) 40 by Srt) 40 by Srt) 40 by Srt) 40 by Srt) 40 by Srt) 40 by Srt) 40 by Srt) 40 by Srt (raw): 0 Srt) 40 by Srt) 40	192.168.56.129 bits), 76 bytes ce 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number) 32 lative sequence nu	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 4304 → 7070 [ACK] Seq-2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 inknown, id 0</pre>
146 Fra Lin Int Tra	778 1486.263984 me 14661: 76 by uux cooked captu ternet Protocol Destination Poo [Stream index: [Conversation Poo [Stream index: [Conversation Poo [Stream index: [Conversation Pool [Stream index: [Conversation Pool Sequence Numbe [Next Sequence Acknowledgment Acknowledgment 1019 = He Flags: 0x002 ( Window: 62720 [Calculated wix	172.17.27.33 ttes on wire (608 re v1 Version 4, Src: 1 vol Protocol, Src 3074 trt: 7070 2083 completeness: Incc m: 0] (relative r (raw): 18816623 Number: 1 (rec Number: 0 number: (raw): 0 State (raw): 40 by (ra	192.168.56.129 bits), 76 bytes ce 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number) 32 lative sequence nu	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 43074 → 7070 [ACK] Seq=2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 inknown, id 0</pre>
146 Fra Lin Tra	778 1486.263984 mme 14661: 76 by ux cooked capturernet Protocol memission Contr Source Port: 4 Destination Po Destination Po Esteranti index: [Conversation - ICP Segment L. Sequence Numbe Sequence Numbe Sequenc	172.17.27.33 tes on wire (608 re v1 Version 4, Src: 1 00 Protocol, Src 208] completeness: Incc n: 0] (relative r: 0 (relative r: (new): 1816623 Number: 1 (rei number (raw): 0 ader Length: 40 by SWI	192.168.56.129 bits), 76 bytes ce 72.17.27.33, Dst: Port: 43074, Dst F omplete, DATA (15) sequence number) 32 lative sequence nu	TCP aptured (608 192.168.56. Port: 7070,	43074 ; bits) on i 129	970 6	<pre>58 4304 → 7070 [ACK] Seq-2568 Ack=2524 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426 inknown, id 0</pre>

a Edit View C-					
	Capture Analyze S				
🔳 🖉 🔘 🚞 📕	🖹 🔀 🔇 🔍 🔶	• 🔹 😫 🛧 👱		Q. Q. 🎹	
ip.addr == 192.168.56.129					
Time	Source	Destination	Protocol	Source Destinat L	
14664 1486.225036		192.168.56.129	TLSv1.2	43074 7070	291 Client Hello
14665 1486.225105		172.17.27.33	TCP	7070 43074	68 7070 → 43074 [ACK] Seq=1 Ack=224 Win=62464 Len=0 TSval=1432070387 TSecr=3929595205
14668 1486.240493		172.17.27.33	TLSv1.2	7070 43074	2468 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
14669 1486.240509 14671 1486.259719		192.168.56.129 192.168.56.129	TLSv1.2	43074 7070 43074 7070	68 43074 → 7070 [ACK] Seq=224 Ack=2401 Win=60416 Len=0 TSval=3929595221 TSecr=1432070403 2331 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
14672 1486.259815		172.17.27.33	TCP	7070 43074	25) Certificate, Cirent Key Exchange, Certificate Verify, Change Lipper spect, Encrypted nanosnake message 68 7070 + 43074 [Ack] Seq-2401 Ack-2487 Win-60416 Len=0 TSval=1432070422 TSecr=3929595240
14673 1486.263520		172.17.27.33	TLSv1.2	7070 43074	19 Change Cipher Spec. Encrypted Handshake Message
14674 1486.263527		192.168.56.129		43074 7070	68 43074 + 7070 [ACK] Seq=2487 ACk=2452 Win=60416 Len=0 TSval=3929595244 TSecr=1432070426
14675 1486.263871	172.17.27.33	192.168.56.129	TLSv1.2	43074 7070	149 Application Data
14676 1486.263934	192.168.56.129	172.17.27.33	TCP	7070 43074	68 7070 → 43074 [ACK] Seq=2452 Ack=2568 Win=60416 Len=0 TSval=1432070426 TSecr=3929595244
14677 1486.263980		172.17.27.33	TLSv1.2	7070 43074	140 Application
14678 1486.263984		192.168.56.129		43074 7070	68 43074 → 7070
14679 1486.264080		192.168.56.129		43074 7070	106 Application [ 68 7070 + 43074 ] Frame 14664: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface unknown,
14680 1486.264128			TCP	7070 43074	
14681 1486.265192 14682 1486.265246		192.168.56.129	TCP	43074 7070 7070 43074	251 Application [ > Linux cooked capture v1 68 7070 + 43074 > Internet Protocol Version 4, Src: 172.17.27.33, Dst: 192.168.56.129
14683 1486.265286		192.168.56.129		43074 7070	too /0/0 + 450/4
14684 1486.265329			TCP	7070 43074	68 7070 + 43074 Y Transport Layer Security
					<ul> <li>TLSv1.2 Record Layer: Handshake Protocol: Client Hello</li> </ul>
					Content Type: Handshake (22)
		744 bits), 2468 bj	/tes captured	d (19744 bits) o	Content Type: Handshake (22) n interface unknown, Version: TLS 1.2 (0x0303)
Linux cooked captu	ire v1				Content Type: Handshake (22) on interface unknown, Version: TL5 1.2 (0x0303) Length: 218
Linux cooked captu Internet Protocol	vre v1 Version 4, Src: 1	92.168.56.129, Dst	t: 172.17.27.	.33	Content Type: Handshake (22) Version: TLS 1.2 (Øx8303) Length: 218 > Handshake Protocol: Client Hello
Linux cooked capto Internet Protocol Transmission Contr	ure v1 Version 4, Src: 1 Tol Protocol, Src	92.168.56.129, Dst	t: 172.17.27.	.33	Content Type: Handshake (22) Version: TLS 1.2 (Øx8303) Length: 218 > Handshake Protocol: Client Hello
Linux cooked captu Internet Protocol Transmission Contr Transport Layer Se	ure v1 Version 4, Src: 1 rol Protocol, Src ecurity	92.168.56.129, Dst	t: 172.17.27. prt: 43074, S	.33	Content Type: Handshake (22) Version: TLS 1.2 (0x8303) Length: 218 > Handshake Protocol: Client Hello
Linux cooked captu Internet Protocol Transmission Contr Transport Layer Se Y TLSv1.2 Record	ure v1 Version 4, Src: 1 rol Protocol, Src ecurity	92.168.56.129, Dst Port: 7070, Dst Po Protocol: Server	t: 172.17.27. prt: 43074, S	.33	Content Type: Handshake (22) Mersian: IS 1.2 (0x0303) Length: 218 > Handshake Protocol: Client Hello
Linux cooked captu Internet Protocol Transmission Contr Transport Layer Se V TLSv1.2 Record Content Typ	ure v1 Version 4, Src: 1 rol Protocol, Src ecurity Layer: H <mark>andshake</mark>	92.168.56.129, Dst Port: 7070, Dst Po Protocol: Server	t: 172.17.27. prt: 43074, S	.33	Content Type: HandShake (22) Wersion: ISL 2 (0x8393) Length: 218 > HandShake Protocol: Client Hello No. MeM - Thre: Med.2000 - Source 173:12233 - Desination: HELBERGS Protocol: TS-12 - Source Part: 4004 - Desination Part: 7007 - Length: 281 - Sher Direct Parts No. MeM - Thre: Hell.2000 - Source 173:12233 - Desination: HELBERGS Protocol: TS-12 - Source Part: 4004 - Desination Part: 7007 - Length: 281 - Sher Direct Parts Show packet bytes
Linux cooked captu Internet Protocol Transmission Contr Transport Layer Se V TLSv1.2 Record Content Typ Version: TI Length: 98	version 4, Src: 1 vol Protocol, Src courity Layer: H <mark>andshake</mark> pe: Handshake (22) LS 1.2 (0x0303)	92.168.56.129, Dsf Port: 7070, Dst Po Protocol: Server	t: 172.17.27. prt: 43074, S	.33	Content Type: Handshake (22)           Interface unknown,           Uersion: IS 1.2 (0x0303)           Length: 218           Handshake Protocol: Client Hello           No. MBH - Time HBL200D - Sume XTL27220 - Desination XELBESLID - Induct: TL542 - Sume Part: 4004 - Desination Part: 700 - Length: 28 - Sine Oleri Malo           Show packet bytes
Linux cooked captu Internet Protocol Transmission Contr Transport Layer SC v TLSv1.2 Record Content Typ Version: Ti Length: 98 > Handshake F	ure v1 Version 4, Src: 1 Tool Protocol, Src ecurity Layer: Handshake (22) L5 1.2 (0x0303) Protocol: Server F	92.168.56.129, Dst Port: 7070, Dst Po Protocol: Server	t: 172.17.27. Dort: 43074, S Hell <mark>o</mark>	.33	Content Type: HandShake (22) Version: ISI 1.2 (0x8303) Length: 218 > HandShake Protocol: Client Hello  No. MeW - Time: Med20208 - Same IT2/2237 - Desinetion: MS-427 - Same Aut: - 4004 - Desinetion Aut: TUD - Length: 281 - Same Distribution
Linux cooked captu Internet Protocol Transmission Contr Transport Layer Se V TLSv1.2 Record Content Typ Version: Ti Length: 98 > Handshake F V TLSv1.2 Record	vre v1 Version 4, Src: 1 vol Protocol, Src ecurity Layer: Handshake (22) LS 1.2 (0x0303) Protocol: Server F Layer: Handshake	92.168.56.129, Dst Port: 7070, Dst Po Protocol: Server Hello Protocol: Certifi	t: 172.17.27. Dort: 43074, S Hell <mark>o</mark>	.33	Content Type: Tandbhake (22) Version: TS 1.2 (9x8303) Length: 218 Show packet bytes  Wireshark - Packet 14675 - CSRC 7b-and-mTLS 12, combined-itc-trace-files 06-01-23, 1100am, pcaping  Frame 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0
Linux cooked captu Internet Protocol Transport Layer So V TLSv1.2 Record Content Tyy Version: Ti Length: 98 > Handshake i V TLSv1.2 Record Content Tyj	vie v1 Version 4, Src: 1 vol Protocol, Src ceurity Layer: Handshake (22) LS 1.2 (0x0003) Protocol: Server F Layer: Handshake 0e: Handshake (22)	92.168.56.129, Dst Port: 7070, Dst Po Protocol: Server Hello Protocol: Certifi	t: 172.17.27. Dort: 43074, S Hell <mark>o</mark>	.33	Content Type: Maddhake (22) Version: IS 1.2 (0x8083) Length: 218 Version: IS 1.2 (0x8083) Length: 218 Handbake Protocol: Client Hello L. Len: 2400 Wireshark-Packet 14675 - CSRC_7b-and-mIL_SI_combined-itc-trace-files_06-01-23_1100am.pcapng Vireshark-Packet 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0 Linux coded capture v1
Linux cooked captu Internet Protocol Transmission Contr Transmission Contr Transport Layer Sc V TLSv1.2 Record Content Ty Version: Ti Length: 98 > Handshake i Content Ty Version: Ti	vie v1 Version 4, Src: 1 ool Protocol, Src ecurity Layer: Handshake (22) LS 1.2 (0x0303) Protocol: Server H Layer: Handshake (22) LS 1.2 (0x0303)	92.168.56.129, Dst Port: 7070, Dst Po Protocol: Server Hello Protocol: Certifi	t: 172.17.27. Dort: 43074, S Hell <mark>o</mark>	.33	Content Type: HandShake (22) Version: IS 1.2 (0x0303) Length: 218 Version: IS 1.2 (0x0303) Length: 218 AndShake Protocol: Client Hello  No. Hell Thre: Hell2000 Surve IX12/223 Desinder: HSUBLAS Protocol: Tokic: T
Linux cooked capt: Internet Protocol Transmission Contr Transport Layer SX v TLSV1.2 Record Content Tyy Version: Ti - Handshake t v TLSV1.2 Record Content Tyy Version: Ti Length: 18:	vie v1 Version 4, Src: 1 rol Protocol, Src ecurity Layer: H <mark>andshake (22)</mark> LS 1.2 (0x0303) Protocol: Server F Layer: Handshake (22) LS 1.2 (0x0303) L4	92.168.56.129, Dst Port: 7070, Dst Pr Protocol: Server Kello Protocol: Certifi	t: 172.17.27. Dort: 43074, S Hell <mark>o</mark>	.33	Content Type: Mandshake (22) Version: IS 1.2 (0x8393) Length: 218 Version: IS 1.2 (0x8393) Length: 218 Hendthake Protocol: Client Hello  No. Held: The: HELDEN' Same UTLIZED' Comments Field SLID: Andrea Tiskiz' Same Are: 400 - Coonseter Are: 700 - Length SU: Same Cher Are  Wireshark: Packet 14575: CSRC, 7b- and-mTL_SL combined-Hc-trace-files_06-01-23_1100arm.pcapng  Frame 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0 Linux code capture v1 Tarsmission Control Protocol, Src Part: 3007, 303, 512192.168.56,129 Transmission Control Protocol, Src Part: 3007, April 192, 1921; 5021 Port: 3007, Seg: 2487, Ack: 2452, Len: 81
Linux cooked captu Internet Protocol Transmission Contr Transport Layer SX V TLSV1.2 Record Content Ty Version: TI Length: 98 Handshake I V TLSV1.2 Record Content Ty Version: TI Length: 18 B Handshake I	vie vl Version 4, Src: 1 ol Protocol, Src scurity Layer: Handshake (22) LS 1.2 (0x0303) Protocol: Server H Layer: Handshake (22) LS 1.2 (0x0303) 44 Protocol: Certific Protocol: Certific	92.168.56.129, Dst Port: 7070, Dst Pr Protocol: Server Mello Protocol: Certifi	t: 172.17.27. prt: 43074, S Hell <mark>o</mark> cat <mark>e</mark>	.33 Seq: 1, Ack: 224	Content Type: Handshake (22) Uversion: IS 1.2 (9x8393) Length: 218 Handshake Protocol: Client Hello Length: 218 Handshake Protocol: Client Hello Re: HMM* Tmm: HMM2502: Sume HTM25223: -Deconders HEMESI2D* Andreak TIS-12* Sume Ant: 4004 - Deconders Ant: 700* Length: 201* SMm2 Offen Show packet bytes Writeshark - Packet 14675: CSRIC_7b-and-mTLS_12_combined-itc-trace-files_06-01-23_1100am.pcapng  Frame 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0 Linux cooked capture V1 Framesian Protocol Version 4, Src: 172.17.27.33, Dst: 192.168.56.129 Transmission Control Protocol, Src Port: 43074, Dst Port: 7070, Seq: 2487, Ack: 2452, Len: 81
Linux cooked capt: Internet Protocol Transmission Contr Transport Layer SC v TLSv1.2 Record Content Ty Version: Ti Length: 98 > Handshake i v TLSv1.2 Record Content Ty Version: Ti Length: 18: > Handshake i v TLSv1.2 Record	vie vl Version 4, Src: 1 ol Protocol, Src scurity Layer: Handshake (22) LS 1.2 (0x0303) Protocol: Server H Layer: Handshake (22) LS 1.2 (0x0303) 44 Protocol: Certific Protocol: Certific	92.168.56.129, DS Port: 7070, DSt Pr Protocol: Server Netlo Protocol: Certifi	t: 172.17.27. prt: 43074, S Hell <mark>o</mark> cat <mark>e</mark>	.33 Seq: 1, Ack: 224	Content Type: MandShake (22) Version: IS 1.2 (0x8383) Length: 218 Handshake Protocol: Client Hello Len: 2400 Wireshark: Packet 14575: CSRC 7b- and ImTLS12 combined-itc-trace-files_06-01-23_1100am.pcapng Vireshark: Packet 14575: CSRC 7b- and ImTLS12 combined-itc-trace-files_06-01-23_1100am.pcapng  Frame 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0 Linux code capture v1 Frame 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0 Linux code capture v1 Frame 14675: 149 bytes on Vire: 13027, 0x33, 0x51 192, 168, 056, 129 Framesision Control Protocol, Src Port: 38076, Seq: 2487, Ack: 2452, Len: 81 Transport Layer Security Tissue: Application Data Protocol. MyperText Transfer Protocol 2
Linux cooked capt: Internet Protocol Transmission Contr Transport Layer SC Content Tyy Version: TI Length: 98 > Handshake I Content Tyy Version: TI Length: 18 > Handshake I Content Tyy	yre v1 Version 4, Src: 1 rol Protocol, Src scurity Layer: Handshake (22) LS 1.2 (0x0303) Protocol: Server F Layer: Handshake (22) LS 1.2 (0x0303) L4 Protocol: Certific Cayer: Handshake	92.168.56.129, DS Port: 7070, DSt Pr Protocol: Server Netlo Protocol: Certifi	t: 172.17.27. prt: 43074, S Hell <mark>o</mark> cat <mark>e</mark>	.33 Seq: 1, Ack: 224	Content Type: Handshake (22) Version: IS 1.2 (9x393) Length: 218 Version: IS 1.2 (9x194)Version IS 1.2 (9x194)Version: IS 1.2 (9x194)Version Version: IS 1.2 (9x194)Version IS 1.2 (9x194)Version IS 1.2 (9x194)Version IS 1.2 (9x194)Version Version: IS 1.2 (9x194)Version IS 1.2 (9x194)Versio
Linux cooked capt: Internet Protocol Transmission Contr Transport Layer SC Content Tyy Version: TI Length: 98 > Handshake I Content Tyy Version: TI Length: 18 > Handshake I Content Tyy	ve v1 Version 4, Src: 1 O Protocol, Src recurity Layer: Handshake (22) S: 1.2 (0x0303) Protocol: Server H Layer: Handshake (22) S: 1.2 (0x0303) H4 Protocol: Certifi Protocol: Certifi Protocol: Certifi Cayer: Handshake Protocol: Certifi S: 1.2 (0x0303)	92.168.56.129, DS Port: 7070, DSt Pr Protocol: Server Netlo Protocol: Certifi	t: 172.17.27. prt: 43074, S Hell <mark>o</mark> cat <mark>e</mark>	.33 Seq: 1, Ack: 224	Content Type: MandShake (22) Version: IS 1.2 (0x8383) Length: 218 Handshake Protocol: Client Hello  Murebark: Packet Maris - Same Dilling - Same Maris BlackSing - Anaxon Tisl2 - Same Ann - GWV - Anaxon Ann - Anaxon Maris
Linux cooked captu Internet Protocol Transport Layer Sr V TLSVL 2. Record Content Ty Version: Ti Length: 98 > Handshake I > TLSVL 2. Record Content Ty Version: Ti Length: 18: > Handshake I > TLSVL 2. Record Content Ty Version: Ti Length: 48. > Handshake I	verion 4, Src: 1 vol.Protocol, Src: eurity Layer: Nandhake se: Handhake se: Handhake se: Handhake (22) Solowith (2000) Protocol: Server H voltake (22) Solowith (2000) Protocol: Server H voltakake Solowith (2000) Solowith (2000)	92.168.56.129, DSP Port: 7070, DSt Pr Protocol: Server Hello Protocol: Certifi ate Protocol: Server	t: 172.17.27. prt: 43074, 5 Hello cate	.33 Seq: 1, Ack: 224	Content Type: Handshake (22) Version: IS 1.2 (9x393) Length: 218 Version: IS 1.2 (9x194)Version IS 1.2 (9x194)Version: IS 1.2 (9x194)Version Version: IS 1.2 (9x194)Version IS 1.2 (9x194)Version IS 1.2 (9x194)Version IS 1.2 (9x194)Version Version: IS 1.2 (9x194)Version IS 1.2 (9x194)Versio
Linux cooked capt) Transmission Cont Transport Layer SV V TLSV1.2 Record Content Tyy Version: Ti Length: 98 > Handshake I > TLSV1.2 Record Content Tyy Version: Ti Length: 88 > Handshake I < TLSV1.2 Record Content Tyy Version: Ti Length: 40 > Handshake I > TLSV1.2 Record > TLSV1.2 Record	ve v1 Version 4, Src: 1 bol Protocol, Src scurity Layer: Handshake (22) S 1.2 (0x030) Protocol: Server H Layer: Handshake V1 Versi Handshake (22) S 1.2 (0x0303) V4 Protocol: Certific Layer: Handshake (22) S 1.2 (0x0303) V4 Protocol: Server H Protocol: Server H Protocol: Server H	92.168.56.129 of Port: 7070, Dst Pr Protocol: Server Hello Protocol: Certifi iate Protocol: Server Yey Exchange Protocol: Certifi	t: 172.17.27. prt: 43074, 5 Hello cate	.33 Seq: 1, Ack: 224	Interface unknown       Content Type: Handshake (22)         Interface unknown       Version: TS 1.2 (0x0393)         Length: 218       Handshake Protocol: Client Hello         I., Len: 2400       Handshake Protocol: Client Hello         Murchark: Packet 14075: CSBC Zbeand-mill5.g2 combined-itc-trace-files_06-01-23_1100am.pcapng       —         Version: 14075: 140 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0       Linux: Cooked capture v1         Linux: Cooked capture v1       Sinternet Protocol Version 4, Src: 172.17.27.33, 0st: 192.168.56.129       —         Transmission Control Protocol, Src Port: 43074, bst Port: 7070, Seq: 2487, Ack: 2452, Len: 81       Version: TLS 1.2 (0x0383)         Version: TLS 1.2 (0x0383)       Length: 71.2 (0x0383)
Linux cooked capty Transpirl Layer Sr V TLSVL.2 Record V tersion: T Length: 80 V TLSVL.2 Record Content Ty Version: T Length: 82 Handshake I V TLSVL.2 Record Content Ty Version: T Length: 48 Handshake I V TLSVL.2 Record Content Ty Version: T Length: 48 Handshake I Handshake I Handsh	ure v1 Version 4, Src: 1 vol Protocol, Src scurity Layer: Mandhake (22) sc: Handhake (22)	92.168.56.129 of Port: 7070, Dst Pr Protocol: Server Hello Protocol: Certifi iate Protocol: Server Yey Exchange Protocol: Certifi	t: 172.17.27. prt: 43074, 5 Hello cate	.33 Seq: 1, Ack: 224	Content Type: Handshake (22) Version: IS 1.2 (0x0303) Length: 218 Handshake Protocol: Client Hello  Wershark. Packet Mario - CRNC - Analysis - Same State Tist2 - Same Ant - GRM - Analysis - Same Content Type: Handshake Protocol: Client Hello  Wireshark. Packet Mario - CSRC 7b- and -mTLS12 combined-Hitc-trace-files (06-01-23,1100am pccapng  Vireshark. Packet Mario - CSRC 7b- and -mTLS12 combined-Hitc-trace-files (06-01-23,1100am pccapng  Frame 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0 Linux code capture V, Science - All Science - Science - CSRC 7b- and -mTLS12 - Content Type: Application Data (23) Version: Lis 1.2 (0x0303) Length: 76 Encrypted Application Data (23) Version: Tis 1.2 (0x0303) Length: 76
Linux cooked capty Internet Protocol Transport Layer Si v TLSV1.2 Record Content Tyy Version: Ti Length: 98 > Handshake I v TLSV1.2 Record Content Tyy Version: Ti Length: 88 > Handshake I v TLSV1.2 Record Content Tyy Version: Ti Length: 40 > Handshake I v TLSV1.2 Record Content Tyy Version: Ti Length: 40 > Handshake I v TLSV1.2 Record Content Tyy Version: Ti Length: 40 > Handshake I	ve v1 Version 4, Src: 1 bol Protocol, Src scurity Layer: Handshake (22) S 1.2 (0x030) Protocol: Server H Layer: Handshake V2 (0x0303) H Protocol: Certific Layer: Handshake (22) S 1.2 (0x0303) H Protocol: Server H Protocol: Server H Protocol: Server H Protocol: Server H	92.168.56.129 of Port: 7070, Dst Pr Protocol: Server Hello Protocol: Certifi iate Protocol: Server Yey Exchange Protocol: Certifi	t: 172.17.27. prt: 43074, 5 Hello cate	.33 Seq: 1, Ack: 224	Content Type: Handshake (22) Version: IS 1.2 (0x0303) Length: 218 Handshake Protocol: Client Hello  Wershark. Packet Mario - CRNC - Analysis - Same State Tist2 - Same Ant - GRM - Analysis - Same Content Type: Handshake Protocol: Client Hello  Wireshark. Packet Mario - CSRC 7b- and -mTLS12 combined-Hitc-trace-files (06-01-23,1100am pccapng  Vireshark. Packet Mario - CSRC 7b- and -mTLS12 combined-Hitc-trace-files (06-01-23,1100am pccapng  Frame 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0 Linux code capture V, Science - All Science - Science - CSRC 7b- and -mTLS12 - Content Type: Application Data (23) Version: Lis 1.2 (0x0303) Length: 76 Encrypted Application Data (23) Version: Tis 1.2 (0x0303) Length: 76
Linux cooked capty Internet Protocol Transport Layer Sr V TLSVL.2 Record Version: T Version: T Length: 98 Version: T Length: 28 Version: T Length: 28 Version: T Length: 28 Version: T Length: 28 Handshake I VSVL.2 Record Content Tyy Version: T Length: 48 Handshake I Version: T Length: 58	ure v1 Version 4, Src: 1 tol Protocol, Src scurity Layer: Mandhake (22) S 1.2 (0x0303) Protocol: Server H Layer: Jandhake (22) S 1.2 (0x0303) Versi Handshake (22) S 1.2 (0x0303) Layer: Handshake S 1.4 (0x0303) Layer: Handshake S 1.2 (0x0303) Layer: Handshake (22) S 1.2 (0x0303)	92.168.56.129, DSP Port: 7070, DST PU Protocol: Server iello Protocol: Certifi ate Protocol: Server Protocol: Certifi	t: 172.17.27. prt: 43074, 5 Hello cate	.33 Seq: 1, Ack: 224	Content Type: MandShake (22) Version: IS 1.2 (0x8383) Length: 218 Version: IS 1.2 (0x8383) Length: 26 Version: IS 1.2 (0x
Linux cooked captu Internet Protocol Transport Layer Si v TLSV1.2 Record Content Ty Version: Ti Length: 98 > Handshake I v TLSV1.2 Record Content Ty Version: Ti Length: 88 > Handshake I v TLSV1.2 Record Content Yy Version: Ti Length: 48 > Handshake I v TLSV1.2 Record Content Ty Version: Ti Length: 48 > Handshake I	ve v1 Version 4, Src: 1 tool Protocol, Src security Layer: Handshake (22) S 1.2 (0x030) Protocol: Server H Layer: Handshake (22) S 1.2 (0x030) 44 Protocol: Certifike Layer: Handshake (22) S 1.2 (0x030) 1 Protocol: Server H Layer: Handshake (22) S 1.2 (0x030) 1 Protocol: Server H Layer: Handshake (22) S 1.2 (0x030) 1 Protocol: Server H Layer: Handshake (22) S 1.2 (0x030) Protocol: Certifike	92.168.56.129 OS Port: 7070, DST PU Protocol: Server Hello Protocol: Certifi Late Protocol: Server Ley Exchange Protocol: Certifi Late Request	rt: 172.17.27. rt: 172.17.27 rt: 43074, 5 Hello cate Cate Key Exchange	.33 Seq: 1, Ack: 224	Content Type: Handshake (22) Version: IS 1.2 (0x0303) Length: 218 Handshake Protocol: Client Hello  Wershark. Packet Mario - CRNC - Analysis - Same State Tist2 - Same Ant - GRM - Analysis - Same Content Type: Handshake Protocol: Client Hello  Wireshark. Packet Mario - CSRC 7b- and -mTLS12 combined-Hitc-trace-files (06-01-23,1100am pccapng  Vireshark. Packet Mario - CSRC 7b- and -mTLS12 combined-Hitc-trace-files (06-01-23,1100am pccapng  Frame 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0 Linux code capture V, Science - All Science - Science - CSRC 7b- and -mTLS12 - Content Type: Application Data (23) Version: Lis 1.2 (0x0303) Length: 76 Encrypted Application Data (23) Version: Tis 1.2 (0x0303) Length: 76
Linux cooked capty Transport Layer Sr V TLSVL.2 Record Content Jy Version: T Length: 98 > Handshake V TLSVL.2 Record Content Jy Version: T Length: 84 > Handshake V TLSVL.2 Record Content Ty Version: T Length: 84 > Handshake V TLSVL.2 Record Content Ty Version: T Length: 84 > Handshake Handshake > Handshake V TLSVL.2 Record Content Ty Version: T Length: 85 > Handshake V TLSVL.2 Record Content Ty Version: T Length: 85 > Handshake V TLSVL.2 Record Version: T	ure v1 Version 4, Src: 1 tol Protocol, Src scurity Layer: Nandshake (22) S 1.2 (0x0303) Protocol: Server H Layer: Jandshake (22) S 1.2 (0x0303) Vertocol: Certific Vertocol: Certific Layer: Handshake S 1.2 (0x0303) L Layer: Handshake (22) S 1.2 (0x0303) L Layer: Handshake (22) S 1.2 (0x0303) L Layer: Handshake (22) S 1.2 (0x0303) Protocol: Certific Layer: Handshake (22) S 1.2 (0x0303)	22.168.56.129, DSP Port: 7070, DST PU Protocol: Server iello Protocol: Certifi ate Protocol: Server rey Exchange Protocol: Certifi ate Request Protocol: Server	rt: 172.17.27. rt: 172.17.27 rt: 43074, 5 Hello cate Cate Key Exchange	.33 Seq: 1, Ack: 224	Content Type: Handshake (22) Version: IS 1.2 (0x0303) Length: 218 Handshake Protocol: Client Hello  Wershark. Packet Mario - CRNC - Analysis - Same State Tist2 - Same Ant - GRM - Analysis - Same Content Type: Handshake Protocol: Client Hello  Wireshark. Packet Mario - CSRC 7b- and -mTLS12 combined-Hitc-trace-files (06-01-23,1100am pccapng  Vireshark. Packet Mario - CSRC 7b- and -mTLS12 combined-Hitc-trace-files (06-01-23,1100am pccapng  Frame 14675: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface unknown, id 0 Linux code capture V, Science - All Science - Science - CSRC 7b- and -mTLS12 - Content Type: Application Data (23) Version: Lis 1.2 (0x0303) Length: 76 Encrypted Application Data (23) Version: Tis 1.2 (0x0303) Length: 76
Linux cooked capty Internet Protocol Transport Layer Si v TLSV.12 Record Content Tyy Version: Ti Length: 98 > Handshake 1 v TLSV.12 Record Content Tyy Version: Ti Length: 98 > Handshake 1 v TLSV.12 Record Content Tyy Version: Ti Length: 48 > Handshake 1 v TLSV.12 Record Content Tyy Version: Ti Length: 48 > Handshake 1 v TLSV.12 Record Content Tyy Version: Ti Length: 48 > Handshake 1 v TLSV.12 Record Content Tyy	ve v1 Version 4, Src: 1 tool Protocol, Src security Layer: Handshake (22) S 1.2 (0x030) Protocol: Server H Layer: Handshake (22) S 1.2 (0x030) 44 Protocol: Certifike Layer: Handshake (22) S 1.2 (0x030) 1 Protocol: Server H Layer: Handshake (22) S 1.2 (0x030) 1 Protocol: Server H Layer: Handshake (22) S 1.2 (0x030) 1 Protocol: Server H Layer: Handshake (22) S 1.2 (0x030) Protocol: Certifike	22.168.56.129, DSP Port: 7070, DST PU Protocol: Server iello Protocol: Certifi ate Protocol: Server rey Exchange Protocol: Certifi ate Request Protocol: Server	rt: 172.17.27. rt: 172.17.27 rt: 43074, 5 Hello cate Cate Key Exchange	.33 Seq: 1, Ack: 224	Content Type: MandShake (22) Version: IS 1.2 (0x8383) Length: 218 Version: IS 1.2 (0x8383) Length: 26 Version: IS 1.2 (0x
Linux conked captu Transport Layer Si v TLSV.12 Record v TLSV.12 Record v TLSV.12 Record Content Tyy version: Ti Length: 88 > Handshake I v TLSV.12 Record Content Tyy Version: Ti Length: 84 > Handshake I v TLSV.12 Record Content Tyy Version: Ti Length: 84 > Handshake I v TLSV.12 Record Content Tyy Version: Ti Length: 84 > Handshake I v TLSV.12 Record Content Tyy	verion 4, Srci 1 Version 4, Srci 1 Layer: Handshake 2: Layer: Handshake 2: Handshake (22) Srotcol: Server H Layer: Handshake 2: Handshake (22) Si 1: 2 (0x0303) 4 Protocol: Certific Layer: Handshake 2: Layer: Handshake 2: Layer: Handshake 2: Layer: Handshake 2: Si 1: 2 (0x0303) Protocol: Server H Layer: Handshake 2: Handshake (22) Si 1: 2 (0x0303) Protocol: Certific Layer: Handshake (22) Si 1: 2 (0x0303)	22.168.56.129, DSP Port: 7070, DST PU Protocol: Server iello Protocol: Certifi ate Protocol: Server rey Exchange Protocol: Certifi ate Request Protocol: Server	rt: 172.17.27. rt: 172.17.27 rt: 43074, 5 Hello cate Cate Key Exchange	.33 Seq: 1, Ack: 224	Content Type: Handshake (22) Version: IS 1.2 (0x8383) Length: 218 Version: IS 1.2 (0x8383) Version: IS 1.2 (0
Linux cooked capt) Transport Layer Si v TISV1.2 Record v TISV1.2 Record Content Tyy Version: Ti Length: 98 Handshake I v TISV1.2 Record Content Tyy Version: Ti Length: 88 Handshake I v TISV1.2 Record Content Tyy Version: Ti Length: 48 Handshake I v TISV1.2 Record Content Tyy Version: Ti Length: 48 Handshake I v TISV1.2 Record Content Tyy Version: Ti Length: 48 Handshake I v TISV1.2 Record Content Tyy Version: Ti Length: 44	verian 4, Src: 1 vol. Protocol, Src: curity Layer: Nandhake (22) Se: Handhake (22) Se: Se: Se: Se: Se: Se: Se: Se: Se: Se:	92.168.56.129, DS Port: 7070, DSt PC Protocol: Server Iello Protocol: Certifi .ate Protocol: Server Protocol: Certifi .ate Request Protocol: Server	rt: 172.17.27. rt: 172.17.27 rt: 43074, 5 Hello cate Cate Key Exchange	.33 Seq: 1, Ack: 224	Content Type: Handshake (22) Version: IS 1.2 (0x8383) Length: 218 Version: IS 1.2 (0x8383) Version: IS 1.2 (0

Figure 10 : mTLS handshake between SNF and NRF

CSRIC\_7b-and-mTLS\_t2\_combined-itc-trace-files\_06-01-23\_1100am.pcapng

63539 6003.566028       172.17.95.197       192.168.56.137       TCP       4312       443       56.43112 - 443       [ST] Seq=6615 Win+0 Len+0         60197 6961.113100       172.17.27.33       192.168.56.137       TLSV1.2       43066       443       114 Application Data         69202 6961.245623       172.17.95.197       192.168.56.137       TLSV1.2       43111       443       68 43966 + 443       [ACK] Seq=5688 Ack=10811 Win=224 Len+0 TSval=3350012094 TSecr=36         69717 6921.14111       172.17.7.95.197       192.168.56.137       TLSV1.2       43114       443       114 Application Data         69753 7021.14268       172.17.7.95.197       192.168.56.137       TLSV1.2       43111       443       68 43066 + 443       [ACK] Seq=988 Ack=10811 Win=224 Len+0 TSval=3350012094 TSecr=36         69754 7021.14668       172.17.7.95.197       192.168.56.137       TLSV1.2       43111       443       [ACK] Seq=9804 Ack=10857 Win=234 Len+0 TSval=3350072095 TSecr=36         70335 7081.115149       172.17.7.33       192.168.56.137       TLSV1.2       4306       443       114 Application Data         70335 7081.115149       172.17.27.33       192.168.56.137       TLSV1.2       4306       443       68 43086 + 443       [ACK] Seq=9722 Ack=582 Win=239 Len+0 TSval=3350072095 TSecr=36         70335 7081.115149       172.17.27.33	Time		Source	Destination	Protocol	Source	Destinat L	angth Info
65590       6903.566028       172.17.95.197       192.168.56.137       TCP       43112       443       556 43112       443       144 Application Date         6919       6961.113100       172.17.27.33       192.168.56.137       TCP       43086       443       114 Application Date         69208       6961.24523       172.17.27.33       192.168.56.137       TCP       43086       443       64 33086 + 443       [ACK] Seq=5608 Ack=5780 Win=239 Len=0 TSval=307220545 TSecr=2691         69208       6961.245623       172.17.27.33       192.168.56.137       TCV       43111       443       66 43086 + 443       [ACK] Seq=5626 Ack=5826 Win=239 Len=0 TSval=3350012094 TSecr=36         69755       7021.114211       172.17.27.33       192.168.56.137       TLSv1.2       43111       443       164 Application Data         69755       7021.46618       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       164 A3086 + 443       [ACK] Seq=9384 Ack=10857 Win=224 Len=0 TSval=3350072095 TSecr=36         70335       7081.115209       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       164 A3086 + 443       [ACK] Seq=9384 Ack=10857 Win=224 Len=0 TSval=3350072095 TSecr=36         70335       7081.115209       172.17.95.197       192.168.56.137       TLSv1.2	68587 690	3.565816	172.17.95.197	192.168.56.137	TLSv1.2	43112	443	99 Encrypted Alert
9197 6961.113100       172.17.27.33       192.166.56.137       TLSV.2       43086       443       164 Application Data         9199 6961.113252       172.17.27.33       192.166.56.137       TLSV.2       43101       443       164 Application Data         9202 6961.24563       172.17.7.55.197       192.166.56.137       TLSV.2       43111       443       164 Application Data         9202 6961.245608       172.17.7.53.19       192.166.56.137       TLSV.2       43101       443       164 Application Data         9751 7021.114268       172.17.7.53.19       192.166.56.137       TLSV.1.2       43101       443       164 Application Data         9755 7021.24618       172.17.7.51.97       192.166.56.137       TLSV.1.2       43111       443       164 Application Data         9755 7021.46618       172.17.7.51.97       192.166.56.137       TLSV.1.2       43111       443       164 Application Data         9756 7021.46618       172.17.7.51.97       192.166.56.137       TLSV.1.2       43111       443       114 Application Data         9137 7081.115149       172.17.95.197       192.166.56.137       TLSV.1.2       43111       443       164 Application Data         9147 741.16622       172.17.95.197       192.166.56.137       TLSV.1.2       43111 <t< th=""><th>8588 690</th><th>3.565949</th><th>172.17.95.197</th><th>192.168.56.137</th><th>TCP</th><th>43112</th><th>443</th><th>68 43112 → 443 [FIN, ACK] Seq=6615 Ack=5574 Win=239 Len=0 TSval=3349954415 TSecr=3696</th></t<>	8588 690	3.565949	172.17.95.197	192.168.56.137	TCP	43112	443	68 43112 → 443 [FIN, ACK] Seq=6615 Ack=5574 Win=239 Len=0 TSval=3349954415 TSecr=3696
9499 6961.113252 172.17.27.33 192.168.56.137 TCP 43086 443 6643065 + 443 [ACK] Seq=5680 Ack=5780 Win=239 Len=0 TSval=307220545 TSecr=2691 1920 6961.245620 172.17.95.197 192.168.56.137 TLSV1.2 43111 443 144 Application Data 922 6961.245620 172.17.95.197 192.168.56.137 TLSV1.2 43086 443 6643065 + 443 [ACK] Seq=9888 Ack=10611 Win=224 Len=0 TSval=3350012094 TSecr=36 9757 7021.14111 172.17.27.33 192.168.56.137 TLSV1.2 43086 443 14 Application Data 9755 7021.14261 172.17.27.33 192.168.56.137 TLSV1.2 43111 443 164 543164 543164 CK] Seq=5726 Ack=5826 Win=239 Len=0 TSval=3350072095 TSecr=36 9757 7021.246609 172.17.95.197 192.168.56.137 TLSV1.2 43086 443 114 Application Data 9756 7021.246609 172.17.95.197 192.168.56.137 TLSV1.2 43086 443 114 Application Data 9757 572.17.17.95.197 192.168.56.137 TLSV1.2 43086 443 114 Application Data 9756 7021.246609 172.17.95.197 192.168.56.137 TLSV1.2 43086 443 643101 + 443 [ACK] Seq=9034 Ack=10857 Win=224 Len=0 TSval=305072095 TSecr=36 9337 081.11549 172.17.27.33 192.168.56.137 TLSV1.2 43086 443 114 Application Data 9756 7021.7.95.197 192.168.56.137 TLSV1.2 43111 443 144 Application Data 97404547 Tsecr=2691 9337 081.14575 172.17.95.197 192.168.56.137 TLSV1.2 43111 443 144 Application Data 97404547 Tsecr=2691 9442 7141.16227 172.17.27.33 192.168.56.137 TLSV1.2 43111 443 64 3111 + 443 [ACK] Seq=9080 Ack=1093 Win=224 Len=0 TSval=3350132096 TSecr=36 9447 141.1627 172.17.27.33 192.168.56.137 TLSV1.2 43086 443 66 43306 + 443 [ACK] Seq=5818 Ack=5918 Win=239 Len=0 TSval=3350132096 TSecr=36 9447 141.1627 172.17.27.33 192.168.56.137 TLSV1.2 43086 443 64 4366 + 443 [ACK] Seq=5818 Ack=5918 Win=239 Len=0 TSval=3350132096 TSecr=2691 1528 7201.1706 172.17.27.33 192.168.56.137 TLSV1.2 43086 443 64 4306 + 443 [ACK] Seq=5814 Ack=5964 Win=239 Len=0 TSval=3350132097 TSecr=369 1137 APP 143.44554 172.17.95.197 192.168.56.137 TLSV1.2 43086 443 64 43086 + 443 [ACK] Seq=5816 Ack=5964 Win=239 Len=0 TSval=335012097 TSecr=369 11528 7201.1706 172.17.27.33 192.168.56.137 TLSV1.2 43086 443 64 43086 + 443 [ACK] Seq=5	8590 690	3.566028	172.17.95.197	192.168.56.137	тср	43112	443	56 43112 → 443 [RST] Seq=6615 Win=0 Len=0
9200 6961.245623 172.17.95.197 192.168.56.137 TLSV1.2 43111 443 114 Application bata 9200 6961.245623 172.17.95.197 192.168.56.137 TLSV1.2 43111 443 64 3111 + 443 [ACK] Seq=8988 Ack=10811 Win=224 Len=0 TSval=3350012094 TSecr=36 9753 7021.114268 172.17.75.137 192.168.56.137 TLSV1.2 43086 443 64 3086 + 443 [ACK] Seq=9034 Ack=10857 Win=239 Len=0 TSval=3350012094 TSecr=36 9754 7021.246689 172.17.95.197 192.168.56.137 TLSV1.2 43111 443 64 3111 + 443 [ACK] Seq=9034 Ack=10857 Win=224 Len=0 TSval=335002095 TSecr=36 9755 7021.246689 172.17.95.197 192.168.56.137 TLSV1.2 43111 443 66 43111 + 443 [ACK] Seq=9034 Ack=10857 Win=224 Len=0 TSval=3350072095 TSecr=36 9335 7081.15199 172.17.75.33 192.168.56.137 TLSV1.2 43086 443 66 43086 + 443 [ACK] Seq=5722 Ack=5872 Win=239 Len=0 TSval=3350972095 TSecr=36 9337 7081.15199 172.17.73.3 192.168.56.137 TLSV1.2 43086 443 66 43086 + 443 [ACK] Seq=9084 Ack=10893 Win=224 Len=0 TSval=3350132096 TSecr=36 9340 7081.24775 172.17.95.197 192.168.56.137 TLSV1.2 43111 443 64 3111 + 443 [ACK] Seq=9088 Ack=10903 Win=224 Len=0 TSval=3350132096 TSecr=36 9447 7141.16227 172.17.733 192.168.56.137 TLSV1.2 43111 443 66 43111 + 443 [ACK] Seq=9188 Ack=5918 Win=239 Len=0 TSval=3350132096 TSecr=36 9447 7141.16227 172.17.733 192.168.56.137 TLSV1.2 43111 443 66 43111 + 443 [ACK] Seq=9188 Ack=5918 Win=239 Len=0 TSval=3350132096 TSecr=36 1528 7201.17096 172.17.75.197 192.168.56.137 TLSV1.2 43111 443 66 43111 + 443 [ACK] Seq=9126 Ack=5918 Win=239 Len=0 TSval=3350132097 TSecr=36 1528 7201.17096 172.17.75.197 192.168.56.137 TLSV1.2 43111 443 68 43111 + 443 [ACK] Seq=9126 Ack=5918 Win=239 Len=0 TSval=335012097 TSecr=36 1528 7201.17096 172.17.75.31 192.168.56.137 TLSV1.2 43111 443 68 43111 + 443 [ACK] Seq=9126 Ack=5964 Win=239 Len=0 TSval=3350122097 TSecr=36 1528 7201.17096 172.17.75.197 192.168.56.137 TLSV1.2 43111 443 68 43111 + 443 [ACK] Seq=9128 Ack=504 Win=239 Len=0 TSval=3350522098 TSecr=36 1533 7201.249777 172.17.55.197 192.168.56.137 TLSV1.2 43111 443 68 43111 + 443 [ACK] Seq=9128 Ack=604 Win=23				192.168.56.137				
9202 6961.245808 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 + 443 [ACK] Seq=8988 Ack=18811 Win=224 Len=0 TSval=3350012094 TSecr=36 9751 7021.114111 172.17.27.33 192.168.56.137 TC.97 43086 443 164 Application Data 9754 7021.24618 172.17.27.33 192.168.56.137 TC.97 43086 443 164 Application Data 9756 7021.24618 172.17.95.197 192.168.56.137 TC.97 43111 443 164 Application Data 9756 7021.24618 172.17.95.197 192.168.56.137 TC.97 43111 443 164 Application Data 937 7081.115149 172.17.27.33 192.168.56.137 TC.97 43086 443 114 Application Data 937 7081.115149 172.17.27.33 192.168.56.137 TC.97 43086 443 114 Application Data 938 7081.24755 172.17.95.197 192.168.56.137 TC.97 43086 443 114 Application Data 9387 081.24775 172.17.95.197 192.168.56.137 TC.97 43011 443 164 3111 443 [ACK] Seq=9080 Ack=10053 Win=224 Len=0 TSval=307340547 TSecr=2691 9387 081.24775 172.17.95.197 192.168.56.137 TC.97 43011 443 64 3111 + 443 [ACK] Seq=9080 Ack=10093 Win=224 Len=0 TSval=3350132096 TSecr=36 944 7141.1622 172.17.7.33 192.168.56.137 TC.97 43014 443 64 4316 4A3 [ACK] Seq=9126 Ack=10949 Win=224 Len=0 TSval=3350132096 TSecr=36 944 7141.24544 172.17.95.197 192.168.56.137 TC.97 43011 443 64 3101 4Application Data 944 7141.1622 172.17.27.33 192.168.56.137 TC.97 43014 443 114 Application Data 944 7141.1622 172.17.27.33 192.168.56.137 TC.97 43014 443 64 3086 + 443 [ACK] Seq=9126 Ack=10949 Win=224 Len=0 TSval=3350132096 TSecr=36 1528 7201.11706 172.17.27.33 192.168.56.137 TC.97 43011 443 164 Application Data 944 7141.24544 172.17.95.197 192.168.56.137 TC.97 43011 443 114 Application Data 944 7141.24544 172.17.95.197 192.168.56.137 TC.97 43014 443 144 Application Data 945 7141.246544 172.17.73.3 192.168.56.137 TC.97 43014 443 144 Application Data 946 7314.246544 172.17.95.197 192.168.56.137 TC.97 43086 443 64 43086 + 443 [ACK] Seq=9126 Ack=10949 Win=224 Len=0 TSval=3350426098 TSecr=2691 1531 7201.24077 172.17.95.197 192.168.56.137 TC.97 43014 443 144 Application Data 1537 7201.17615 172.17.73.3 192.168.56.137 TC.97 43014 443 64 33086 + 443								68 43086 → 443 [ACK] Seq=5680 Ack=5780 Win=239 Len=0 TSval=307220545 TSecr=2691134616
9751       921.114111       172.17.27.33       192.168.56.137       TLSV1.2       43086       443       114 Application Data         9753       7021.114268       172.17.27.33       192.168.56.137       TLSV1.2       43086       443       164 Application Data         9753       7021.142688       172.17.95.197       192.168.56.137       TLSV1.2       43111       443       164 Application Data         9756       7021.246609       172.17.27.33       192.168.56.137       TLSV1.2       43111       443       64 3111 + 443       [ACK] Seq=9034 Ack=10857 Win=224 Len=0 TSval=3350072095 TSecr=36         9357       7021.17.27.33       192.168.56.137       TLSV1.2       43111       443       64 43166 + 443       [ACK] Seq=9080 Ack=10903 Win=224 Len=0 TSval=3350072095 TSecr=36         9357       172.17.27.33       192.168.56.137       TLSV1.2       43111       443       66 43166 + 443       [ACK] Seq=9080 Ack=10903 Win=224 Len=0 TSval=3350132096 TSecr=36         9447       174.11662       172.17.7.73       192.168.56.137       TLSV1.2       43086       443       164 Application Data         9447       174.11662       172.17.95.197       192.168.56.137       TLSV1.2       43086       443       164 Application Data         9447       174.11662       172.17.95.197				192.168.56.137				
9753 7021.114268       172.17.27.33       192.168.56.137       TCP       43086       443       68 43086 + 443       [ACK] Seq=5726 Ack=5826 Win=239 Lene® TSval=307280546 TSecr=2691         9754 7021.24618       172.17.95.197       192.168.56.137       TCP       43081       443       144 Application Data         9756 7021.24608       172.17.95.197       192.168.56.137       TCP       43111       443       144 Application Data         9335 7061.11519       172.17.27.33       192.168.56.137       TCP       43086       443       164 Application Data         9337 7081.11519       172.17.27.33       192.168.56.137       TCP       43111       443       144 Application Data         9338 7081.247575       172.17.95.197       192.168.56.137       TCP       43111       443       164 X3966 + 443       [ACK] Seq=9038 Ack=10903 Win=224 Lene® Tsval=3350132096 Tsecr=36         9348 7081.247575       172.17.95.197       192.168.56.137       TCP       43111       443       164 X3966 + 443       [ACK] Seq=9048 Ack=10903 Win=224 Lene® Tsval=3350132096 Tsecr=36         9447 141.16227       172.17.75.197       192.168.56.137       TCP       43111       443       164 X3966 + 443       [ACK] Seq=9126 Ack=10903 Win=224 Lene® Tsval=3350132096 Tsecr=36         1528 7201.12706       172.17.75.197       192.168.56.137								68 43111 → 443 [ACK] Seq=8988 Ack=10811 Win=224 Len=0 TSval=3350012094 TSecr=36968595
9754 7021.246618       172.17.95.197       192.168.56.137       TLSV.2       43111       443       114 Application bata         9756 7021.246609       172.17.95.197       192.168.56.137       TLSV.2       43111       443       64 43111 + 443       [ACK] Seq=9034 Ack=10857 Win=224 Len=0 Tsval=3350972095 Tsecr=36         9355 7081.11539       172.17.27.33       192.168.56.137       TLSV.1.2       43086       443       64 43066 + 443       [ACK] Seq=9727 Ack=5872 Win=239 Len=0 Tsval=30507340547 Tsecr=36         9387 7081.17539       172.17.27.33       192.168.56.137       TLSV.1.2       43086       443       114 Application Data         9387 7081.17575       172.17.95.197       192.168.56.137       TLSV.1.2       43111       443       164 43plication Data         9394 7141.1662       172.17.27.33       192.168.56.137       TLSV.1.2       43086       443       164 43plication Data         9447 7141.11622       172.17.27.33       192.168.56.137       TLSV.1.2       43086       443       164 43plication Data         9448 7141.248544       172.17.95.197       192.168.56.137       TLSV.1.2       43086       443       164 43plication Data         9448 7141.248544       172.17.95.197       192.168.56.137       TLSV.1.2       43086       443       164 43086 + 443       [ACK] Seq=9126								
9755 7021.246809       172.17.95.197       192.168.56.137       TCP       43111       443       68 43111 + 443       ACK       Seq=9034 Ack=10857 Win=224 Len=0 Tsval=3350072095 Tsecr=36         9355 7081.15149       172.17.27.33       192.168.56.137       TCP       43086       443       114 Application Data         9335 7081.15199       172.17.27.33       192.168.56.137       TCP       43086       443       66 43014 Application Data         9338 7081.15199       172.17.27.33       192.168.56.137       TCSV.1.2       43111       443       66 43114.743       ACK   Seq=5772 Ack=5872 Win=239 Len=0 Tsval=3350132096 Tsecr=36         9340 7081.247755       172.17.95.197       192.168.56.137       TCSV.1.2       43111       443       66 43114.7443       ACK   Seq=9080 Ack=10903 Win=224 Len=0 Tsval=3350132096 Tsecr=36         944 741.1627       172.17.27.33       192.168.56.137       TCSV.1.2       43086       443       114 Application Data         944 741.1627       172.17.27.33       192.168.56.137       TCSV.1.2       43111       443       64 33111 + 443       ACK   Seq=5818 Ack=5918 Win=239 Len=0 Tsval=3350132096 Tsecr=36         944 741.148474       172.17.95.197       192.168.56.137       TCSV.1.2       43111       443       64 33111 + 443       ACK   Seq=5864 Ack=5964 Win=239 Len=0 Tsval=3350192097 Tsecr=36      <								
3335 7081.115149       172.17.27.33       192.168.56.137       TLSV.2       43086       443       114 Application Data         3337 7081.115309       172.17.27.33       192.168.56.137       TLSV.2       43086       443       64 3086 + 443       [ACK] Seq=5772 Ack=5872 Win=239 Len=0 TSval=307340547 TSecr=2691         3338 7081.247575       172.17.7.33       192.168.56.137       TLSV.2       43111       443       114 Application Data         3240 7081.247575       172.17.7.33       192.168.56.137       TLSV.1.2       43181       443       [ACK] Seq=9080 Ack=10903 Win=224 Len=0 TSval=3350132096 TSecr=36         9242 7141.16622       172.17.7.33       192.168.56.137       TLSV.1.2       43184       443       [ACK] Seq=9080 Ack=10903 Win=224 Len=0 TSval=3350132096 TSecr=36         9244 7141.16227       172.17.27.33       192.168.56.137       TLSV.1.2       43184       443       [AcK] Seq=9126 Ack=10949 Win=224 Len=0 TSval=3350132096 TSecr=2691         9244 7141.16227       172.17.95.197       192.168.56.137       TCP       43114 4pplication Data       64 3114 4pplication Data         9346 7141.24854       172.17.73.3       192.168.56.137       TCP       43184       443       144 Application Data         1538 720.11706       172.17.73.3       192.168.56.137       TLSV.1.2       43184       426 K43       54								
3337 7081.115309       172.17.27.33       192.168.56.137       TCP       43086       443       66 43086 + 443       [ACK] Seq=5772 Ack=5872 Win=239 Len=0 TSval=307340547 TSecr=2691         3338 7081.247575       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       164 Application Data         3340 7081.247750       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       164 Application Data         3944 7141.11662       172.17.73.3       192.168.56.137       TCP       43111       443       66 4316K.1 Seq=9680 Ack=10903 Win=224 Len=0 TSval=3350132096 TSecr=36         9944 7141.11662       172.17.73.3       192.168.56.137       TCP       43086       443       66 43086 + 443 [ACK] Seq=9126 Ack=518 Win=239 Len=0 TSval=3350132096 TSecr=36         9944 7141.1662       172.17.95.197       192.168.56.137       TCP       43111       443       66 43086 + 443 [ACK] Seq=9126 Ack=5018 Win=239 Len=0 TSval=335012097 TSecr=36         1528 7201.117096       172.17.73.3       192.168.56.137       TLSv1.2       43086       443       114 Application Data         948 7141.248544       172.17.73.3       192.168.56.137       TLSv1.2       43086       443       164 43086 + 443       [ACK] Seq=9126 Ack=10949 Win=224 Len=0 TSval=335012097 TSecr=36         1528 7201.117056       172.17.73.3       192								
3333 7081.247575       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       114 Application bata         3340 7081.247575       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       64 3111 + 443       [ACK] Seq=9080 Ack=10903 Win=224 Len=0 TSval=3350132096 TSecr=36         9342 7141.16020       172.17.7.33       192.168.56.137       TLSv1.2       43086       443       114 Application Data         9944 7141.16027       172.17.7.51.97       192.168.56.137       TLCv       43086       443       164 3086 + 443       [ACK] Seq=9126 Ack=10903 Win=224 Len=0 TSval=3350132096 TSecr=36         9944 7141.16027       172.17.75.197       192.168.56.137       TLSv1.2       43011       443       164 XJB1c+403       [ACK] Seq=9126 Ack=10949 Win=224 Len=0 TSval=3350132097 TSecr=36         9945 7141.248736       172.17.75.197       192.168.56.137       TLSv1.2       43086       443       164 Application Data         1528 7201.11206       172.17.7.73.3       192.168.56.137       TLSv1.2       43086       443       164 Application Data         1538 7201.1206       172.17.7.31       192.168.56.137       TLSv1.2       43086       443       164 A3111 + 443       Ack] Seq=9122 Ack=5064 Win=239 Len=0 TSval=3350520898 TSecr=2691         1538 7201.120977       172.17.95.197 <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>								
3349 7081,247750       172,17,95,197       192,168,56,137       TCP       43111       443       66 43111       +443       [AK] Seq=9080 Ack=10903 Win=224 Len=0 Tsval=3350132096 TSecr=36         3942 7141,11662       172,17,27,33       192,168,56,137       TCP       43086       443       114 Application Data         3944 7141,116227       172,17,27,33       192,168,56,137       TCP       43086       443       164 Application Data         9944 7141,10227       172,17,27,33       192,168,56,137       TCP       43086       443       66 43086 + 443 [ACK] Seq=9126 Ack=10949 Win=23 Len=0 TSval=335012097 TSecr=36         9946 7141,24854       172,17,27,33       192,168,56,137       TCP       43111       443       164 Application Data         9946 7141,24854       172,17,27,33       192,168,56,137       TCP       43111       443       164 Application Data         1528 7201,117266       172,17,27,33       192,168,56,137       TCP       43086       443       164 Application Data         1531 7201,249601       172,17,95,197       192,168,56,137       TCP       43011       443       164 S1024       124,2717       412,24 Len=0 TSval=3350252098 TSecr=36         1531 7201,249777       172,17,95,197       192,168,56,137       TCP       43011       443       144 Application Data <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>								
9942 7141.116022       172.17.27.33       192.168.56.137       TLSV.1.2       43086       443       114 Application Data         9944 7141.116227       172.17.27.33       192.168.56.137       TLSV.1.2       43086       443       114 Application Data         9944 7141.14627       172.17.75.137       192.168.56.137       TLSV.1.2       43111       443       164 43086 + 443       [ACK] Seq=5818 Ack=5918 Win=239 Len=0 TSval=307400548 TSecr=2691         9946 7141.248544       172.17.75.197       192.168.56.137       TLSV.1.2       43111       443       164 43086 + 443       [ACK] Seq=5816 Ack=5918 Win=239 Len=0 TSval=3350192097 TSecr=36         1528 7201.117266       172.17.27.33       192.168.56.137       TLSV.1.2       43086       443       114 Application Data         1530 7201.117266       172.17.27.33       192.168.56.137       TLSV.1.2       43086       443       164 43086 + 443       [ACK] Seq=5864 Ack=5964 Win=239 Len=0 TSval=335012097 TSecr=2691         1531 701.249601       172.17.27.33       192.168.56.137       TLSV.1.2       43086       443       164 Application Data         1531 701.24977       172.17.95.197       192.168.56.137       TLSV.1.2       43086       443       164 Application Data         1727 7261.18326       172.17.27.33       192.168.56.137       TLSV.1.2       43086 </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>								
9944 7141.116227 172.17.27.33 192.168.56.137 TCP 43086 443 68 43086 → 443 [ACK] Seq=5818 Ack=5918 Win=239 Lene0 TSval=307400548 TSecr=2691 9946 7141.248736 172.17.95.197 192.168.56.137 TCP 43111 443 144 Application Data 9947 7141.248736 172.17.733 192.168.56.137 TCP 43111 443 68 43114 + 443 [ACK] Seq=9126 Ack=10949 Win=224 Lene0 TSval=3350192097 TSecr=36 1528 720.11706 172.17.27.33 192.168.56.137 TCP 43181 443 68 43086 + 443 [ACK] Seq=9126 Ack=5964 Win=239 Lene0 TSval=3350192097 TSecr=36 1530 720.11726 172.17.73.3 192.168.56.137 TCP 43181 443 68 43086 + 443 [ACK] Seq=9126 Ack=5964 Win=239 Lene0 TSval=336052097 TSecr=2691 1531 7201.249601 172.17.95.197 192.168.56.137 TCP 43111 443 114 Application Data 1533 7201.249777 172.17.95.197 192.168.56.137 TCP 43111 443 114 Application Data 1717 7261.118326 172.17.7.33 192.168.56.137 TCP 43111 443 114 Application Data 1717 7261.118326 172.17.7.33 192.168.56.137 TCP 43111 443 114 Application Data 1717 7261.118326 172.17.7.13 192.168.56.137 TCP 43111 443 114 Application Data 1717 7261.118326 172.17.7.13 192.168.56.137 TCP 43111 443 68 43086 + 443 [ACK] Seq=9120 Ack=6010 Win=239 Lene0 TSval=305252058 TSecr=36 1718 7261.118326 172.17.7.13 192.168.56.137 TCP 43111 443 114 Application Data 1717 7261.118326 172.17.7.13 192.168.56.137 TCP 43111 443 68 43086 + 443 [ACK] Seq=9120 Ack=6010 Win=239 Lene0 TSval=307520550 TSecr=2691 1717 7261.118326 172.17.7.13 192.168.56.137 TCP 43111 443 68 43111 + 443 [ACK] Seq=9120 Ack=6010 Win=239 Lene0 TSval=307520550 TSecr=2691 1727 7261.118326 172.17.7.15.197 192.168.56.137 TCP 43111 443 68 43111 + 443 [ACK] Seq=9128 Ack=1041 Win=234 Lene0 TSval=30552058 TSecr=2691 1737 7261.250707 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 + 443 [ACK] Seq=9218 Ack=1041 Win=234 Lene0 TSval=3358312099 TSecr=36 1757 payload (46 bytes)								
8946 7141.248544       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       114 Application Data         9948 7141.24876       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       114 Application Data         1528 7201.17266       172.17.73.3       192.168.56.137       TLSv1.2       43111       443       64 3111 + 443       445       64 3111 + 443       447       114 Application Data         1538 7201.17266       172.17.27.33       192.168.56.137       TCP       43086       443       66 43086 + 443       [ACK] Seq=9126 Ack=10949 Win=224 Len=0 TSval=336042087 TSecr=36         1537 7201.47266       172.17.27.33       192.168.56.137       TCP       43086       443       66 43086 + 443 [ACK] Seq=9172 Ack=10949 Win=224 Len=0 TSval=336052098 TSecr=36         1537 7201.4797       172.17.95.197       192.168.56.137       TCP       43086       443       114 Application Data         1270 7261.118158       172.17.27.33       192.168.56.137       TCP       43086       443       114 Application Data         12173 7261.250544       172.17.95.197       192.168.56.137       TCP       43086       443       114 Application Data         12173 7261.250544       172.17.95.197       192.168.56.137       TCP       43086       443								
9488 7141.748736 172.17.95.197 192.168.56.137 TCP 43111 443 66 43111 → 443 [ACK] Seq=9126 Ack=10949 Win=224 Len=0 TSval=3350192097 TSecr=36 1528 7201.11706 172.17.27.33 192.168.56.137 TCP 43086 443 114 Application Data 1530 7201.12726 172.17.27.33 192.168.56.137 TCSv1.2 43086 443 68 43086 → 443 [ACK] Seq=9126 Ack=1996 Win=239 Len=0 TSval=307460549 TSecr=2691 1531 7201.249601 172.17.95.197 192.168.56.137 TCSv1.2 43111 443 168 43111 → 443 [ACK] Seq=9172 Ack=10995 Win=224 Len=0 TSval=3350252098 TSecr=36 12172 7261.118256 172.17.733 192.168.56.137 TCSv1.2 43086 443 114 Application Data 12172 7261.118256 172.17.733 192.168.56.137 TCP 43086 443 114 Application Data 12172 7261.118256 172.17.733 192.168.56.137 TCP 43086 443 114 Application Data 12172 7261.11826 172.17.95.197 192.168.56.137 TCP 43086 443 114 Application Data 12172 7261.11826 172.17.95.197 192.168.56.137 TCP 43086 443 114 Application Data 12175 7261.250707 172.17.95.197 192.168.56.137 TCP 43086 443 68 43086 → 443 [ACK] Seq=9120 Ack=6010 Win=239 Len=0 TSval=305252058 TSecr=361 12175 7261.250707 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 → 443 [ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=30550312099 TSecr=361 12175 7261.250707 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 → 443 [ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=33530312099 TSecr=361 12175 7261.250707 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 → 443 [ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=33530312099 TSecr=361 12175 7261.25070 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 → 443 [ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=33530312099 TSecr=361 12175 7261.25070 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 → 443 [ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=33530312099 TSecr=361 12175 7261.25070 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 → 443 [ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=3350312099 TSecr=361 12175 7261.25070 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 → 443 [ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=3350312099 TSecr=361 1								
1528 7201.117066       172.17.27.33       192.168.56.137       TLSV.2       43086       443       114 Application Data         1530 7201.117266       172.17.27.33       192.168.56.137       TLSV.2       43086       443       114 Application Data         1530 7201.249601       172.17.95.197       192.168.56.137       TLSV.2       43111       443       164 Application Data         1533 7201.249777       172.17.95.197       192.168.56.137       TLSV.2       43111       443       164 Application Data         1533 7201.249777       172.17.73.3       192.168.56.137       TLSV.2       43111       443       164 Application Data         1720 7261.11826       172.17.73.3       192.168.56.137       TLSV.2       43181       443       164 Application Data         1727 7261.118326       172.17.27.33       192.168.56.137       TLSV.2       43086       443       164 Application Data         1727 7261.128074       172.17.95.197       192.168.56.137       TLSV.2       43086       443       66 43086 + 443 [AcK] Seq=912 Ack=6010 Win=239 Len=0 TSval=3350320500 TSecr=2691         1275 7261.250747       172.17.95.197       192.168.56.137       TLSV.2       43111 443       443 pilcation Data         1275 7261.250707       172.17.95.197       192.168.56.137       TLSV.2								
1530 7201.117266       172.17.27.33       192.168.56.137       TCP       43086       443       68 43086 + 443       [ACK] Seq=5864 Ack=5964 Win=239 Len=0 TSval=307460549 TSecr=2691         1531 7201.249601       172.17.95.197       192.168.56.137       TCP       43081       443       68 43086 + 443       [ACK] Seq=5864 Ack=5964 Win=239 Len=0 TSval=307460549 TSecr=2691         1531 7201.24977       172.17.95.197       192.168.56.137       TCP       43111       443       164 Application Data         1210 7261.118158       172.17.27.33       192.168.56.137       TCP       43086       443       164 Application Data         12172 7261.118158       172.17.95.197       192.168.56.137       TCP       43086       443       144 Application Data         12172 7261.118158       172.17.95.197       192.168.56.137       TCP       43086       443       144 Application Data         12173 7261.258764       172.17.95.197       192.168.56.137       TCP       43086       443       164 43114       443       144 Application Data         12173 7261.258707       172.17.95.197       192.168.56.137       TCP       43111       443       64 43111 + 443       443       144 Application Data         12173 7261.258707       172.17.95.197       192.168.56.137       TCP       43111       4								
1531 7201.249601       172.17.95.197       192.168.56.137       TLSV1.2       43111       443       114 Application Data         1533 7201.249777       172.17.95.197       192.168.56.137       TLSV1.2       43111       443       114 Application Data         1270 7261.118358       172.17.27.33       192.168.56.137       TLSV1.2       43086       443       164 Application Data         2172 7261.118358       172.17.27.33       192.168.56.137       TLSV1.2       43086       443       164 Application Data         2172 7261.118326       172.17.95.197       192.168.56.137       TLSV1.2       43086       443       164 Application Data         2173 7261.256707       172.17.95.197       192.168.56.137       TLSV1.2       43111       443       144 Application Data         2175 7261.250707       172.17.95.197       192.168.56.137       TLSV1.2       43111       443       144 Application Data         2175 7261.250707       172.17.95.197       192.168.56.137       TLSV1.2       43111       443       164 Application Data         2175 7261.250707       172.17.95.197       192.168.56.137       TLSV1.2       43111       443       68 43111 + 443       44X       564       561.47       561.47       561.47       561.47       561.47       561.47								
1533 7201.249777       172.17.95.197       192.168.56.137       TCP       43111       443       68 43111 + 443       ACK] Seq=9172 Ack=10995 Win=224 Len=0 TSval=3350252098 TSecr=36         12170 7261.118158       172.17.27.33       192.168.56.137       TCP       43086       443       114 Application Data         12170 7261.128326       172.17.27.33       192.168.56.137       TCP       43086       443       64 Application Data         12172 7261.118356       172.17.7.33       192.168.56.137       TCP       43086       443       66 A9316CX] Seq=5910 Ack=6010 Win=239 Len=0 TSval=3350252095 TSecr=2691         2173 7261.250544       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       68 43111 + 443       443       Ack       564 9306C + 443       FCK] Seq=9218 Ack=1041 Win=224 Len=0 TSval=3350312099 TSecr=369         2175 7261.250707       172.17.95.197       192.168.56.137       TCP       43111       443       68 43111 + 443       ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=3350312099 TSecr=369         2175 7261.250707       172.17.95.197       192.168.56.137       TCP       43111       443       68 43111 + 443       ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=3350312099 TSecr=369         2175 7261.250707       172.17.95.197       192.168.56.137       TCP       43111       443       68 43111 + 443								
2170 7261.118158 172.17.27.33 192.168.56.137 TLSv1.2 43086 443 114 Application Data 2172 7261.118326 172.17.27.33 192.168.56.137 TCP 43086 443 64 3086 + 443 [ACK] Seq=510 Ack=6010 Win=239 Len=0 TSval=307520550 TSecr=2691 2173 7261.250707 172.17.95.197 192.168.56.137 TCP 43111 443 114 Application Data 2175 7261.50707 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 + 443 [ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=3350312099 TSecr=369 [Bytes sent since last PSH flag: 46] TCP payLoad (46 bytes)								
2172 7261.118326       172.17.27.33       192.168.56.137       TCP       43866       443       66 43866 + 443       [Ack] Seq=5910       Ack=6010       Win=239       Len=0       TSval=307520550       TSecc=2691         2173 7261.250544       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       114       Application       Data         1275 7261.250707       172.17.95.197       192.168.56.137       TCP       43111       443       66       43111 + 443       (Ack] Seq=9218       Ack=11041       Win=224       Len=0       TSval=3369312099       TSecr=360         1275 7261.250707       172.17.95.197       192.168.56.137       TCP       43111       443       66       43111 + 443       (Ack] Seq=9218       Ack=11041       Win=224       Len=0       TSval=3350312099       TSecr=360         1275 7261.250707       172.17.95.197       192.168.56.137       TCP       43111       443       66       43111 + 443       (Ack] Seq=9218       Ack=11041       Win=224       Len=0       TSval=3350312099       TSecr=360         129       Hot       Hot       Hot       Hot       Hot       Hot       Win       Hot       Win       Hot       Win       Hot       Win       Win       Win       Win								
2173 7261.250544       172.17.95.197       192.168.56.137       TLSv1.2       43111       443       114 Application Data         2175 7261.250707       172.17.95.197       192.168.56.137       TCP       43111       443       68 43111 + 443       4ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=3350312099 TSecr=36         [Bytes sent since last PSH flag: 46]         00000 00 04 00 0         0000 00 04 00 0         0000 00 04 00 0         0000 00 04 5 a0 06								
2175 7261.250707 172.17.95.197 192.168.56.137 TCP 43111 443 68 43111 → 443 [ACK] Seq=9218 Ack=11041 Win=224 Len=0 TSval=3350312099 TSecr=36 [Bytes sent since last PSH flag: 46] TCP payload (46 bytes) 000 00 04 00 0 0010 45 a0 00 6								
[Bytes sent since last PSH flag: 46] TCP payload (46 bytes) TCP payload (46 bytes) TCP payload (46 bytes)								
TCP payload (46 bytes) 0010 45 a0 00 6	1/3 /20	1.230/0/	1/2.1/.33.13/	192.108.30.137	TCF	45111	445	00 4111 4 443 [ACK] 364-3210 ACK-11041 WIH-224 LEH-0 13081-333012033 136(1-3039039
				flag: 46]				
ransport Layer Security 0020 c0 a8 38 8								0020 c0 a8 38 89 a8
TLSV1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol     Odd a0 66 8a 3     Odd a0 66 8a 3								

*Figure 11: Encrypted mTLS traffic between UDM and AMF* 

#### **Expected Results:**

. .....

- 1. Each VNF performs an mTLS handshake to mutually authenticate both ends of the API.
- 2. Data transmitted on SBI is encrypted.

#### Success Criteria:

- 1. Mutual authentication is implemented prior to SBI communications.
- 2. Data in transit is encrypted: cannot decode SUPI, IMEI, IMEISV, or NR Cell ID; cannot identify network function IP addresses, including AMF, SMF, NRF, and AUSF.

#### Results

Condition	Status
Mutual authentication is implemented prior to	Success: Network functions mutually
SBI communications	authenticate immediately after TCP session
	established and before any data exchanged.
Data in transit is encrypted: cannot decode	Success: All messages are encrypted;
SUPI, IMEI, IMEISV, NR Cell ID; cannot identify	cannot read contents to decipher PEI; IP
network function IP addresses, including AMF,	addresses are viewable, but no way to
SMF, NRF, and AUSF	associate them with specific NFs.
Overall Test	Successfully demonstrated that mTLS
	implementation encrypted data on SBA
	interfaces.

## Test Case 3 – Prevent Expired SBI Attach Request

### Test Case ID: TC-SBI-03

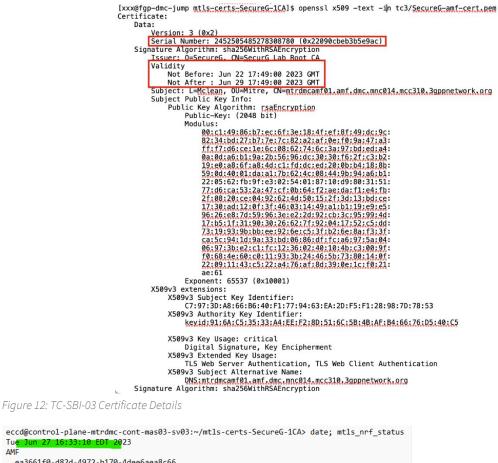
#### Description:

Utilizing the same configuration setup as the previous tests, Test Case 3 is designed to demonstrate mTLS, and to verify that expired credentials on one end will lead to a failed SBI connection. This prevents any out-of-date, and potentially vulnerable, network functions from attaching to the network.

#### **Objectives:**

- Demonstrate the ability to authenticate/authorize both sides of an HTTPS connection using mTLS.
- Demonstrate the inability of an NF with expired credentials to attach to the SBI when mTLS is implemented.

The first part of this test was conducted on June 27, 2023. First, a new certificate with near-term expiration was installed on the AMF. **Error! Reference source not found.** shows the relevant details of the certificate parameters. Of particular note is the certificate validation date, June 22, prior to certificate installation, and the certificate expiration date, June 29, two days after certificate installation. After installation of the new certificate, the AMF was re-registered to re-authenticate it with other NFs. Figure 13: and Figure 14: show the status of the certificate after installation; note the REGISTERED status in Figure 15: TC-SBI-03 Certificate Handshake Showing Certificate Serial Number and the Certificate State entry on the last line in Figure 14: indicating VALID. Figure 14: also shows both the web server and client-side authorization key usage, which indicate that mTLS has been implemented.



Tue Jun 27 16:33:10 EDT 2023 AMF ea3661f0-d82d-4972-b170-4dee6aea8c66 mfStatus REGISTERED - namf-comm REGISTERED - namf-mt REGISTERED - namf-mt REGISTERED - fagin mtrdmcamf01

Figure 13: TC-SBI-04 AMF registration status

mtrdmcamf@l erv@eric-pc	-mm-controller=0 ANCB ~ # gsh l	ist_node_credentialt_node_credential_node_credential_node_credentialg_node_credentiale_node_credentialt_node_credential_node_credential
Parameter Planned Data	Active Data	
timestamp	20230627114752	
planState	-	
ul (UserLabel)	NULL	
sn (SubjectName)	L= <u>Mclean.OU</u> =Mitre,CN= <u>mtrdmcamf</u>	02.anf.dmc.mc024.mcc320.3gppnetwork.org
et (EnrollmentTimer)	60	
ki (KeyInfo)	RSA_2048	
ep (EnrollmentProgress)	an (ActionName)	installCredentialEredUri
-	di (Additionellnfo) pi (ProgressInfo) pp (ProgressPercentage) res (Result) resi (ResultInfo) şt (State) ai (ActionId) tas (TimeActionCompleted) tas (TimeActionCompleted) tas (TimeActionCompleted)	NULL 100 5VCCESS NULL FINISHED 7 2023-06-27T11:47:52-05:00 2023-06-27T11:47:52-05:00
rm (RenewalMode)	MANUAL	
eat (ExpiryAlarmThreshold)	30	
Type (EnrollmentType)	PKCS12	
cc (CertificateContent)	version (Version)	3(0x2)
2a 47 cf 0b 64 f2 ae da f1	issuer (Issuer) validFrom (ValidFrom) validTo (ValidTo) publicKey (PublicKey) 08 62 74 6c 3a 97 bd ed a4 0a 0 e4 fb 2f 08 20 ce 44 92 62 4d 5	22090FCBED3559AC ligorithm sha559ithtR54Encryption 055ceur66, OK55ceur67, OK55ceur60, OK55ceur60, OK
keyid:91:64:C5:35:33:A4:EE: DNS:mirdmcam101.ami.dnc.mnc	<pre>keyUsage (KeyUsage) extensionContent (ExtensionCon F2:8D:51:6C:58:4B:AF:B4:66:76:D</pre>	X509v3 Key Usage: Digital Signature, Key EnciphermentX509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication
cs (CertificateState)	VALID	

Figure 14: TC-03 Certificate Status During Valid Period

Figure 15 and Figure 16: show Wireshark captures of SBI messages during the mTLS handshake protocol, specifically the key exchange from AMF (172.17.13.136) to NRF (192.168.56.143)—the AMF received a new IP address when reregistered. Figure 15 shows the AMF certificate serial number (0x22090cbeb3b5e9ac), which matches that in Figure 12: TC-SBI-03 Certificate Details. Figure 16: shows the validity period, agreeing with that in **Error! Reference source not found.** 

전 🔘 📙 🖾 🕱 🖻 🔍 👳 👳 🗿	ts Telephony Wirek						
ddr==192.168.56.143) 8.8 (tls.record.version == 0x	0303)						
Time	Source	Destination	Protocol	Rngap	Angap	Length Info	
381 2023-06-27 16:22:17.642892	172.17.13.136	192.168.56.143	TLSv1.2			114 Application Data	
383 2023-06-27 16:22:17.643060	192.168.56.143	172.17.13.136	TLSv1.2			114 Application Data	
385 2023-06-27 16:22:17.647908	172.17.13.136	192.168.56.143	TLSv1.2			114 Application Data	
387 2023-06-27 16:22:17.648075	192.168.56.143	172.17.13.136	TLSv1.2			114 Application Data	
570 2023-06-27 16:22:42.251833	172.17.13.136	192.168.56.143	TLSv1.2			99 Encrypted Alert	
572 2023-06-27 16:22:42.251952	172.17.13.136	192.168.56.143	TLSv1.2			99 Encrypted Alert	
574 2023-06-27 16:22:42.251975	192.168.56.143	172.17.13.136	TLSv1.2			99 Encrypted Alert	
576 2023-06-27 16:22:42.252082 687 2023-06-27 16:22:44.368406	192.168.56.143 172.17.13.136	1/2.1/.15.136	TL5v1.2 TL5v1.2			99 Encrypted Alert 287 Client Hello	
691 2023-06-27 16:22:44.369582	192.168.56.143	172.17.13.136	TLSv1.2			1595 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done	
709 2023-06-27 16:22:44.417734	172.17.13.136	192.168.56.143	TLSv1.2			2250 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake M	lossaga
711 2023-06-27 16:22:44.418256	192.168.56.143	172.17.13.136	TLSV1.2			119 Change Cipher Spec, Encrypted Handshake Message	waand a
713 2023-06-27 16:22:44.418230	172.17.13.136	192.168.56.143	TLSv1.2			149 Application Data	
715 2023-06-27 16:22:44,418723	192,168,56,143	172.17.13.136	TLSv1.2			152 Application Data	
Checksum Status: Unverified]							A 0060 02 08 22 0
Irgent Pointer: 0							0070 48 86 f7 0
ptions: (12 bytes), No-Operation (NO	P), No-Operation (	(NOP), Timestamps					0080 03 55 04 0
TCP Option - No-Operation (NOP)							0090 19 06 03 5 00e0 61 62 20 5
Kind: No-Operation (1)							0000 30 36 32 3
<pre>/ TCP Option - No-Operation (NOP)</pre>							00:0 36 32 39 3
Kind: No-Operation (1)							00d0 06 03 55 0
Y TCP Option - Timestamps							00c0 0c 06 03 55
Kind: Time Stamp Option (8)							00f0 38 06 03 55 0100 66 30 31 20
Length: 10							0100 66 30 31 20
Timestamp value: 154631834: TSv		r 3556446408					0120 74 77 6f 7
Timestamp echo reply: 355644640	8						0130 09 2a 86 4
Timestamps]							0140 00 30 82 0
[Time since first frame in this TC							0150 Be 18 4f et
[Time since previous frame in this [SEQ/ACK analysis]	ICP stream: 0.048	138000 seconds]					0160 a2 af 0e f 0170 6c 3a 97 b
[iRTT: 0.000086000 seconds]							0180 30 f6 2f c
[Bytes in flight: 2182]							0190 0b b4 18 88
[Bytes sent since last PSH flag: 2	1921						01a0 94 a6 b1 2
CP payload (2182 bytes)	101						01b0 31 51 77 d
sport Layer Security							01c0 fb 2f 08 20 01d0 17 30 ad 12
TLSv1.2 Record Laver: Handshake Proto	col: Certificate						01e0 26 e8 7d 59
Content Type: Handshake (22)							01f0 1f 31 90 30
Version: TLS 1.2 (0x0303)							0200 9b bb ee 92
Length: 1782							0210 9a 33 bd 0
Mandshake Protocol: Certificate							0220 fc 12 36 0 0230 93 3b 24 46
Handshake Type: Certificate (11	)						0240 76 af 8d 3
Length: 1778							0250 81 b0 30 85
Certificates Length: 1775							0260 c7 97 3d a
<ul> <li>Certificates (1775 bytes)</li> </ul>							0270 98 7d 78 5
			an and first interest of			A contract of the second	0280 14 91 6a c 0290 66 76 d5 44
	/a0030201020208220	90CDe0305e9ac300d06092	as64s86†70d01010b(1	s-at-commonName-mt	rancant01.	amf.dmc.mnc014.mcc310.3gppnetwork.org,id-at-organizationalUnitName=Hitre,id-at-localityName=Hclean)	02n0 64 63 62 65
✓ signedCertificate							02b0 06 08 2b 04
version: v3 (2) serialNumber: 0x22090ct							02c0 05 07 03 0
	eososesse						02d0 31 6d 74 72
SerialNumber: 0x22090ct							
✓ signature (sha256WithR5		sha256WithRSAEncryption					02e0 2e 64 6d 63 02f0 31 30 2e 33

Figure 15: TC-SBI-03 Certificate Handshake Showing Certificate Serial Number

2223-06-27 16:22:17.62798 12.27.17.13.18 12.2.16.5.6.14 17.27.17.13.18 15.4.2 13.4 Application bate 2223-06-27 16:22:42.25385 17.27.17.13.18 15.4.2 15.4.2 39 Encrypted Alert 2223-06-27 16:22:42.25385 17.27.17.13.18 15.4.2 39 Encrypted Alert 2223-06-27 16:22:42.25385 12.27.17.13.18 15.4.2 39 Encrypted Alert 2233-06-27 16:22:44.25384 12.27.17.13.18 15.4.2 39 Encrypted Alert 2233-06-27 16:22:44.25384 12.27.17.13.18 15.4.2 39 Encrypted Itert 2233-06-27 16:22:44.25384 12.27.17.13.18 15.4.2 39 Encrypted Itert 2233-06-27 16:22:44.25384 12.17.13.18 15.2.2.48 5.4.18 15.4.2 39 Encrypted Itert 2233-06-27 16:22:44.4854 17.17.13.18 15.4.2.2 139 Encrypted Itert 2233-06-27 16:22:44.4854 12.17.13.18 15.4.2.2 139 Encrypted Itert 2233-06-27 16:22:44.4854 12.17.13.18 15.4.2.2 139 Encrypted Itert 2233-06-27 16:22:44.4854 12.17.13.18 15.4.2.2 139 Encrypted Itert 2233-06-27 16:22:44.4854 12.1.11.18 15.4.2.11 18.4.2.2.11.18 15.4.2.2 139 Encrypted Itert 2233-06-27 16:22:44.4854 12.1.11.18 15.4.2.1 11.18 15.4.2.2 139 Encrypted Itert 2233-06-27 16:22:44.4854 12.1.11.18 15.4.2.2.11 15.4.2.2 139 Encrypted Itert 2233-06-27 16:22:44.4854 12.1.11.18 15.4.2.2.1 11.18 15.4.2.2 139 Encrypted Itert 2233-06-27 16:22:4.4.1854 12.1.11 18.4.2.2.4.11.18 15.4.2.2.1 11.18 15.4.2.2.1 13.4.2.2.1 13.4.2.2.1 13.4.2.2.2.2.4.4.2.2.2.2.2.2.2.4.4.2.2.2.2.2.2.2.4.4.2.2.2.2.2.2.2.4.4.2.2.2.2.2.2.2.2.2.4.4.2.2.2.2.2.2.2.2.2.4.4.2	Time		Q II				
2023 06.27 15:22:17.64282 12:27.17.13.18 12:185.64.24 17:27.17.13.18 12:185.64.24 17:27.17.13.18 12:185.64.24 17:27.17.13.18 12:185.64.24 17:27.17.13.18 13:19.12.11.27.17.13.18 12:185.64.24 17:27.17.13.18 13:19.12.11.27.17.13.18 12:185.64.24 17:27.17.13.18 13:19.12.11.27.17.13.18 13:19.12.12.11.27.17.13.18 13:19.12.12.11.27.17.13.18 13:19.12.12.12.11.27.17.13.18 13:19.12.12.12.11.27.17.13.18 13:19.12.12.12.11.27.17.13.18 13:19.12.12.12.11.27.17.13.18 13:19.12.12.12.12.11.27.17.13.18 13:19.12.12.12.11.27.17.13.18 13:19.12.12.12.11.27.12.11.27.11.27.17.13.18 13:19.12.12.12.12.11.27.11.27.11.27.11.27.11.27.11.27.17.11.27.11.27.17.17.17.17.17.17.17.17.17.17.17.17.17	10.00	(x0303)					
2823-06.27 16:22:17.64889 17.2.77.13.18 19.2.08.5.43 T.54.2 114 Application bats 2823-06.27 16:22:17.6489 17.2.77.13.18 17.2.77.13.18 T.54.2 114 Application bats 2823-06.27 16:22:42.2538 17.2.77.13.18 T.54.2 114 Application bats 2823-06.27 16:22:44.2589 17.2.77.13.18 T.54.2 114 Application bats 2823-06.27 16:22:44.2589 17.2.17.13.18 T.54.2 114 Application bats 2823-06.27 16:22:44.2589 19.2.106.5.61 17.2.77.13.18 T.54.2 125 Exercised Application bats 2823-06.27 16:22:44.2589 19.2.106.5.61 11.2.48.11.11 (5.46.26.26.26.26.26.26.26.26.26.27.20.27.	201 2022-06-27 16:22:17 642002	Source	Destination	Protocol	Bridan	Angap	Length Info
2223-6-22 16:22:17.64089 12.17.61.26 12.22:17.61.26 12.22:17.61.26 13.2 12.21.61.5.6.1.8 15.0.2 13.6.6.6.18 15.0.2 14.6.18 15.0.2 14.6.18 15.			192,168,56,143			1.1.1.1.1.1.1	
222-0-27 16/22/17/62/097 222-0-27 16/22/17/51/38 122.175.13.18 120.185.65.143 TUSU.2 99 Encrypted Alert 222-0-27 16/22/42.29508 20.126.165.61.43 127.175.13.18 150.12 99 Encrypted Alert 222-0-27 16/22/42.29508 20.126.156.163 127.175.13.18 150.12 99 Encrypted Alert 222-0-27 16/22/42.29508 20.126.156.163 127.175.13.18 150.12 1010 C 200 C 2	383 2023-06-27 16:22:17.643060	192.168.56.143	172.17.13.136	TLSv1.2			
2823-69.27 16:22:42.25829 172.17.13.18 192.184.56.143 TUSU.2 99 Encrypted Alert 2823-69.27 16:22:44.25864 172.17.13.18 192.184.56.143 TUSU.2 99 Encrypted Alert 2823-69.27 16:22:44.25864 172.17.13.18 192.184.56.143 TUSU.2 99 Encrypted Alert 2823-69.27 16:22:44.25864 172.17.13.18 192.184.56.143 TUSU.2 195 Encrypted Alert 2823-69.27 16:22:44.25864 172.17.13.18 192.184.56.143 TUSU.2 195 Encrypted Alert 2823-69.27 16:22:44.25864 172.17.13.18 192.184.56.143 TUSU.2 195 Encrypted Alert 2823-69.27 16:22:44.25864 172.17.13.18 TUSU.2 195 Encrypted Hello 2823-69.27 16:22:44.25864 172.17.13.18 192.17.13.18 TUSU.2 195 Encrypted Hello 2823-69.27 16:22:44.25864 172.17.13.18 TUSU.2 195 Encrypted Hello 2823-69.27 16:22:44.25864 172.17.13.18 TUSU.2 195 Encrypted Hello 2823-69.27 16:22:44.25864 172.17.13.18 TUSU.2 195 Encrypted Hello 2823-69.27 16:22:44.25864 172.18 TUSU.2 195 Encrypted Hello 2823-69.27 16:22:44.25864 172.18 TUSU.2 195 Encrypted Hello 2823-69.27 16:22:44.25864 172.18 TUSU.2 195 Encrypted Hello 2824-67.27 16:22:44.25864 172.10 TUSU.2 195 Encrypted Hello 2824-67.27 16:22:44.25864 172.10 TUSU.2 195 Encrypted Hello 2824-67.27 16:22:44.2	385 2023-06-27 16:22:17.647908	172.17.13.136	192.168.56.143	TLSv1.2			114 Application Data
2022-06-27 16:22:42.53509 172.171.13.16 192.46.56.143 172.171.31.16 1555.2 2022-06-27 16:22:42.53507 192.42:42:42 2022-06-27 16:22:42.53507 192.42:42:42 2022-06-27 16:22:44.30684 172.171.31.16 175.1.2 99 Incrypted Alert 2022-06-27 16:22:44.30684 127.171.31.16 175.1.2 1955 Server Hells, Certificate, Server Key Exchange, Certificate Reguest, Server Hells 2022-06-27 16:22:44.30684 127.171.31.16 175.1.2 1955 Server Hells, Certificate, Server Key Exchange, Certificate Reguest, Server Hells 2022-06-27 16:22:44.30684 127.171.31.16 175.1.2 1955 Server Hells, Certificate, Server Key Exchange, Certificate Key Exchange, Cherificate Key Exc	387 2023-06-27 16:22:17.648075	192.168.56.143	172.17.13.136	TLSv1.2			114 Application Data
<pre>:422-60/2 16:22:42.5309( 19:21.65.61.43 17:2.7.1.116 15:1.2 19:1.crypted Alert 2823-60/2 15:22:42.5308( 17:21.715.15 19:21.45.51.43 15:1.2 29:1.1000 Alert 2823-60/2 15:22:44.8058( 17:21.715.15 19:21.65.61.43 15:1.2 29:1.1000 Alert 2823-60/2 15:22:44.8058( 17:21.715.15 19:21.65.61.43 15:1.2 19:1.1000 Alert 2823-60/2 15:22:44.8058( 17:21.715.15 19:21.65.61.43 15:1.2 19:1.1000 Alert 2823-60/2 15:22:44.8058( 17:21.715.15 19:21.65.61.43 15:1.2 19:1.1000 Alert 2823-60/2 15:22:44.8058( 17:21.715.15 19:21.65.61.43 15:1.2 19:4.1000 Alert 2823-60/2 15:22:44.8058( 17:21.715.15 19:21.65.61.43 15:1.2 19:4.1000 Alert 2823-60/2 15:22:44.8058( 17:21.715.15 19:21.65.61.43 15:1.2 19:4.1000 Alert 2823-60/2 15:22:44.8058( 17:71.717.11 (16:1.56.56.43 15:1.2 19:4.1000 Alert 2823-60/2 15:22:44.8058( 17:71.717.11 (16:1.56.56.43 15:1.2 19:4.1000 Alert 2823-60/2 15:22:44.8058( 17:71.717.11 (16:1.56.56.44 15:1.2 19:4.1000 Alert 2823-60/2 15:22:44.8058( 17:71.717.11 (16:1.56.56.44 15:4.1000 Alert 2823-60/2 15:22:4.4.8058( 17:71.717.11 (16:1.56.56.44 15:4.1000 Alert 29.1.1000 Alert 20.1.1000 Alert 20.1.1000</pre>	570 2023-06-27 16:22:42.251833	172.17.13.136	192.168.56.143	TLSv1.2			99 Encrypted Alert
2823-06-27 16:22:43.83606 19:22:127:13:15 12:22:127:13:15 15:12 15:12 27 Client Helio 2823-06-27 16:22:44.83082 13:21:16:61.64 127:17:13:18 T5:12 15:55 Erver Helio Certificate, Server Key Exchange, Certificate Request, Server Helio Certificate, Client Key Exchange, Certificate Request, Server Helio Certificate Represt, Server Key Schange, Certificate Represt, Server Key Schange, Certificate Represt, Server Helio Certificate Represt, Server Key Schange Cerificate Represt, Server Key Schange Certificate Represt, S	572 2023-06-27 16:22:42.251952						
222-06-27 15:22:44.96969 172.77.13.136 122.145.54.137 172.77.13.156 122.17.13.136 122.	574 2023-06-27 16:22:42.251975						
2022-06.27 15:22:44.3028 192.166.61.43 122.17.13.16 12.47.13.16 154.2 1955 Enver Mella, Certificate, Enver Key Exchange, Certificate Reguest, Server Mella Certificate, Clear Key Exchange, Certificate Werlfs, Chemer Key Exchange, Certificate Reguest, Server Mella Certificate, Clear Key Exchange, Certificate Werlfs, Chemer Key Exchange, Certificate Reguest, Server Mella Certificate, Clear Key Exchange, Certificate Reguest, Server Mella Certificate, Clear Key Exchange, Certificate Werlfs, Chemer Key Exchange, Certificate Reguest, Server Mella Certificate, Clear Key Exchange, Cl	576 2023-06-27 16:22:42.252082						
2823-06-27 15:22:44.8256 15:21:45:265 63:45 172.171.31:36 122.164.56:143 125.12. 119 Change Clerificate Months Reside 195.12. 119 Clerificate Months Reside 195.12. 119 Clerificate Months Reside 195.12.							
2823-66-27 15:22:44.4826 122:163.54.4 122:17:13:18 TL5V1.2 119 Ange Clpher Spec, Encrypted Handbake Hessage 2823-66-27 15:22:44.4826 122:17:13:18 TL5V1.2 119 Ange Clpher Spec, Encrypted Handbake Hessage Algorithm Id: 1.2.400.11340.1.11 (hs2504thb8Ancryption) * Issue: notsequence (0) * Indequence 12 time (1d-at-compatizationales-Secured) * Object 1d: 2.5.4.18 (1d-at-compatizationales-Secured) * Intervision principal (1d-at-compatizationales-Secured) * Intervision (1d-at-compa	591 2023-06-27 16:22:44.369582						
<pre>2222-06-22 16:22:44.4824 127.27.13.136 122.06.56.143 125.12 15.4.2 139 Application Data 2023-06-27 16:22:44.4826 127.27.13.136 122.06.56.143 175.12 139 Application Data 2023-06-27 16:22:44.4827 129 Application Data Algorithm Id: 13.16.40.113491.11.11 (sh2564tht84fsrcppton) * issue: rdsEquence 2 lises (id-at-companizationNase-Secure(s) * dDSEquence 1 item (id-at-companizationNase-Secure(s) * dDSEquence 3 item (id-at-companizationNase-Secure(s) * dDSEquence 1 item (i</pre>							
<pre>2x22.4672 16:22:44.41721 192.16.46.41 172.72.11.16 154.04 154.04 172.72.11.16 154.04 1</pre>							
<pre>Algorithm Id: 1.2.440.11340.1.1.11 (sha250dth854fncryption)      Visuer: rdstegence (0)     Vidioquence 1:em: (id=4-commoName=Secured iab Root CA, id=4-organizationName=Secured)     Vidioquence item: 1:em (id=4-commoName=Secured)     Vidioquence item: 1:em (id=4-commoName=Secured iab Root CA)     Vidioquence item: 1:em (id=4-commoName=Secured).secile(s)     Vidioquence ite</pre>							
<pre>v isseer indisequence (0) v indisequence (0) v indisequence (1 is (1 det-components-Secured) v indisequence (1 det (1 d</pre>	15 2025-06-27 16:22:44.418721	192.168.56.143	177.17.14.136	1150(1,2			152 ADDITCATION WATA
<pre></pre>	<pre></pre>	nguishedName item (: 2.5.4.3 (id-at-comm tring: printableStri leString: SecurG Leb (0) -22 17:49:00 (UTC) 0) -29 17:49:00 (UTC) 0) s (id-at-commonName	id-at-commonName=Secur monName) Ing (1) > Root CA ====================================	G Lab Root CA)	ork.org,id-at-org	anizationa	lUnitMamedMitre,id-st-localityMamedMclean)
<pre>     # RDEGenerice West 1 time (id-a-corganizationalinitame=Mitre)     WelativeDistinguishedmes time (id-a-corganizationalinitame=Mitre)     Object 1d: 2.5.4.11 (id-at-corganizationalinitame=Mitre)     V DirectoryString pintableString (1)</pre>		2.5.4.7 (id-at-located tring: printableStri	alityName)	ean)			
♥ RelativeDistinguishedName item (id-at-organizationalUnitName=Nitre) Object Id: 2.5.4.11 (id-at-organizationalUnitName) ♥ DirectoryString: printableString (1)	<ul> <li>RelativeDisti</li> <li>Object Id:</li> <li>DirectoryS</li> </ul>	lestring: Mclean	and an advantage and	tool			
Object Id: 2.5.4.11 (id-at-organizationalUnitime) * DirectoryString: printableString (1)	<ul> <li>RelativeDisti</li> <li>Object Id:</li> <li>DirectoryS</li> <li>printab</li> </ul>			cre)			
V DirectoryString: printableString (1)	<ul> <li>RelativeDisti</li> <li>Object Id:</li> <li>DirectoryS</li> <li>prigtab</li> <li>RDNSequence teem</li> </ul>	: 1 item (id-at-org		(thang-Mitra)			
	<pre></pre>	: 1 item (id-at-org nguishedName item (:	id-at-organizationalUn	itName=Mitre)			
printableString: Nitre	<pre></pre>	: 1 item (id-at-org nguishedName item (: 2.5.4.11 (id-at-org	id-at-organizationalUn ganizationalUnitName)	itName=Mitre)			
* RDNSequence item: 1 item (id-at-commonName=mtrdmcamf01.amf.dmc.mnc014.mcc310.3gppnetwork.org)	<pre>% RelativeDisti Object Id:</pre>	: 1 item (id-at-org nguishedName item (: 2.5.4.11 (id-at-org tring: printableStr:	id-at-organizationalUn ganizationalUnitName)	itName=Mitre)			
RelativeDistinguishedName item (id-at-commonName-mtrdmcamf01.amf.dmc.mnc014.mcc310.3gppnetwork.org)	<pre></pre>	: 1 item (id-at-org nguishedName item (: 2.5.4.11 (id-at-org tring: printableStr: leString: Mitre	id-at-organizationalUn ganizationalUnitName) lng (1)	5	(ppnetwork.org)		
Object Id: 2.5.4.3 (id-at-commonName)	<pre>% RelativeDist:</pre>	: 1 item (id-at-org nguishedName item (: 2.5.4.11 (id-at-org tring: printableStr: leString: Mitre : 1 item (id-at-com	id-at-organizationalUn ganizationalUnitName) lng (1) nonNane=mtrdmcamf01.am	f.dmc.mnc014.mcc310.3p		rk.org)	
✓ DirectoryString: printableString (1)	<pre></pre>	<pre>:: 1 item (id-at-org nguishedName item (: 2.5.4.11 (id-at-org tring: printableStri leString: Nitre :: 1 item (id-at-com nguishedName item (:</pre>	id-st-organizationalUn ganizationalUnitName) lng (1) nonName=mtrdmcamf01.am id-at-commonName=mtrdm	f.dmc.mnc014.mcc310.3p		rk.org)	
printableString: mtrdmcamf01.amf.dmc.mnc014.mcc310.3gppnetwork.org	<ul> <li>Relativalisti</li> <li>Object dil</li> <li>DirectoryS</li> <li>pritabi</li> <li>RollSequence Res</li> <li>Relativalisti</li> <li>Object dil</li> <li>Solkequence iten</li> <li>Relativalisti</li> <li>Object dil</li> <li>V DirectoryS</li> </ul>	: 1 item (id-at-org nguishedName item (: 2.5.4.11 (id-at-org tring: printableStri leString: Mitre :: 1 item (id-at-com nguishedName item (: 2.5.4.3 (id-at-com tring: printableStri tring: printableStri	id-at-organizationalUn ganizationalUnitName) ing (1) monName=mtrdmcamf01.am id-at-commonName=mtrdm monName) ing (1)	f.dmc.mnc014.mcc310.3g camf01.amf.dmc.mnc014.		rk.org)	
✓ subjectPublicKeyInfo	<ul> <li>Relativaliti</li> <li>Object Idi</li> <li>Object Idi</li> <li>Relativaliti</li> <li>Object Idi</li> <li>Object Idi</li> <li>Object Idi</li> <li>Object Idi</li> <li>Object Idi</li> <li>Skikequanci itee</li> <li>Relativaliti</li> <li>Object Idi</li> </ul>	: 1 item (id-at-org nguishedName item (: 2.5.4.11 (id-at-org tring: printableStri leString: Mitre :: 1 item (id-at-com nguishedName item (: 2.5.4.3 (id-at-com tring: printableStri tring: printableStri	id-at-organizationalUn ganizationalUnitName) ing (1) monName=mtrdmcamf01.am id-at-commonName=mtrdm monName) ing (1)	f.dmc.mnc014.mcc310.3g camf01.amf.dmc.mnc014.		rk.org)	

*Figure 16:* TC-*SBI*-03 Certificate Handshake Showing Validity Period

The second part of the test occurred on June 29, 2023, starting shortly before the certificate expiration time of 17:49:00 UTC (13:49 EDT), and with final captures taken after the certificate expiration. Figure 17 shows the same details as in Figure 14: , but queried at 17:50:49, shortly after the desired certificate expiration, in which the status still shows VALID. Figure 18 then shows the same statistics at 17:56:38, where now the Certificate State indicates EXPIRED.

Thu Jun 29 17:50:49 UTC 2023

TLP:GREEN:5GSTB

Parameter Planned Data	Active Data	
timestamp	20230627114752	
planState	-	
ul (UserLabel)	NULL	
sn (SubjectName)	L=Hclean,OU=Hitre,CN=mtrdmcamf	21.amf.dmc.mucRl4.mc310.3gpmetwork.mcg
et (EnrollmentTimer)	68	
ki (KeyInfo)	RSA_2048	
ep (EnrollmentProgress)	an (ActionName)	1nstallCredentialEcoNri
	pi (ProgressInfo) pp (ProgressPercentage) ress (Result) ress (ResultInfo) st (State) ai (ActionId) tas (TimeActionCampleted) tas (TimeActionCampleted)	NULL 180 SUCCESS NULL 77 72 7223-06-27T11:47:52-05:00 2223-06-27T1:47:52-05:00 2223-06-27T1:47:52-05:00 2223-06-27T1:47:52-05:00
rm (RenewalMode)	MANUAL	
eat (ExpiryAlarmThreshold)	30	
type (EnrollmentType)	PKCS12	
cc (CertificateContent)	version (Version)	3(8x2)
ae da f1 e4 fb 2f 08 20 ce 33 bd 06 86 df <u>f</u> <u>s</u> a6 97 5a	issuer (Issuer) validFrom (ValidFrom) validTo (ValidFrom) publickey (Publickey) 6: 3a 97 bd ed a4 0a dd a5 b1 9 49 26 24 d5 15 27 3d 13 bd c 64 00 97 33 42 c1 fc 13 36 24 69 07 39 42 c2 fc 10 10 10 10 10 10 evisage (Keylisage) extensionContent (ExtensionCom	X509v3 Key Usage: Digital Signature, Key EnciphermentX509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication

Figure 17: TC-SBI-03 Certificate Details Shortly after Expiration

Thu Jun 29 17:56:38 UTC 200 mtrdmsamf01 erv@eris-pr		ussh get_node_credential -nci mtlsIC3
Parameter Planned Data	Active Data	
timestamp	20230629125340	
planState	-	
ul (UserLabel)	NULL	
sn (SubjectName)	L=Mclean,OU=Mitre,CN=mtrdmcanf@	1.amf.dmc.mocR14.mcc318.3gpportwork.org
et (EnrollmentTimer)	60	
ki (KeyInfo)	RSA_2048	
ep (EnrollmentProgress)	an (ActionName)	installCredentialFromVri
-	pi (ProgressInfo) pp (ProgressPercentage) res (Result) resi (ResultInfo) st (State) ai (ActionId) tas (TimeActionStarted) tac (TimeActionCompleted)	NULL NUL SUCCESS NULL FUISHED 7 2823-06-2711:47:52-05:00 2823-06-2711:47:52-05:00
rm (RenewalMode)	MANUAL	
eat (ExpiryAlarmThreshold)	30	
type (EnrollmentType)	PKC512	
cc (CertificateContent)	version (Version)	3(0x2)
ae da f1 e4 fb 2f 08 26 ce 33 bd 06 86 df fc a6 97 5a kexid:91:64:C5:35:33:A4:EE	04 92 62 4d 50 15 2f 3d 13 bd ce 04 06 97 3b e2 c1 fc 12 36 02 40 publicKeyAlgorithm (PublicKeyAl keyUsage (KeyUsage) extensionContent (ExtensionCont	<ul> <li>0-SecureG, ON-SecurEG Lab. Root CA.</li> <li>2023-0-0-2717:49:08+08:08</li> <li>2023-06-2717:49:08+08:08</li> <li>2023-06-2717:49:08+08:08</li> <li>2023-06-2717:49:08+08:08</li> <li>2024-06-2717:49:08+08:08</li> <li>2025-06-2717:49:08+08:08</li> <li>2025-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08+08:08</li> <li>2026-06-2717:49:08</li> <li>2026-06-2717:49:08-08</li> <li>2026-0717:49:08-08</li> <li>2026-0717:49:08-08</li> <li>2026-08-2717:49:08-08</li> <li>2026-08-2717:49:08-08</li> <li>2026-08</li> <li>2026-08-2717:49:08-08</li> <li>2026-08-28</li> <li>2026-08-2717:49:08-08</li> <li>2026-08</li> <li>2026-08<!--</td--></li></ul>
cs (CertificateState)	EXPIRED	

Figure 18: TC-SBI-03 Certificate Details Seven Minutes after Expiration

Figure 19 shows traffic from the ITC trace files in which we see encrypted application data between an AMF IP address (172.17.95.197) and the NRF (192.168.56.143) at 13:59:08 EDT. However, one minute later, at 13:59:16, we see alerts from that IP address and a different AMF IP address (172.17.27.33) to the NRF, followed by [RST, ACK] messages tearing down the corresponding TCP connections. Figure 20 shows the subsequent initiation of reconnection with Confidential and Proprietary to the 5G Security Test Bed – Not for Disclosure 26 a Client Hello, Server Hello, and eventual key exchange failure due to certificate expiration. Figure 21 shows a fatal alert message, indicating certificate expiration as the cause of failure.

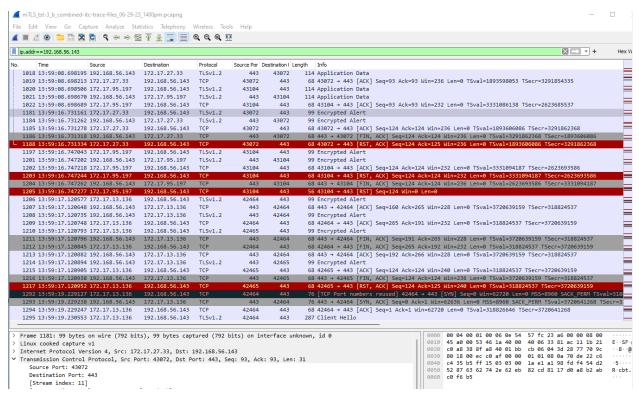


Figure 19: TC-SBI-03 Alerts and [RST, ACK] Messages after Certificate Expiration

Edit View Go Capture						
🔳 🧟 💿 🚞 🛅 🔁	۹ ⇔ ⇔ ≅	₹ 🕹 📃 🔳	9, 9, 9, <u>1</u>	E		
.addr==192.168.56.143						
Time Source		Destination	Protocol		Destination I	
211 13:59:17.120796 192.			TCP	443	42464	68 443 → 42464 [FIN, ACK] Seq=191 Ack=265 Win=228 Len=0 TSval=3720639159 TSecr=31882455
212 13:59:17.120845 172.		192.168.56.143	TCP	42464	443	68 42464 → 443 [FIN, ACK] Seq=265 Ack=192 Win=232 Len=0 TSval=318824537 TSecr=372063915
213 13:59:17.120882 192.			тср	443	42464	68 443 → 42464 [ACK] Seq=192 Ack=266 Win=228 Len=0 TSval=3720639159 TSecr=318824537
214 13:59:17.120894 192.			TLSv1.2	443	42465	99 Encrypted Alert
215 13:59:17.120905 172.		192.168.56.143	TCP	42465	443	68 42465 → 443 [ACK] Seq=124 Ack=124 Win=240 Len=0 TSval=318824537 TSecr=3720639159
216 13:59:17.120938 192.			TCP	443	42465	68 443 → 42465 [FIN, ACK] Seq=124 Ack=124 Win=236 Len=0 TSval=3720639159 TSecr=3188245
217 13:59:17.120952 172.		192.168.56.143	ТСР ТСР	42465 42464	443 443	68 42465 → 443 [RST, ACK] Seq=124 Ack=125 Win=240 Len=0 TSval=318824537 TSecr=37206391
292 13:59:19.229127 172.		192.168.56.143				76 [TCP Port numbers reused] 42464 → 443 [SYN] Seq=0 Win=62720 Len=0 MSS=8960 SACK_PER/
293 13:59:19.229238 192. 294 13:59:19.229247 172.		172.17.13.136 192.168.56.143	TCP	443 42464	42464 443	76 443 → 42464 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=37206412
294 13:59:19.229247 172. 295 13:59:19.230553 172.			TCP TLSv1.2	42464	443	68 42464 → 443 [ACK] Seq=1 Ack=1 Win=62720 Len=0 TSval=318826646 TSecr=3720641268 287 Client Hello
295 13:59:19.230553 172. 296 13:59:19.230584 192.			TLSV1.2 TCP	42464		
296 13:59:19.230584 192. 297 13:59:19.230829 172.		192.168.56.143	ТСР	443	42464 443	68 443 → 42464 [ACK] Seq=1 Ack=220 Win=62464 Len=0 TSval=3720641269 TSecr=318826647 76 [TCP Port numbers reused] 42465 → 443 [SYN] Seg=0 Win=62720 Len=0 MSS=8960 SACK PEN
297 13:59:19.230829 172. 298 13:59:19.230923 192.			TCP	42465	445	76 [TCP Port numbers reused] 42465 → 445 [STN] Seq=0 WIN=62720 Len=0 MSS=6960 SACK_PER 76 443 → 42465 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK PERM TSval=3720641
298 13:59:19.230923 192. 299 13:59:19.230932 172.		192.168.56.143	TCP	445	42405	76 445 → 42465 [STN, ACK] Seq=0 ACK=1 Win=62750 Len=0 MSS=8960 SACK_PENH ISVal=5720641 68 42465 → 443 [ACK] Seq=1 Ack=1 Win=62720 Len=0 TSval=318826647 TSecr=3720641269
300 13:59:19.231772 192.			TLSv1.2	42465	445	1595 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello D
301 13:59:19.231783 172.			TCP	445	42404	68 42464 → 443 [ACK] Seq=220 Ack=1528 Win=61440 Len=0 TSval=318826648 TSecr=3720641270
302 13:59:19.232369 172.			TLSv1.2	42464	445 44 <mark>3</mark>	68 42464 → 445 [ACK] Seq=220 ACK=1528 WIN=61440 Len=0 TSV81=518826648 TSecr=3/206412/0 287 Client Hello
303 13:59:19.232415 192.			TCP	42465	445	
			TLSv1.2	443	42465	68 443 → 42465 [ACK] Seq=1 Ack=220 Win=62464 Len=0 TSval=3720641271 TSecr=318826649
304 13:59:19.233580 192. 305 13:59:19.233586 172.		192.168.56.143	TCP	443	42465	1595 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello D 68 42465 → 443 [ACK] Seq=220 Ack=1528 Win=61440 Len=0 TSval=318826650 TSecr=3720641272
306 13:59:19.248321 172.			TLSv1.2	42465	443	2250 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
307 13:59:19.248378 192.			TCP	42464	445	68 443 → 42464 [ACK] Seg=1528 Ack=2402 Win=60416 Len=0 TSval=3720641287 TSecr=31882666
308 13:59:19.248647 192.			TLSv1.2	445	42464	75 Alert (Level: Fatal, Description: Certificate Expired)
309 13:59:19.248660 172.			TCP	445	42404	68 42464 → 443 [ACK] Seq=2402 Ack=1535 Win=61440 Len=0 TSval=318826665 TSecr=372064128
310 13:59:19.248721 192.			TCP	42404	4445	68 443 → 42464 [FIN, ACK] Seq=1535 Ack=2402 Win=60416 Len=0 TSval=3720641287 TSecr=318
311 13:59:19.248749 192.			ТСР	443	42464	68 443 → 42464 [RST, ACK] Seq=1536 Ack=2402 Win=60416 Len=0 TSval=3720641287 TSecr=318
312 13:59:19.321065 172.		192.168.56.143	TLSv1.2	42465	42404	2250 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
313 13:59:19.321123 192.			TCP	443	42465	68 443 → 42465 [ACK] Seg=1528 Ack=2402 Win=60416 Len=0 TSval=3720641359 TSecr=31882673
314 13:59:19.321393 192.			TLSv1.2	443	42465	75 Alert (Level: Fatal, Description: Certificate Expired)
315 13:59:19.321403 172.		192.168.56.143	TCP	42465	42403	68 42465 → 443 [ACK] Seq=2402 Ack=1535 Win=61440 Len=0 TSval=318826738 TSecr=372064136
316 13:59:19.321449 192.			TCP	443		68 443 → 42465 [FIN, ACK] Seq=1535 ACK=1535 WIN-61446 LEN=0 TSVa1=518828758 TSECI=572864156
10 13.33.13.321	100.30.145	1/2.1/.15.150	TCI	445	42405	
4005 007 1 1	1 (2224)		1 1 (2)			ce unknown, id 0 0000 00 04 00 01 00 06 5e bf 2b 6d f5 9a 00 00 0
ame 1295: 287 bytes on nux cooked capture v1	wire (2296 D	1ts), 287 bytes (	aptured (22	296 DITS) (	on interta	Ice unknown, 1d 0
		47 47 476 8-4-				0020 c0 a8 38 8f a5 e0 01 bb f0 e3 a8 0d c7 5d
ternet Protocol Version ansmission Control Prot						
ansmission Control Prot Source Port: 42464	ocor, src Po	rt: 42464, DST PC	mu: 445, 50	:ч: 1, АСК	: 1, Len:	0040 dd c4 /a t4 16 03 03 00 d6 01 00 00 d2 03 0
Destination Port: 42464						0050 9d c6 77 e2 e4 80 0b 1b 20 0a 12 be d9 f8 b
[Stream index: 28]						0060 4f 58 cb c7 3a 86 dd ec 31 b8 5e 0f a9 71
			11			0070 00 06 00 ff c0 30 c0 2f 01 00 00 a3 00 00 0
[Conversation complete [TCP Segment Len: 219]	ness: comple	ce, wrim_DAIA (65	21			0080 00 30 00 00 2d 6d 74 72 64 6d 63 6e 72 66 0090 2e 64 6d 63 2e 6d 6e 63 30 31 34 2e 6d 63 6e

Figure 20: TC-SBI-03 SBI mTLS Client Hello and Fatal Alerts

#### TLP:GREEN:5GSTB

mTLS_tst-3_b_combined-itc-trace-files_06-29-2	23_1400pm.pcapng				-
ile Edit View Go Capture Analyze St [ 🔳 🙋 💿 🚞 🔚 🔀 💽   🍳 ⇔ 🕾					
tcp.stream eq 28		444			× +
Time Source	Destination	Protocol	Source Por De	estination I L	
1292 13:59:19.229127 172.17.13.136	192.168.56.143	тср	42464	443	76 [TCP Port numbers reused] 42464 $\rightarrow$ 443 [SYN] Seq=0 Win=62720 Len=0 MSS=8960 SACK_PERM TS
1293 13:59:19.229238 192.168.56.143	172.17.13.136	TCP	443	42464	76 443 → 42464 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=3720641268
1294 13:59:19.229247 172.17.13.136	192.168.56.143	TCP	42464	443	68 42464 → 443 [ACK] Seq=1 Ack=1 Win=62720 Len=0 TSval=318826646 TSecr=3720641268
1295 13:59:19.230553 172.17.13.136	192.168.56.143	TLSv1.2	42464	443	287 Client Hello
1296 13:59:19.230584 192.168.56.143		TCP	443	42464	68 443 → 42464 [ACK] Seq=1 Ack=220 Win=62464 Len=0 TSval=3720641269 TSecr=318826647
1300 13:59:19.231772 192.168.56.143		TLSv1.2	443	42464	1595 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
1301 13:59:19.231783 172.17.13.136	192.168.56.143	TCP	42464	443	68 42464 → 443 [ACK] Seq=220 Ack=1528 Win=61440 Len=0 TSval=318826648 TSecr=3720641270
1306 13:59:19.248321 172.17.13.136	192.168.56.143	TLSv1.2	42464	443	2250 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Ha
1307 13:59:19.248378 192.168.56.143		TCP	443	42464	68 443 → 42464 [ACK] Seq=1528 Ack=2402 Win=60416 Len=0 TSval=3720641287 TSecr=318826665
1308 13:59:19.248647 192.168.56.143		TLSv1.2	443	42464	75 Alert (Level: Fatal, Description: Certificate Expired)
1309 13:59:19.248660 172.17.13.136	192.168.56.143	TCP	42464	443	68 42464 → 443 [ACK] Seq=2402 Ack=1535 Win=61440 Len=0 TSval=318826665 TSecr=3720641287
1310 13:59:19.248721 192.168.56.143 1311 13:59:19.248749 192.168.56.143		TCP TCP	443 443	42464 42464	68 443 → 42464 [FIN, ACK] Seq=1535 Ack=2402 Win=60416 Len=0 TSval=3720641287 TSecr=318826 68 443 → 42464 [RST, ACK] Seq=1536 Ack=2402 Win=60416 Len=0 TSval=3720641287 TSecr=318826
					Wireshark · Follow TCP Stream (tcp.stream eq 28) · mTLS_tst-3_b_combined-itc-trace-files_06-29-23_1
Sequence Number (raw): 3344784702 [Next Sequence Number: 1535 (r Acknowledgment Number: 2402 (r Acknowledgment Number: 2402 (r Acknowledgment number (raw): 4041 1000 = Header Length: 32 byt Flags: 0x018 (PSH, ACK) Window: 236 [calculated window size: 60416] [Window size scaling factor: 256] (Lecksum: 0xb2fe [unverified] [Checksum Status: Unverified] [Checksum Status: Unverified] [Checksum Status: Unverified] [Checksum Status: Unverified] [Checksum Status: Unverified] [SeQ/ACK analysis] TCP payload (7 bytes)	e sequence number elative sequence elative ack numbe 453934 es (8)	) number)] r)	Timestamps		<pre>port: 443 packets: packet: 1295 peer: 0 index: 0 if isstand in the isstand isstan</pre>
ransport Layer Security ' TLSv1.2 Record Layer: Alert (Leve Content Type: Alert (21) Version: TLS 1.2 (0x0303) Length: 2 ✓ Alert Message Level: Fatal (2)	l: Fatal, Descrip	tion: Certi	ficate Expir	red)	990EjVsF43T2ZOqu1TgCYp4gX/3TI2McQLTFVO5uSy9R2swjmXKSAnk1jm?5jpxS03pX82 VvG6186p60Kyhogis+H881K7gXXfVHv09cG1980u7p20U1py2G12LTUJvK2jk7K06erLU T14+51bvYnx0t2/vo110=1PRQnYkvGg14Hc1v5u1jXSW2/QUKTwF00q0+HL2Sis Wmip2S32N01g14u04hspg415dH4KXSXUH73HfL68Rdrcncds51Q108Tig0H0MmvhC95HL0Esi RQTDAQABo4SM1G6M4kG3LUdexQCHAaHGYDVR08BYEF0em3Pd+VTIjHBNpspNRdh22- ALUdTwQMBa4F7R7U12pO7jVfsWbWrd52LUdexQCHAAHGYDVR08BYEF0em3Pd+VTIjHBNpspNRdh22- BggrEBgEEBQCAQVTKkyYB80UHAwIu0AYDVR08BDEwL41tbXRvZG1ibnJmVDEuZG1iLm1uY2A
Description: Certificate Exp	pired (45)				2 client pkts, 2 server pkts, 3 turns.

*Figure 21 : TC-SBI-03 mTLS Fatal Alert Details* 

Figure 22: T shows the result of querying the state of the AMF at the NRF around the same time as the fatal alert discussed above. At this time, the AMF is still REGISTERED with the NRF. However, one minute later, re-querying the state indicates the status of the network function has changed to SUSPENDED, as shown in Figure 23: TC-SBI-03 AMF Status at NRF at 14:01 EDTFigure 23.

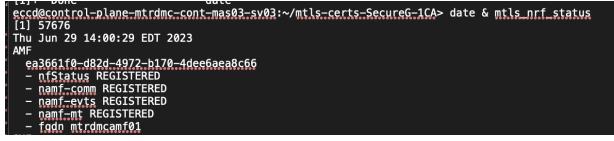


Figure 22: TC-SBI-03 AMF Status at NRF at 14:00 EDT

eccd@control-plane-mtrdmc-cont-mas03-sv03:~/mtls-certs-SecureG-1CA> date & mtls_nrf_status [1] 8551
Thu Jun 29 14:01:25 EDT 2023
AMF
ea3661f0-d82d-4972-b170-4dee6aea8c66
– nfStatus SUSPENDED
– namf-comm REGISTERED
– namf-evts REGISTERED
– namf-mt REGISTERED
- fadn mtrdmcamf01

Figure 23: TC-SBI-03 AMF Status at NRF at 14:01 EDT

#### Success Criteria:

1. Mutual TLS encryption prevents NF with invalid credentials from attaching on the SBI.

#### Results

Condition	Status
Mutual authentication enables NFs with valid	Success: Prior to certificate expiration,
credentials to attach on the SBI	installation is successful; AMF certificate
	shows as VALID; AMF service shows as
	REGISTERED; and encrypted application
	data is exchanged between AMF and NRF.
Mutual authentication prevents NF with invalid	Success: After certificate expiration, AMF
credentials from attaching on the SBI	certificate shows as EXPIRED; AMF service
	shows as SUSPENDED; and TCP connection
	between AMF and NRF is terminated,
	preventing any further data exchange.
Overall Test	Successfully demonstrated that mTLS
	prevents NFs with expired credentials
	from attaching on the network by
	terminating their connections.

### Test Case 4 – Prevent Unknown VNF Attach Request

#### Test Case ID: TC-SBI-04

### Description:

Utilizing the same configuration setup as the previous tests, Test Case 4 is designed to demonstrate mTLS, and to verify that invalid credentials on one end will lead to a failed SBI connection. This will prevent any unwanted network functions from attaching to the network.

#### **Objectives:**

- Demonstrate the ability to authenticate/authorize both sides of an HTTPS connection using mTLS.
- Demonstrate the inability of an NF with invalid credentials to attach to the SBI when mTLS is implemented.

For this test, an alternative Certificate Authority, AMF-root-CA, is installed only on the AMF, and a new certificate signed using that CA is also installed for mTLS authentication. Figure 24 shows the details of the AMF-root-CA, and Figure 25 shows the AMF-root-CA Certificate State as VALID. Figure 26 shows the AMF certificate using the AMF-root-CA, and Figure 27 shows that certificate as VALID on the AMF.

```
[xxx@fgp-dmc-jump tc4]$ openssl x509 -text -in SecureG-tc4-cacert-root.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3099358877564513673 (0x2b03227a60afad89)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: 0=SecureG, CN=AMF-root-CA
        Validity
            Not Before: Jun 22 17:56:00 2023 GMT
            Not After : Jun 22 17:56:00 2025 GMT
        Subject: 0=SecureG, CN=AMF-root-CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
                Modulus:
                     00:d3:da:2c:8a:35:c4:d6:34:44:55:1e:9a:2c:a9:
                     73:5c:da:41:fc:6a:93:10:69:c8:d8:e9:b8:38:0f:
                     d2:52:58:0e:0e:bb:2f:45:c9:c8:75:8a:89:0a:a4:
                     7f:54:62:ec:dd:a9:05:51:e9:c5:fa:7b:16:a3:70:
                    39:11:f1:22:0a:be:1f:80:c0:d3:30:e9:88:df:91:
                     a2:16:0c:c5:ce:b3:1b:98:74:9d:b0:cc:65:0f:d9:
                     cb:6d:99:cb:fe:7d:96:b8:f3:6c:d5:1c:fe:4b:ae:
                    9f:aa:a0:26:85:42:2f:ee:4d:34:69:07:0b:59:ca:
b1:80:37:25:5c:66:6d:ce:9d:dd:e6:77:eb:b0:cc:
12:48:0c:e9:44:73:69:d8:d4:c8:df:a8:0e:3d:d3:
                     70:f2:d2:f4:6d:1d:d5:8e:9c:10:18:69:9a:b2:4a:
                     86:15
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA: TRUE
            X509v3 Subject Key Identifier:
                2E:FD:D9:43:58:B5:17:AA:75:0A:68:92:B7:09:67:B0:1B:A9:04:D4
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
```

Figure 24: TC-SBI-04 CA Certificate Details

Parameter Planned Data	Active Data	
timestamp	20230629211303	
lanState	-	
is (ManagedState)	ENABLED	
c (CertificateContent)	version (Version)	3(0x2)
d 42 27 03 74 b6 2c e0 1 22 0a be 1f 80 c0 d3	94 32 f8 50 da 52 cc 49 4c b0 e9 10 13 98 8c 30 e9 88 df 91 a2 16 0c c5 cc b3 1b 98 74 9c 47 3 69 d8 d4 c8 df a8 0e 3d d3 70 f2 d2 f4 publicKeyAlgorithm (PublicKeyAlgorithm) keyUsage (KeyUsage) extensionContent (ExtensionContent)	0=5ccure6, CN=M4F-root-CA 2023-06-22717:55:00+00:00 2023-06-22717:55:00+00:00 30 62 01 22 30 04 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0 03 82 01 0a 02 82 01 01 00 d3 da 2c 8a 35 c4 d6 34 44 55 1e 9a 4 5 C 02 87 58 a8 90 aa 47 f5 46 2c c3 da 90 55 1e 9c 55 fa 7b 16 a3 70 b8 df 2b 4a 63 23 eb 21 01 a1 7d f5 6a 76 96 51 38 c8 40 4e cc 27 7 0f ef 01 73 11 48 f5 9c 3b 7f 54 7c 4c 2c 73 16 0f c0 73 11 48 f5 9c 3b 7f 54 7c 4c 2c 73 c5 1c 1e 4b ae 9f aa a0 26 85 42 2f ee 4d 34 69 07 0b 59 ca b1 80 77 25 5c 66 6d ce 9d dd 16 d1 dd 58 ec 10 18 65 99 ab 24 38 61 55 0c 38 01 00 01

cs (CertificateState) VALID

*Figure 25 : TC-SBI-04 CA Certificate State* 

[xxx@fgp-dmc-jump tc4]\$ openssl x509 -text -in SecureG-amf-cert.pem Certificate: Data: Version: 3 (0x2) Serial Number: 8911013846515656376 (0x7baa47e17e2726b8) Signature Algorithm: sha256WithRSAEncryption Issuer: O=SecureG, CN=AMF-root-CA Validity Validity Not Before: Jun 22 17:59:00 2023 GMT Not After : Jun 22 17:59:00 2024 GMT Subject: L=Mclean, OU=Mitre, CN=mtrdmcamf01.amf.dmc.mnc014.mcc310.3gppnetwork.org Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) Modulue: Modulus: ulus: 00:a9:ad:b7:55:70:3e:17:2f:48:18:55:f5:3f:16: 5c:13:f9:5a:13:30:ca:a0:8f:2e:1e:db:31:5c:04: 15:56:b2:0c:99:28:9c:d5:b1:9c:97:1f:4e:fd:12: b0:8b:bd:51:10:12:41:1c:8b:da:35:f0:31:1e:34: 0c:40:14:0f:1e:ae:95:f5:43:05:ee:04:8b:49:f5: 8b:a1:0e:91:52:af:76:66:49:f4:89:0c:95:d2:d5: 23:05:72:83:9a:91:da:77:c4:fd:df:63:08:ce:db: ec:35:49:de:8b:cf:4a:20:8f:d5:eb:08:d5:04:44: 68:19:ad:a2:29:b7:6e:3b:3f:72:3b:1e:49:fe:28: 35:98:7d:01:ad:61:35:79:68:77:61:0f:77:c1:ed: f4:aa:01:66:91:37:57:88:34:7e:40:0f:1a:9d:72: 15:56:56:7b:37:06:28:93:10:d4:a4:ca:f0:41:38: 41:38:34:70:01:ad:61:35:79:68:74:64:00:1a:9d:72: f4:aa:01:66:91:37:57:88:34:7e:40:0f:1a:9d:72: f5:56:7b:37:05:70:66:8e:91:10:d4:a4:ca:f0:41:38: f5:56:7b:37:57:80:34:7e:40:0f:1a:9d:72: f5:56:7b:37:7b:37:70:10:6f:8e:91:10:d4:a4:ca:f0:41:38: f5:56:7b:37:55:70:66:8e:91:10:d4:a4:ca:f0:41:38: f5:56:7b:37:7b:37:70:10:d1:36:10:d4:a4:ca:f0:41:38: f5:56:7b:37:7b:37:7b:10:d1:20:41:38: f5:56:7b:37:7b:37:7b:37:7b:30:34:7e:40:0f:1a:9d:72: f5:56:7b:37:7b:37:7b:37:57:30:10:d4:35:7b fc:56:d7:b3:70:d6:8e:9a:10:d4:a4:ca:f0:41:38: 87.3e:ee:e8:cd:8c:84:db:8a:26:55:58:90:99:06: 05:10:ca:f4:92:45:35:83:f6:36:94:e2:b1:8c:48: 1e:f9:10:cd:a3:a8:14:b2:02:89:3a:3b:0f:ac:22: 57.53:20:d8:a7.f0:bb:97:49:7e:9d:0b.31:ad:15: b0:01:f3:ea:47:2:80:58:58:86:c2:50:da:49:ef 9b:01:f3:ea:47:3c:80:58:5a:8e:c2:59:da:49:ef: a6:cf Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 6E:50:F1:88:40:4F:B0:FE:F9:BB:D2:31:35:65:F8:2C:5B:99:4A:97 X509v3 Authority Key Identifier: keyid:2E:FD:D9:43:58:B5:17:AA:75:0A:68:92:B7:09:67:B0:1B:A9:04:D4 X509v3 Key Usage: critical Digital Signature, Key Encipherment X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication X509v3 Subject Alternative Name: DNS:mtrdmcamf@l.amf.dmc.mnc@l4.mcc310.3gppnetwork.org Signature Algorithm: sha256WithRSAEncryption

Figure 26: TC-SBI-04 AMF Certificate Details

=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get\_node\_credential -nci mtlsIC4
Parameter Active Data

TLP:GREEN:5GSTB

Parameter Planned Data	Active para
timestamp	20230629173142
planState	_
ul (UserLabel)	NULL
sn (SubjectName)	L=Mclean,0U=Mitre,ON=mtrdmcamf01.amf.dmc.mnc814.mcc310.3gppnetwork.org
et (EnrollmentTimer)	60
ki (KeyInfo)	R54_2048
ep (EnrollmentProgress)	an (ActionName) installCredentialEropUri
-	adi (AdditionalInfo)         NULL           pi (Progressifino)         NUL           pp (Progressifino)         NUL           resi (Resultinfo)         SUCCESS           resi (Resultinfo)         NULL           si (ActionId)         PINSHED           ai (ActionId)         2423-66-29117:31:42-05:00           tas (TimeActionCompleted)         2423-66-29117:31:42-05:00           tas (TimeActissTistusUpdate)         2423-66-29117:31:42-05:00
rm (RenewalMode)	MANUAL
eat (ExpiryAlarmThreshold)	30
Type (EnrollmentType)	PKC512
cc (CertificateContent)	version (Version) 3(0x2)
8b cf 4a 20 8f d5 eb d8 d5 58 90 99 06 05 10 ca f4 92	serialNumber (SerialNumber)       78AA47E12722688         signatureAlgorithm (SignatureAlgorithm)       0=SecureG, (D=AMF-root-CA         validFrom (ValidFrom)       0=SecureG, (D=AMF-root-CA         validFrom (ValidFrom)       2024-66-2217:59:08+08:08         publickey (Publickey       2024-66-2217:59:08+08:08         validFrom (ValidFrom)       2024-66-2217:59:08+08:08         publickey (Publickey       2024-66-2217:59:08+08:08         validFrom (ValidFrom)       2024-66-2217:59:08+08:16:08         validFrom (ValidFrom)       2024-66-2217:59:08+08:16:08         validFrom (ValidFrom)       2024-66-2217:59:08+08:16:08         validFrom (ValidFrom)       2024-66-2217:20:08         validFrom (ValidFrom)       2024-66-2217:20:08         validFrom (ValidFrom)       2032-86         validFrom (ValidFrom)       2032-86         validFrom (ValidFrom)
cs (CertificateState)	VALID
1. Summary and the state of	

Figure 27: TC-SBI-04 AMF Certificate State

Figure 28 shows the Hello message from the NRF (192.168.56.143) to the AMF (172.17.13.170, where the AMF IP address was re-assigned during a restart of the NF), initiating the key exchange. That message shows the request from the NRF uses the original SecureG Lab Root CA (as can be seen in Error! Reference source not found. for Test Case 3). Figure 29 shows the AMF response to the NRF declaring a fatal alert, indicating an unknown CA on packet 15. Shortly after that fatal alert, we can see the [FIN, ACK] message tearing down the TCP connection.

	• <u>í</u> tc-merge-20230629-213131.	pcapng				
	■ ₫ ⑧ 🖿 🗋 🕺 🗳 🔍 👄 👄 🛎 🚽 其 📃 🔍		••			
App						
No.	Time Source Destination Protocol Length Info					
e						Sval=3409528478 T
						ertificate Reques
						TSval=307692813
						ertificate Reques
						TSval=307692813
			atal, Descr			TC1240052047
1						) TSval=340952847
			atal, Descr			Len=0 TSval=3409
						TSval=340952847
						Len=0 TSval=3409
_	CETTITEALES LENGTH. 302					03 55 04 03 13 12 5
	<ul> <li>Certificates (982 bytes)</li> </ul>					20 52 6f 6f 74 20 43
	Certificate Length: 979		0110	0 1e 17 0o	32 33 30 35	31 34 31 35 33 30 30
	V Certificate: 308203cf308202b7a003020102020807201ae956b66b95300d06092a864886	f70d01010b				34 31 35 33 30 30 30
	v signedCertificate		0130			55 04 06 13 02 55 53 13 06 4d 63 6c 65 63
	version: v3 (2)					0b 13 05 4d 69 74 72
	serialNumber: 0x07201ae956b66b95					03 13 2d 6d 74 72 64
	<ul> <li>signature (sha256WithRSAEncryption)</li> </ul>					6d 63 2e 6d 6e 63 3
	Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)					2e 33 67 70 70 6e 6 30 82 01 22 30 0d 0
	<pre>v issuer: rdnSequence (0)</pre>		01-1			01 05 00 03 82 01 0 <sup>-</sup>
	v rdnSequence: 2 items (id-at-commonName=SecurG Lab Root CA,id-at-org	anizationN				00 9a 89 eb 2a 0b 0
	RDNSequence item: 1 item (id-at-organizationName=SecureG)					4a 71 7a d2 60 93 7 <sup>.</sup>
	RelativeDistinguishedName item (id-at-organizationName=SecureContent)	)	01d0			5b 1f e3 7b 7b 64 ea
	Object Id: 2.5.4.10 (id-at-organizationName)					d3 20 93 28 43 52 1 98 e2 b9 02 79 09 8
	<ul> <li>DirectoryString: printableString (1)</li> </ul>					7f 0e 1b da 0f 56 f:
	printableString: SecureG		0210	ce a9 e8	8 e2 b2 6e a1	bd 8a bf 81 f2 22 bl
	RDNSequence item: 1 item (id-at-commonName=SecurG Lab Root CA)	at (A)	0220			74 df 7c bb ba 73 0
	<ul> <li>RelativeDistinguishedName item (id-at-commonName=SecurG Lab Ro Object Id: 2.5.4.3 (id-at-commonName)</li> </ul>	OL CA)				02 0a da 39 3b 08 d 3e 4b 56 ee 63 0c 5
						9d 89 2f 1a a2 78 3
_	<ul> <li>DirectoryString: printableString (1)</li> <li>printableString: SecurG Lab Root CA</li> </ul>					ed 94 28 8c 1f d0 d4
	validity					3a f3 b3 62 86 16 fa
	<pre>valually v notBefore: utcTime (0)</pre>					21 6a 14 6a 1b 20 a
	utcTime: 2023-05-14 15:30:00 (UTC)					3d c5 1f 5e ba 45 d0 a0 38 73 96 9a f8 42
	$\sim$ notAfter: utcTime (0)					45 02 03 01 00 01 a
	utcTime: 2023-11-14 15:30:00 (UTC)		02c0	30 81 b4	4 30 09 06 03	55 1d 13 04 02 30 00
	<pre>v subject: rdnSequence (0)</pre>					04 14 e7 a6 9f 73 de
	v rdnSequence: 4 items (id-at-commonName=mtrdmcnrf01.dmc.mnc014.mcc31	0.3appnetw				35 17 61 7b 66 7e 30 16 80 14 91 6a c5 3
	<ul> <li>RDNSequence item: 1 item (id-at-countryName=US)</li> </ul>	o. ogppricer				af b4 66 76 d5 40 c
	RelativeDistinguishedName item (id-at-countryName=US)		0310	06 03 55	5 1d 0f 01 01	ff 04 04 03 02 05 a
I	Object Id. 2.5.4.6 (id_at_countriAlama)		0320	06 03 55	5 1d 25 04 16	30 14 06 08 2b 06 03
<i>_</i> ··						

Figure 28: TC-SBI-04 NRF to AMF Key Exchange

TLP:GREEN:5GSTB

5G STB Report Based on CSRIC VII Recommendations

Figure 29: TC-SBI-04 AMF-to-NRF Key Exchange Failure

#### Success Criteria:

1. Mutual authentication prevents an untrusted NF from attaching on the SBI.

## Results

Condition	Status
Certificate signed by new Certificate Authority installed successfully on AMF	<b>Success</b> – Certificate using "AMF-root-CA" successfully installed on AMF.
Handshake between AMF and NRF fails	<b>Success</b> – AMF responds to NRF with "Unknown CA" fatal alert.
Overall Test	Successfully demonstrated that mTLS prevents NFs with invalid credentials from attaching on the SBI.

## Test Case 5 – Implement Multi-Domain mTLS on SBI

#### Test Case ID: TC-SBI-05

#### Description:

Utilizing the same configuration setup as the previous tests, this test case is intended to demonstrate mTLS across security domains, and to verify that mutual TLS sessions can be established across vendor boundaries when the root certificate is bound to different CAs.

### **Objectives:**

Demonstrate the ability to securely implement a 5G core solution based on different vendors.

Demonstrate the ability to use cross-signed certificates to establish trust across the security domains.

As with Figure 2, which showed the network elements in the configuration used for tests cases 1-4, Figure reflects a similar configuration, but with the AMF emphasized as the network function responsible for cross-signing certificates, which is tested in Test Case 5.

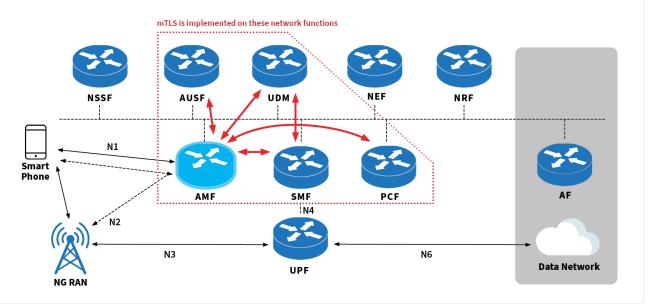


Figure 30: Intra-Network mTLS across Security Domains

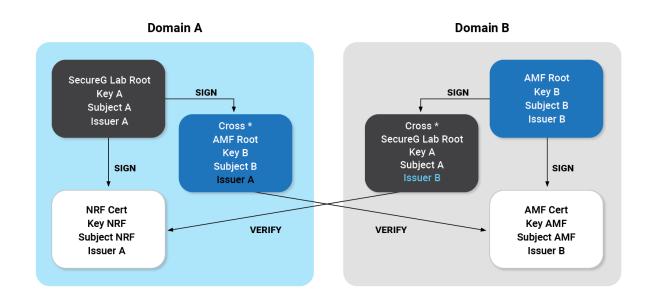


Figure 31: Cross-Signing of Certificates for Intra-Network mTLS

As shown in Figure 31: Cross-Signing of Certificates for Intra-Network mTLS, each root certificate is cross-signed by the other. Specifically, Domain A (corresponding to the Secure G Lab Root certificate and the NRF) uses its root certificate to cross-sign the AMF Root certificate in addition to signing the NRF certificate. Similarly, for Domain B (corresponding to the AMF), the AMF Root certificate cross-signs the Secure G Lab Root certificate in addition to signing the AMF certificate.

Figure 32: NRF Root Issuer and Subject, Figure 33: NRF Cross-Signing of AMF-root-CA, and Figure 34: NRF Certificate Signed by SecureG Lab Root CA show the NRF-related certificates, all with the Issuer listed as "SecurG Lab Root CA" and with the three Subjects listed as "SecurG Lab Root CA," the "AMF-root-CA," and the NRF certificate, respectively. Conversely, Figure 35, Figure 36, and Figure 37 show the AMF certificates, all with the Issuer listed as "AMF-root-CA" and with the three Subjects listed as the "AMF-root-CA," the "SecurG Lab Root CA," and the AMF certificate. Figure 38 then shows the AMF's successful registration with the NRF.

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 2706013596051015078 (0x258db1074dff85a6)
Signature Algorithm: sha256WithRSAEncryption
Issuer: O=SecureG, CN=SecurG Lab Root CA
Validity
Not Before: Mar 6 23:10:00 2023 GMT
Not After : Mar 6 23:10:00 2033 GMT
Subject: O=SecureG, CN=SecurG Lab Root CA
```

*Figure 32: NRF Root Issuer and Subject* 

Certificate: Data: Version: 3 (0x2) Serial Number: 2147267338593882708 (0x1dcca0448aafd254) Signature Algorithm: sha256WithRSAEncryption Issuer: O=SecureG, CN=SecurG Lab Root CA Validity Not Before: Jul 6 21:34:00 2023 GMT Not After : Jul 6 21:34:00 2024 GMT Subject: O=SecureG, CN=AMF-root-CA

Figure 33: NRF Cross-Signing of AMF-root-CA

Certificate: Data: Version: 3 (0x2) Serial Number: 513439947004734357 (0x7201ae956b66b95) Signature Algorithm: sha256WithRSAEncryption Issuer: O=SecureG, CN=SecurG Lab Root CA Validity Not Before: May 14 15:30:00 2023 GMT Not After : Nov 14 15:30:00 2023 GMT Not After : Nov 14 15:30:00 2023 GMT Subject: C=US, L=Mclean, OU=Mitre, CN=mtrdmcnrf01.dmc,mnc014,mcc310.3gppnetwork.org

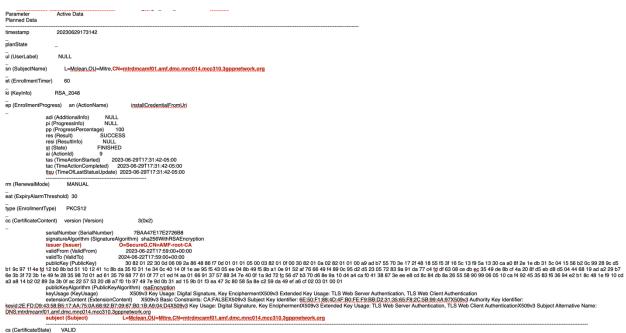
Figure 34: NRF Certificate Signed by SecureG Lab Root CA

Parameter Active Data Planned Data	
timestamp 20230629211303	
planState _	
m (ManagedState) ENABLED	
co (CertificateContent)         3(0x2)           -         serialNumber (SerialNumber)         2803227460AF089           -         signatureAgorithm)         base of the Second Content)         9000000000000000000000000000000000000	b5
keyUsage (KeyUsage) X509/3 Key Usage: Certificate Sign, CRL Sign extensionContent (ExtensionContent) X509/3 Basic Constraints: CA:TRUEX509/3 Subject Key Identifier: <u>2E:FD:D9:43:58:B5:17:AA:75:0A:68:92:87:09:67:80:1B:A9:04:D4X509/3</u> Key Usage: Certificate Sign, CRL Sign subject (Subject) O=SecureG, CN=AMF-root-CA	
cs (CertificateState) VALID	

Figure 35: AMF Root Issuer and Subject

Parameter Active Data Planned Data
timestamp 20230713135655
planState _
me (ManagedState) ENABLED
C (CertificateContent) version (Version) 3(0x2)
<ul> <li>serialkunder (Serialkunder)</li> <li>SF (0572250016F34)</li> <li>SignaturAgorythmi (SignaturAgorythmi (SignaturAgorythmi) (Si</li></ul>

Figure 36: AMF Cross-signing of SecureG Lab Root CA



cs (CertificateState) VALID

Figure 37: AMF Certificate Signed by AMF-root-CA



Figure 38: AMF Registration Status

Confidential and Proprietary to the 5G Security Test Bed – Not for Disclosure

Figure 39 through Figure 41 show Wireshark windows interpreting the messages captured on the SBI through the ITC traces. Specifically, Figure 39 shows the NRF sharing its certificate with the AMF through server Hello, Certificate, and Key Exchange messages. We can verify the common name, serial number, and issuer from Figure 34. Figure 40 and Figure 40 show the AMF's response with its certificates, including both the AMF certificate (Figure 40), matching parameters shown originally in **Error! Reference source not found.**, and the AMF root certificate (Figure 41), displaying the certificate parameters from Figure 35. We also see in Figure 41 the finalization of the handshake and the ability to exchange encrypted application data between the AMF and NRF.

•			d mTLS_tc	5_combined-ite	_20230713-	-143836.pcapng
	o 🗙 🗂 🗖 🕲 🚺	5 Q 🍝 🛋	🖮 🛣 🕹 🖡			Π
oph	y a display filter <%/>					
PER /	Time	Source	Destination	Protocol	Length	Info
	132 2023-07-13 13.30.43.2373		132.100.30.143	TCD		AA2 A2464 [ACK] Con-1 Adv-220 Win-62464 Lon-0 Towel-200202206 Tower
	133 2023-07-13 15:38:45.2579		172.17.13.170	TCP		443 → 42464 [ACK] Seq=1 Ack=220 Win=62464 Len=0 TSval=299393386 TSecr
	134 2023-07-13 15:38:45.2588 135 2023-07-13 15:38:45.2588		192.168.56.143 172.17.13.170	TLSv1.2 TCP		Client Hello 443 → 42465 [ACK] Sea=1 Ack=220 Win=62464 Len=0 TSval=299393387 TSecr
	136 2023-07-13 15:38:45.2588		172.17.13.170	TLSv1.2		Server Hello, Certificate, Server Key Exchange, Certificate Request,
	137 2023-07-13 15:38:45.2591		192.168.56.143	ТСР		42464 → 443 [ACK] Seg=220 Ack=1572 Win=61184 Len=0 TSval=4261760336 T
	138 2023-07-13 15:38:45.2614		172.17.13.170	TLSv1.2		Server Hello, Certificate, Server Key Exchange, Certificate Request,
	139 2023-07-13 15:38:45.2614		192.168.56.143	TCP		42465 → 443 [ACK] Seq=220 Ack=1572 Win=61184 Len=0 TSval=4261760339 T
	140 2023-07-13 15:38:45.2658		192.168.12.34	SCTP		SACK (Ack=0, Arwnd=32768)
	141 2023-07-13 15:38:45.2659		192.168.12.26	SCTP		SACK (Ack=0, Arwnd=32768)
	142 2023-07-13 15:38:45.2679		10.220.67.18	SCTP		SACK (Ack=0, Arwnd=32768)
	143 2023-07-13 15:38:45.2694	192.168.56.146	192.168.56.33	DIAMETER	292	<pre>cmd=Capabilities-Exchange Answer(257) flags= appl=Diameter Common</pre>
	144 2023-07-13 15:38:45.2695	192.168.56.33	192.168.56.146	SCTP	64	SACK (Ack=0, Arwnd=32768)
	145 2023-07-13 15:38:45.2709	10.205.67.206	192.168.255.226	SCTP	64	SACK (Ack=0, Arwnd=32768)
	146 2023-07-13 15:38:45.3117	172.17.13.170	192.168.56.143	TLSv1.2	2243	Certificate, Client Key Exchange, Certificate Verify, Change Cipher S
	147 2023-07-13 15:38:45.3118	192.168.56.143	172.17.13.170	TCP	68	443 → 42465 [ACK] Seq=1572 Ack=2395 Win=60416 Len=0 TSval=299393440 T
	148 2023-07-13 15:38:45.3123	192.168.56.143	172.17.13.170	TLSv1.2	119	Change Cipher Spec, Encrypted Handshake Message
	Certificate Length: 979					
	<ul> <li>Certificate: 308203cf308</li> </ul>	202b7a00302010202	0807201ae956b66b95	300d06092a86	4886f70d010	010b (id-at-commonName=mtrdmcnrf01.dmc.mnc014.mcc310.3gppnetwork.org,i
	v signedCertificate					
	version: v3 (2)					
	serialNumber: 0x072					
	✓ signature (sha256W1		a i constanti	222 12		
			11 (sha256WithRSAE	ncryption)		
	<pre>v issuer: rdnSequence</pre>					
			nName=SecurG Lab R		organizatio	onName=SecureG)
			-organizationName=			
			em (id-at-organiza -organizationName)		ireg)	
	2	String: printable	-	, ,		
		bleString: Secure				
			-commonName=Secur	Lab Root CA	1	
			em (id-at-commonNa			
		1: 2.5.4.3 (id-at-		Inc-Securo Lui	HOUL CH	
		String: printable				
		bleString: SecurG				
	<pre>v validity</pre>	thangt becard				
	<pre>v notBefore: utcTin</pre>	me (0)				
		05-14 15:30:00 (1	ITC)			
	<pre>v notAfter: utcTime</pre>		80.270f.0			

Figure 39: NRF to AMF Server Hello, Certificate Exchange

			d mTLS_tc	5_combined-it	c_20230713-	-143836.pcapng
	1 🛛 🗖 🏹	ଅ 🔍 🝝 🕳	😟 🛪 🔸 🛙			Π
oply a	display filter <¥/>					•
	Time	Source	Destination	Protocol	Length	Info
14	3 2023-07-13 15:38:45.2694	192,168,56,146	192.168.56.33	DIAMETER	292	<pre>cmd=Capabilities-Exchange Answer(257) flags= appl=Diameter Comm</pre>
	4 2023-07-13 15:38:45.2695		192.168.56.146	SCTP		SACK (Ack=0, Arwnd=32768)
14	15 2023-07-13 15:38:45.2709	10.205.67.206	192.168.255.226	SCTP	64	SACK (Ack=0, Arwnd=32768)
14	6 2023-07-13 15:38:45.3117	172.17.13.170	192.168.56.143	TLSv1.2	2243	Certificate, Client Key Exchange, Certificate Verify, Change Cipher
14	7 2023-07-13 15:38:45.3118	192.168.56.143	172.17.13.170	TCP	68	443 → 42465 [ACK] Seq=1572 Ack=2395 Win=60416 Len=0 TSval=299393440
14	48 2023-07-13 15:38:45.3123	192.168.56.143	172.17.13.170	TLSv1.2	119	Change Cipher Spec, Encrypted Handshake Message
14	9 2023-07-13 15:38:45.3123	172.17.13.170	192.168.56.143	TCP	68	42465 → 443 [ACK] Seq=2395 Ack=1623 Win=61184 Len=0 TSval=426176039
15	0 2023-07-13 15:38:45.3127	172.17.13.170	192.168.56.143	TLSv1.2	149	Application Data
15	i 2023-07-13 15:38:45.3127	192.168.56.143	172.17.13.170	TCP	68	443 → 42465 [ACK] Seq=1623 Ack=2476 Win=60416 Len=0 TSval=299393441
	2 2023-07-13 15:38:45.3128		172.17.13.170	TLSv1.2		Application Data
15	3 2023-07-13 15:38:45.3128	172.17.13.170	192.168.56.143	TCP	68	42465 → 443 [ACK] Seq=2476 Ack=1707 Win=61184 Len=0 TSval=426176039
	4 2023-07-13 15:38:45.3130		192.168.56.143	TLSv1.2		Application Data
	5 2023-07-13 15:38:45.3130		172.17.13.170	TCP		443 → 42465 [ACK] Seq=1707 Ack=2514 Win=60416 Len=0 TSval=299393441
15	6 2023-07-13 15:38:45.3137	172.17.13.170	192.168.56.143	TLSv1.2		Application Data
	i7 2023-07-13 15:38:45.3137		172.17.13.170	TCP		443 → 42465 [ACK] Seq=1707 Ack=2660 Win=60416 Len=0 TSval=299393442
15	8 2023-07-13 15:38:45.3138	172.17.13.170	192.168.56.143	TLSv1.2	2146	Application Data
	Certificates (1/68 bytes)					
	Certificate Length: 970					
		8202aea00302010202	087baa47e17e2726b8	300d06092a86	4886f70d010	010b id-at-commonName=mtrdmcamf01.amf.dmc.mnc014.mcc310.3gppnetwork
	<ul> <li>signedCertificate</li> </ul>					
	version: v3 (2)					
	serialNumber: 0x7b					
	<ul> <li>signature (sha256W)</li> </ul>		o wa north totalo	17 B		
		2.840.113549.1.1.1	.1 (sha256WithRSAE	ncryption)		
	<pre>v issuer: rdnSequence</pre>		and the second			
		items (id-at-commor			zationName=	SecureG)
		tem: 1 item (id-at				
		stinguishedName ite			ureG)	
		d: 2.5.4.10 (id-at				
		yString: printable				
		ableString: Secure		-+ (1)		
		tem: 1 item (id-at				
		stinguishedName ite		me=AMF-root-	LA)	
		d: 2.5.4.3 (id-at-				
		yString: printable				
		ableString: AMF-roo	JI-LA			
	validity	(0)				
	v notBefore: utcTi		TC)			
		-06-22 17:59:00 (U	10)			
	v notAfter: utcTim	ne (0)				

Figure 40: AMF to NRF Certificate Exchange: AMF Certificate

				🚄 mTLS_tc	5_combined-it	c_20230713-	143836.pcapng
	a 💿 🗖		ै ९ 🔶 🔿	🖮 🐺 👲 🗖			Ŧ
Apply a	display filter < \#/>					•••	•
	Time		Source	Destination	Protocol	Length	Info
14	3 2023-07-13 15	:38:45.2694	192.168.56.146	192.168.56.33	DIAMETER	292	<pre>cmd=Capabilities-Exchange Answer(257) flags= appl=Diameter Common</pre>
14	4 2023-07-13 15	:38:45.2695	192.168.56.33	192.168.56.146	SCTP	64	SACK (Ack=0, Arwnd=32768)
14	5 2023-07-13 15	:38:45.2709	10.205.67.206	192.168.255.226	SCTP	64	SACK (Ack=0, Arwnd=32768)
14	6 2023-07-13 15	:38:45.3117	172.17.13.170	192.168.56.143	TLSv1.2		Certificate, Client Key Exchange, Certificate Verify, Change Cipher S
14	7 2023-07-13 15	:38:45.3118	192.168.56.143	172.17.13.170	TCP	68	443 → 42465 [ACK] Seq=1572 Ack=2395 Win=60416 Len=0 TSval=299393440 T
14	8 2023-07-13 15	:38:45.3123	192.168.56.143	172.17.13.170	TLSv1.2		Change Cipher Spec, Encrypted Handshake Message
	9 2023-07-13 15			192.168.56.143	тср		42465 $\rightarrow$ 443 [ACK] Seq=2395 Ack=1623 Win=61184 Len=0 TSval=4261760390
	0 2023-07-13 15			192.168.56.143	TLSv1.2		Application Data
15	51 2023-07-13 15	:38:45.3127	192.168.56.143	172.17.13.170	тср		443 → 42465 [ACK] Seq=1623 Ack=2476 Win=60416 Len=0 TSval=299393441
	52 2023-07-13 15			172.17.13.170	TLSv1.2		Application Data
	53 2023-07-13 15			192.168.56.143	TCP		42465 → 443 [ACK] Seq=2476 Ack=1707 Win=61184 Len=0 TSval=4261760390
	54 2023-07-13 15			192.168.56.143	TLSv1.2		Application Data
	5 2023-07-13 15			172.17.13.170	TCP		443 → 42465 [ACK] Seq=1707 Ack=2514 Win=60416 Len=0 TSval=299393441
	6 2023-07-13 15			192.168.56.143	TLSv1.2		Application Data
	57 2023-07-13 15			172.17.13.170	TCP		443 → 42465 [ACK] Seq=1707 Ack=2660 Win=60416 Len=0 TSval=299393442
15	8 2023-07-13 15	:38:45.3138	172.17.13.170	192.168.56.143	TLSv1.2	2146	Application Data
	encrypte	d: 60752f5705	c10b9ce8dcf63f2231	.3734766360be6610c3	30bf23dd52764	4032fe61ba5	:566
	Certificate	Length: 792					
	<ul> <li>Certificate</li> </ul>	: 30820314308	3201fca00302010202	082b03227a60afad89	300d06092a86	4886f70d010	10b (id-at-commonName=AMF-root-CA,id-at-organizationName=SecureG)
	<pre>v signedCe</pre>	rtificate					
		n: v3 (2)					
			03227a60afad89				
			ithRSAEncryption)				
				1 (sha256WithRSAE	ncryption)		
		: rdnSequence					
				Name=AMF-root-CA,		zationName=	SecureG)
	V RDNSequence item: 1 item (id-at-organizationName=SecureG)						
	V RelativeDistinguishedName item (id-at-organizationName=SecureG)						
	`					ureG)	
	``	Object I	d: 2.5.4.10 (id-at	-organizationName)		ureG)	
	`	Object I √ Director	d: 2.5.4.10 (id–at yString: printable	-organizationName) String (1)		ureG)	
		Object I ∨ Director printa	d: 2.5.4.10 (id–at yString: printable bbleString: Secure	-organizationName) String (1) 5	)	ureG)	
	~ F	Object I ∨ Director printa DNSequence it	d: 2.5.4.10 (id-at yString: printable ableString: Secure tem: 1 item (id-at	-organizationName) String (1) G -commonName=AMF-ro	) Dot-CA)		
	~ F	Object Io Directory printa DNSequence in RelativeDis	d: 2.5.4.10 (id-at yString: printable ableString: Secure tem: 1 item (id-at stinguishedName ite	-organizationName) String (1) G -commonName=AMF-rc em (id-at-commonName	) Dot-CA)		
	~ F	Object I Directory printa DNSequence it RelativeDis Object I	d: 2.5.4.10 (id-at yString: printable ubleString: Secure tem: 1 item (id-at tinguishedName ite d: 2.5.4.3 (id-at-	-organizationName) String (1) G -commonName=AMF-rc em (id-at-commonName)	) Dot-CA)		
	~ F	Object I Object I printa DNSequence it RelativeDis Object I Object I	d: 2.5.4.10 (id-at yString: printable ubleString: Secure tem: 1 item (id-at tringuishedName it d: 2.5.4.3 (id-at- yString: printable	-organizationName) String (1) 5 -commonName=AMF-rc em (id-at-commonName) String (1)	) Dot-CA)		
	~ F	Object In Directory printa DNSequence in RelativeDis Object In Directory printa	d: 2.5.4.10 (id-at yString: printable ubleString: Secure tem: 1 item (id-at tinguishedName ite d: 2.5.4.3 (id-at-	-organizationName) String (1) 5 -commonName=AMF-rc em (id-at-commonName) String (1)	) Dot-CA)		
	√ F √ validi	Object I v Directory printa DNSequence if v RelativeDis Object I v Directory printa ty	d: 2.5.4.10 (id-at ystring: printable ableString: Secure tem: 1 item (id-at stinguishedName ite d: 2.5.4.3 (id-at- yString: printable ableString: AMF-roo	-organizationName) String (1) 5 -commonName=AMF-rc em (id-at-commonName) String (1)	) Dot-CA)		
	✓ F ✓ validi ✓ voti	Object I Directory printa DNSequence i RelativeDis Object I Directory printa ty Before: utcTi	d: 2.5.4.10 (id-at ystring: printable ableString: Secure tem: 1 item (id-at stinguishedName ite d: 2.5.4.3 (id-at- yString: printable ableString: AMF-roo	-organizationName) String (1) 5 -commonName=AMF-rc mm (id-at-commonNa commonName) String (1) String (1)	) Dot-CA)		

Figure 41: AMF to NRF Certificate Exchange: AMF-root-CA

#### Success Criteria:

1. Mutual authentication succeeds with certificates provided from separate root CAs.

### Results

Condition	Status
Mutual authentication succeeds with certificates provided from separate root CAs	Success - Clients were able to exchange keys from separate root CAs, resulting in encrypted application data flowing between AMF and NRF.
Overall Test	Successfully demonstrated that mTLS works across security domains and vendor boundaries when the NF certificates come from different CAs.

# **Conclusions and Next Steps**

This initial set of tests focusing on the 5G SBI successfully demonstrated the efficacy of mTLS encrypting communications among network functions. The five test cases incrementally illustrated mTLS security features, ranging from protecting sensitive information on the SBI to requiring valid credentials for connections between network functions.

Test Case 1 showed that, in the event of a network breach, information within the network can be vulnerable to exposure. Specifically, the test identified a range of sensitive information that could be obtained and exploited by an entity observing traffic on the SBI. The observable information includes UE data such as the IMSI/SUPI, IMEISV, and the Cell ID to which the UE is attached; it also includes information that can enable mapping the network functions in the core, such as IP addresses of the different functions.

Test Case 2 confirmed the effect of mutual authentication and encryption among network functions using mTLS. The sensitive UE information that was viewable in Test Case 1 becomes inaccessible in Test Case 2 due to the mTLS encryption. In addition, while IP addresses are still visible, their association with specific network functions is obscured with the use of mTLS.

Test Case 3 demonstrated the ability of the system to identify and reject connections initiated by expired certificates. In the case tested, a certificate was valid when installed, but then expired at a time specified as part of the certificate. The test showed how the system detects the invalidity of the certificate after the expiration time and rejects new connections initiated by the network function with the expired certificate.

Test Case 4 then explores the situation in which a certificate is deemed valid on the network function on which it is installed (in this test, as a result of installing the corresponding root certificate on that same network function), but it is not valid on other network functions because they use a different root certificate. The test clearly shows that despite each certificate being valid on its host network function, the mTLS connection is rejected because trust has not been established between the network functions.

Finally, Test Case 5 cross-signs the certificates on the different network functions, establishing the trust that was lacking in Test Case 4. The test results show that the cross-signing enables sharing of certificates in such a way as to enable the successful mTLS connection, verifying authenticity of the participating network functions and enabling protection of the traffic between them.

All five tests were successful, verifying the CSRIC VII recommendation to implement mutually authenticated transport layer security to enhance 5G security. The mTLS ability to authenticate the validity of network functions that attempt to connect to an SBI, while restricting access to the network from invalid network functions, demonstrates its value as a foundational component of Zero Trust. Together, this round of tests verify the important role mTLS can play as a Zero Trust enabler.

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 (<u>hpunjabi@ctia.org</u>; (202) 845-5701), or visit <u>https://5gsecuritytestbed.com/</u>.

# Appendix: Acronyms

3GPP	3rd Generation Partnership Project
5G STB	5G Security Test Bed
AMF	Access and Mobility Management Function
BBU	Baseband Unit
CA	Certificate Authority
CSRIC	Communications Security, Reliability, and Interoperability Council
DHS	Department of Homeland Security
DMC	Dual-Mode Core
eMBB	Enhanced Mobile Broadband
FCC	Federal Communications Commission
IMEISV	International Mobile Station Equipment Identity Software Version
IPsec	Internet Protocol Security
ITC	Integrated Traffic Capture
ITU	International Telecommunications Union
mTLS	Mutual Transport Layer Security
NF	Network Function
NIST	National Institute of Standards and Technology
NR	New Radio
PCAP	Packet Capture
PCC	Packet Core Controller
RAN	Radio Access Network
SBA	Service-Based Architecture
SBI	Service-Based Interface
SUPI	Subscription Permanent Identifier
TAC	Technical Advisory Committee

Confidential and Proprietary to the 5G Security Test Bed – Not for Disclosure

TLS	Transport Layer Security
ТР	Test Point
UDM	Unified Data Management
UE	User Equipment
UMD	University of Maryland
VNF	Virtual Network Function
WG	Working Group
ZT	Zero Trust
ZTA	Zero Trust Architecture