5G SECURITY TEST BED™

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 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 3rd 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
    - Protecting Information in Transit
    - Roaming Security
    - Subscriber Privacy
    - Zero Trust Network Security
    - False Base Station Detection and Protection
    - 5G Cloud Network Security

- Secondary Use Cases: Devices and Applications
    - High-Resolution Video Surveillance (e.g. Smart Cities, Large Venues)
    - LTE/5G Drones with High-Resolution Video Feedback (e.g. Smart Cities)
    - Dynamic Supply Chain Verification (Real-Time Monitoring and Logistics)
    - Automated, Reconfigurable Factories
    - Autonomous Vehicles
    - 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

Service-Based Architecture and Mutual Transport Layer Security. 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.[1]

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).

Testing SBA Domain Security as Part of Zero Trust. 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.[2] The Office of Management and Budget followed up with additional guidance for federal agencies that included requirements to encrypt network traffic.[3] 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.[4]

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*.[5]

---

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

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

[3] OMB, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, M-22-09, (Jan. 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[4] NIST, SP 800-207, Zero Trust Architecture, at 8 (Aug. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

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

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*.[6] 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:

[6] CSRIC VII WG3, Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security (Mar. 2021), https://www.fcc.gov/file/20606/download.

1. Demonstrate Clear SBI Vulnerabilities:
    a. 5G STB Test Case 1: 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. 5G STB Test Case 2: 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. 5G STB Test Case 3: 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. 5G STB Test Case 4-: 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. 5G STB Test Case 5: 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.

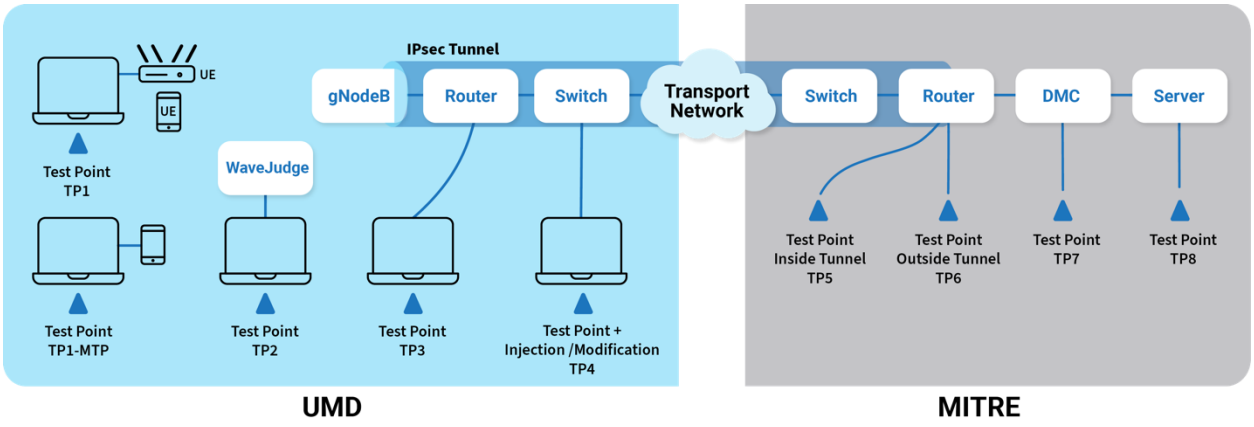

Figure 1: 5G STB Lab Component Block Diagram and Test Points

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.

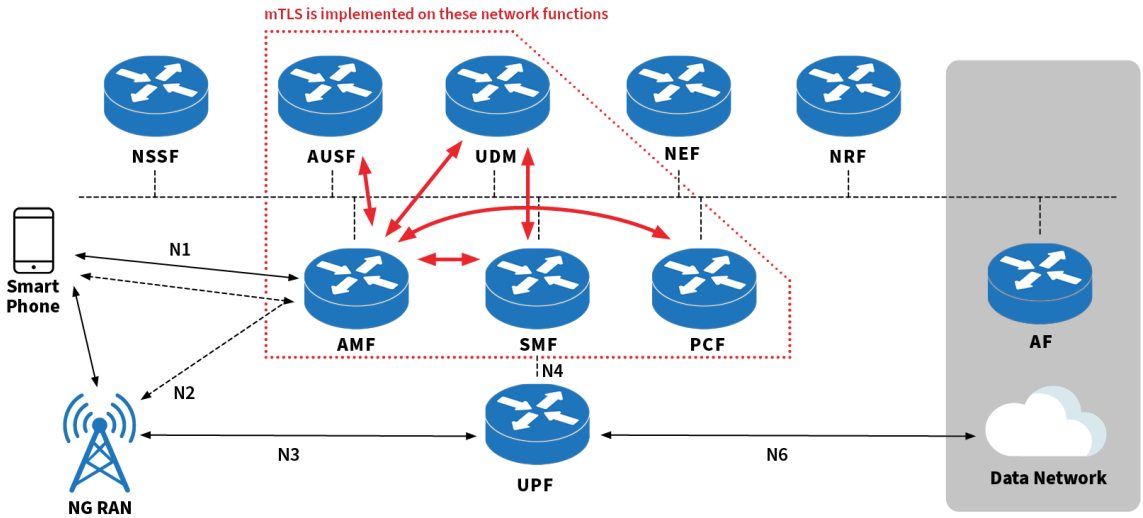

Figure 2: Basic UE Attach and PDU Request on SBI

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

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

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:
    - User information
    - Device information
    - Location information
    - 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.

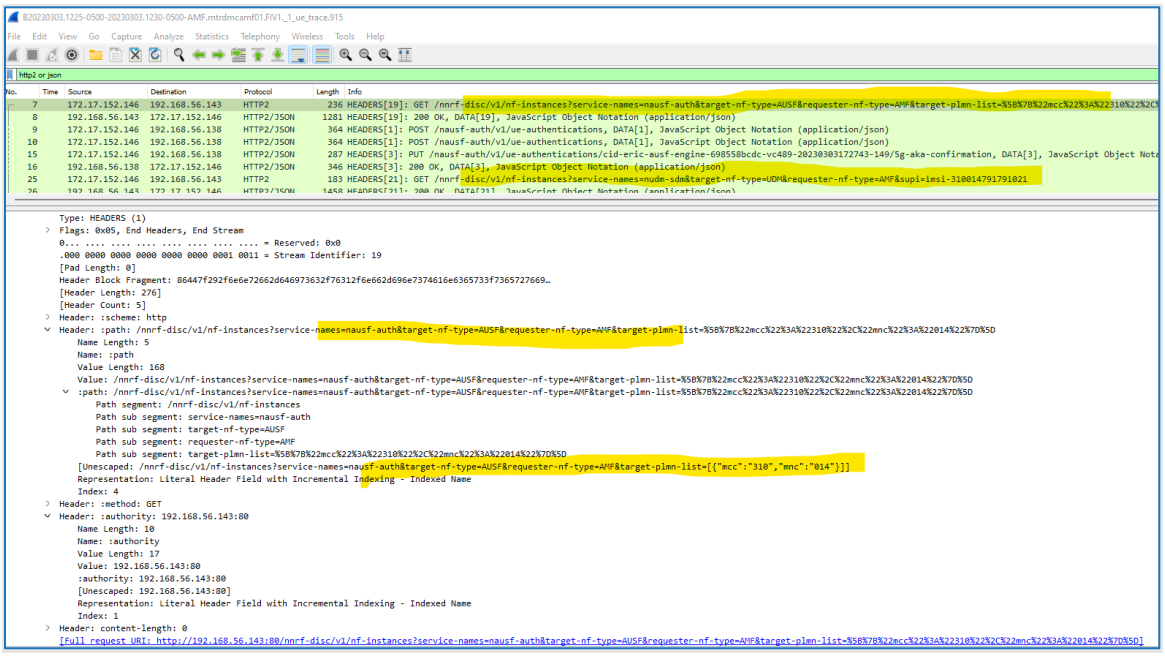

Figure 3: Wireshark window showing UE trace with AMF request for AUSF services

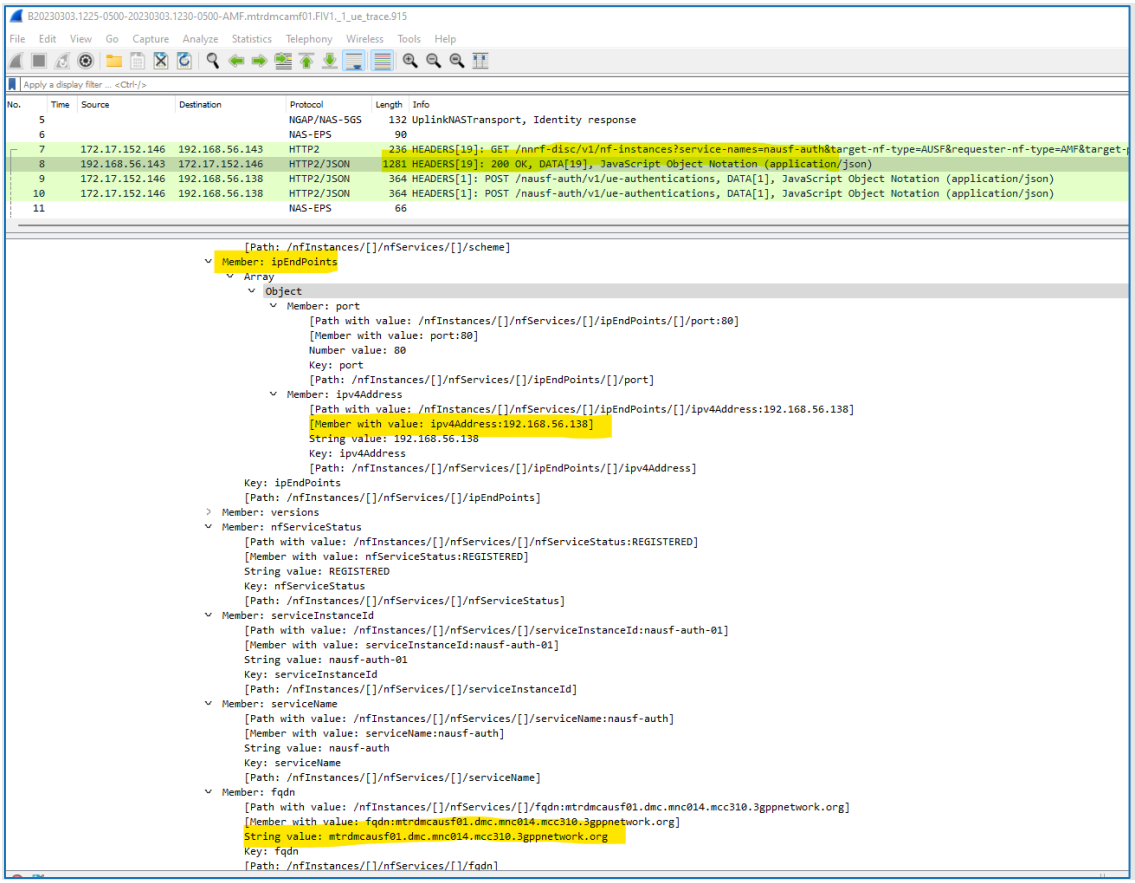

Figure 4: Wireshark window showing UE trace with NRF response to AMF request for AUSF services

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[7] (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.

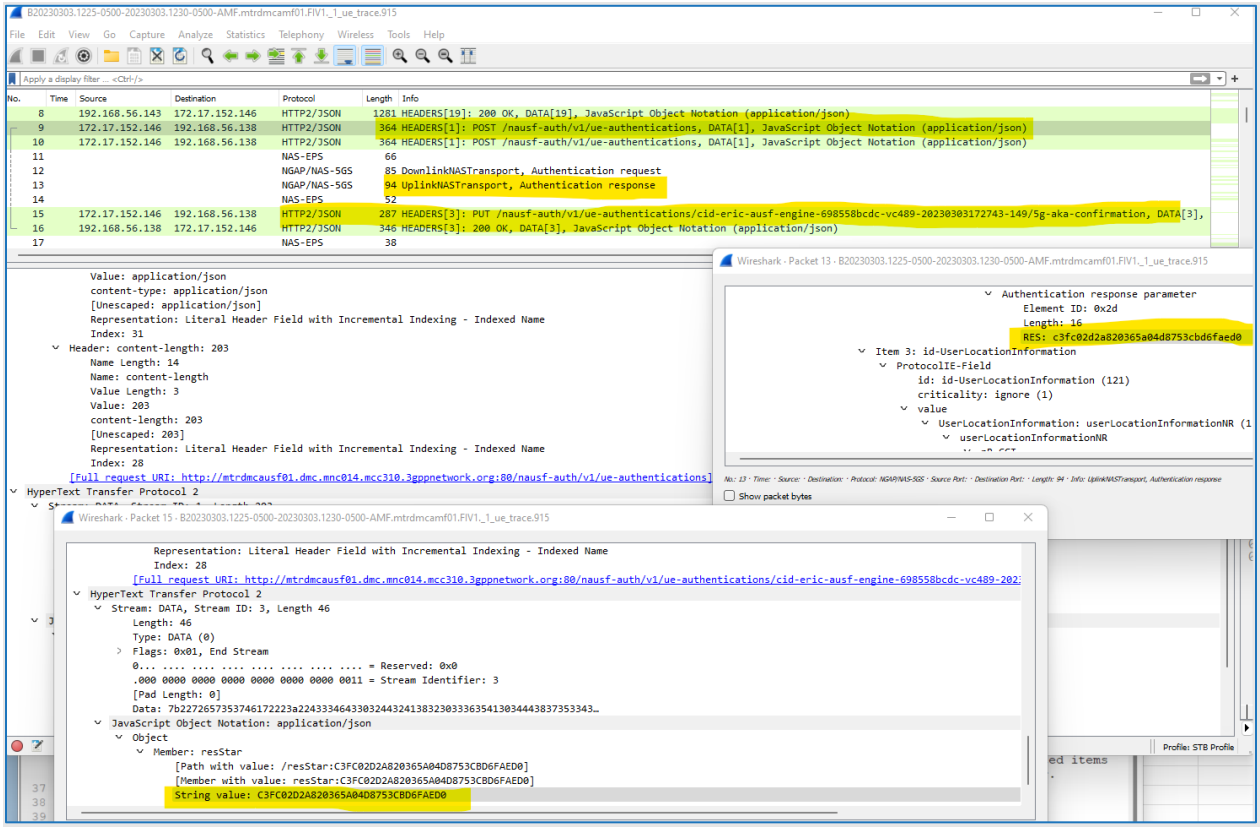

Figure 5: AMF initialization of UE authentication

[7] "NAS signaling" carries the user data from the user equipment to the MME through the S1 pathway.

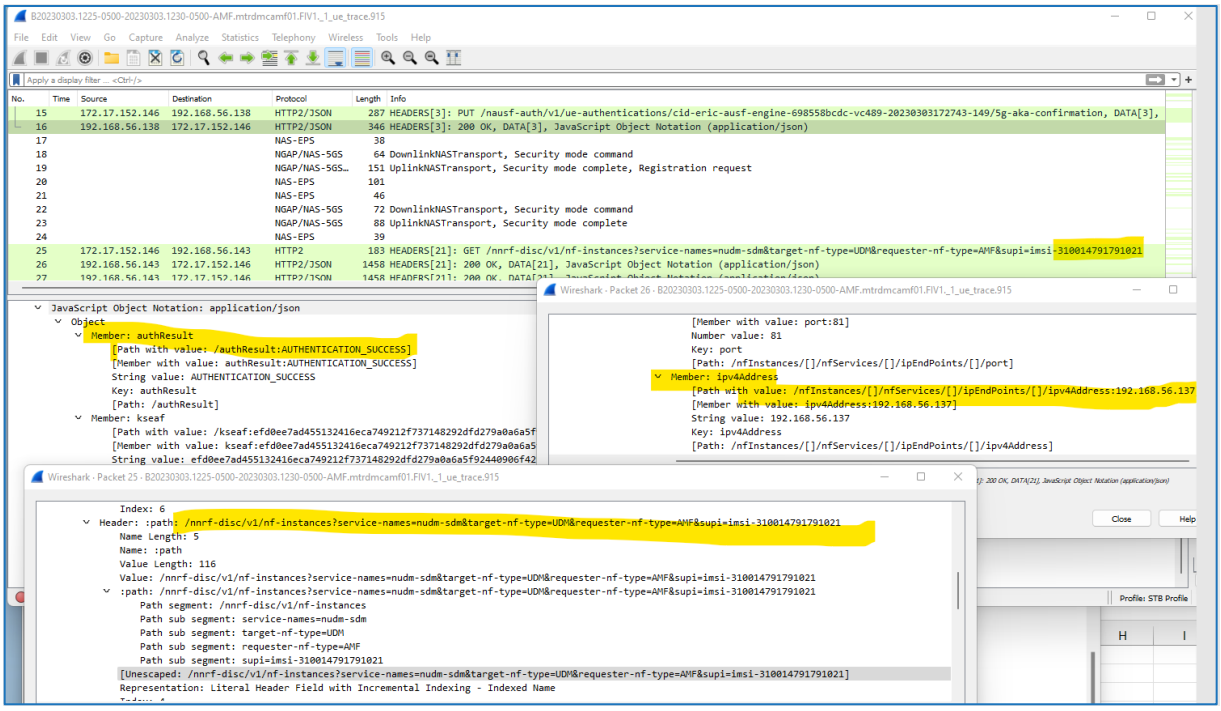

Figure 6: Wireshark window of UE trace showing UDM IP address

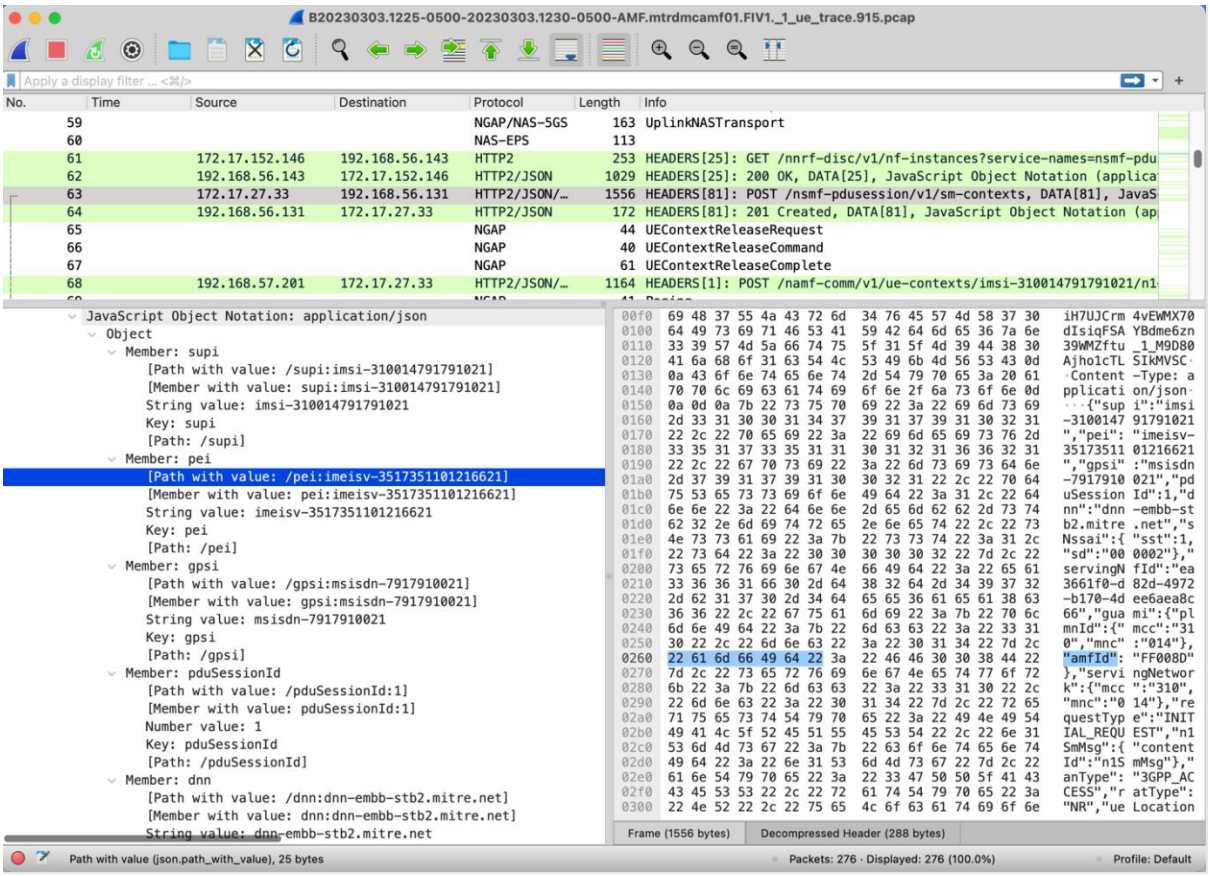

Figure 7: Wireshark UE trace showing UE PEI: SUPI, IMEISV

Table 2: Network Function IP Addresses identified in UE Trace

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

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.

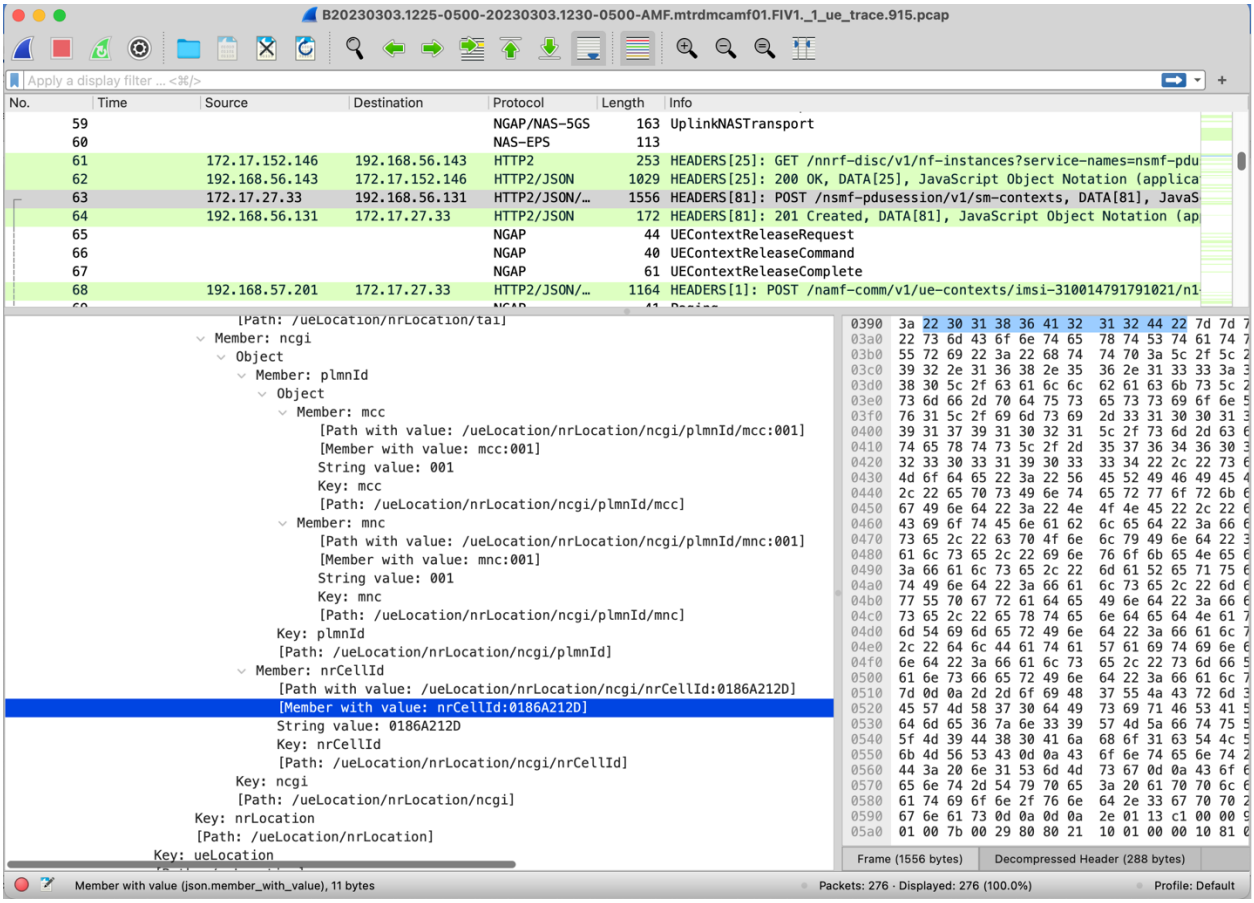

Figure 8: Wireshark UE Trace showing NR Cell ID

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.

Results

Condition	Status
Able to eavesdrop on SBA interfaces	**Success:** HTTP2 and other messages are decipherable.
Able to capture device/user/connection specific information, specifically SUPI, IMEISV, and NR Cell ID	**Success:** Identified SUPI, IMEISV, and NR Cell ID in PDU Establishment message.
Able to capture network information, specifically AMF, SMF, NRF, and AUSF IP addresses	**Success:** Identified 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.

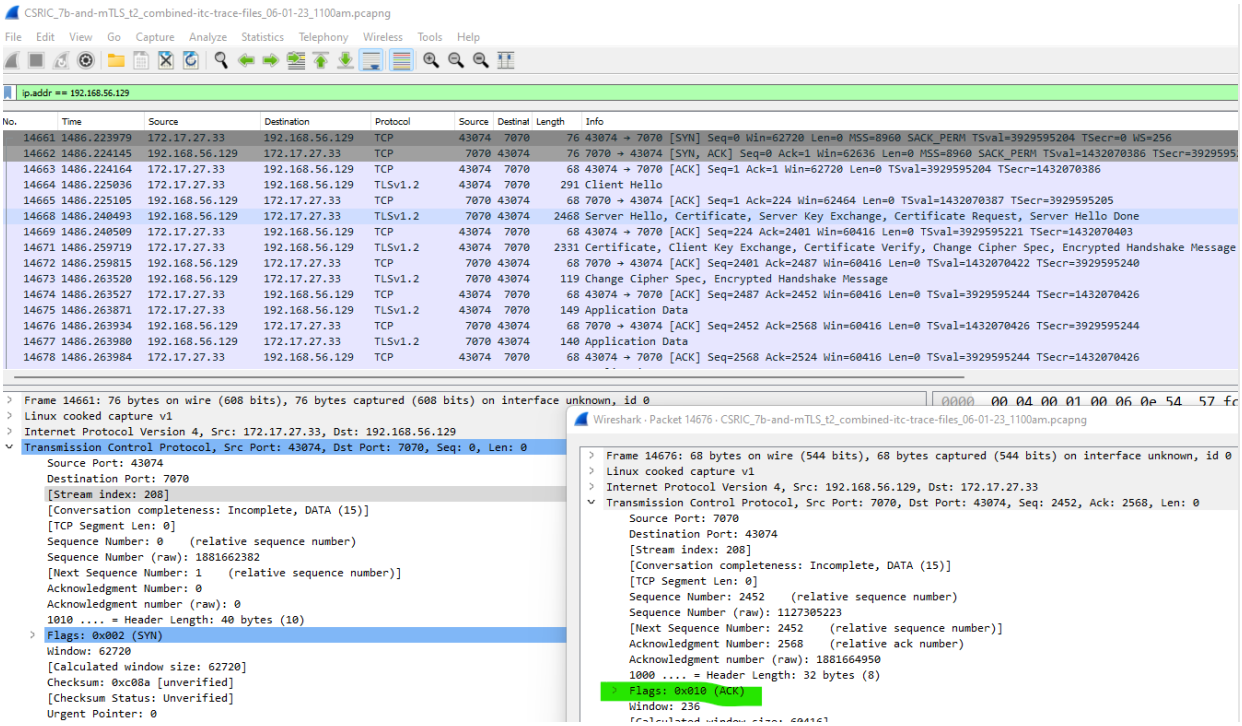

Figure 9: TCP session establishment for TC-SBI-02

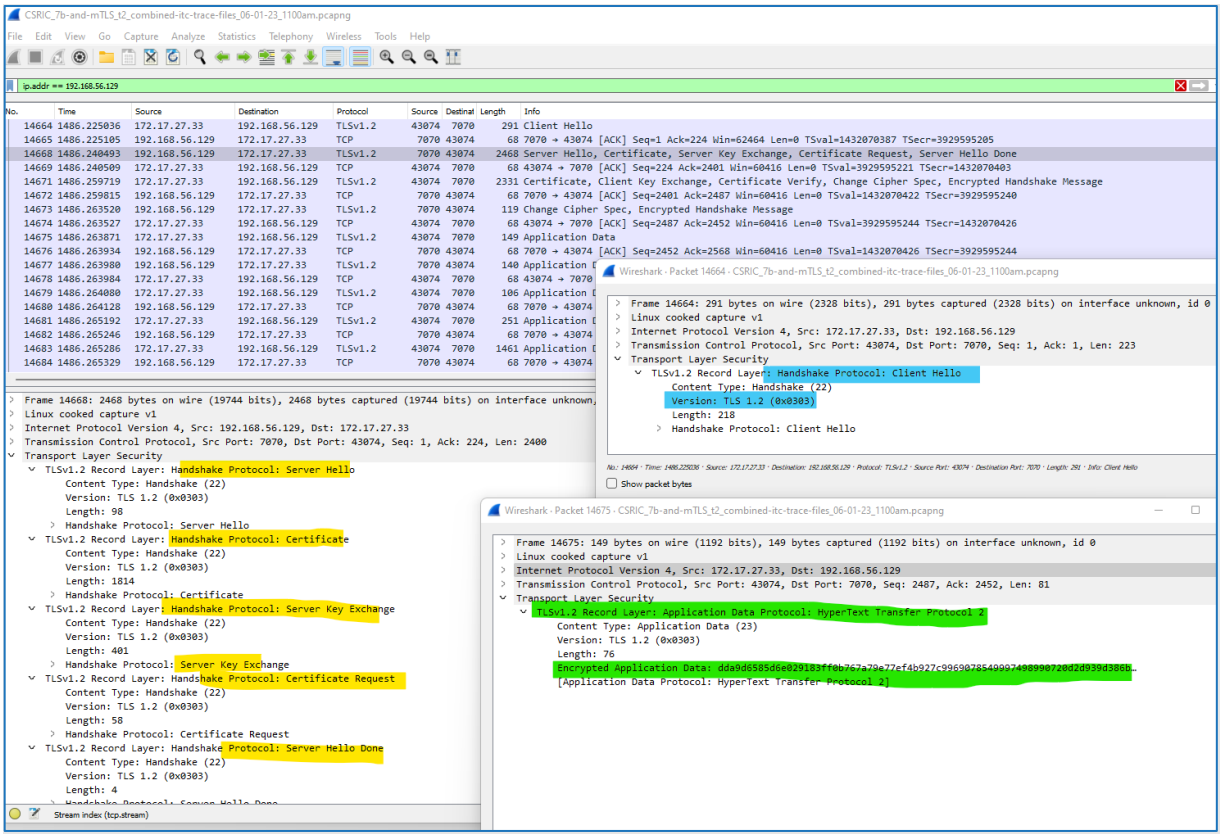

Figure 10 : mTLS handshake between SNF and NRF

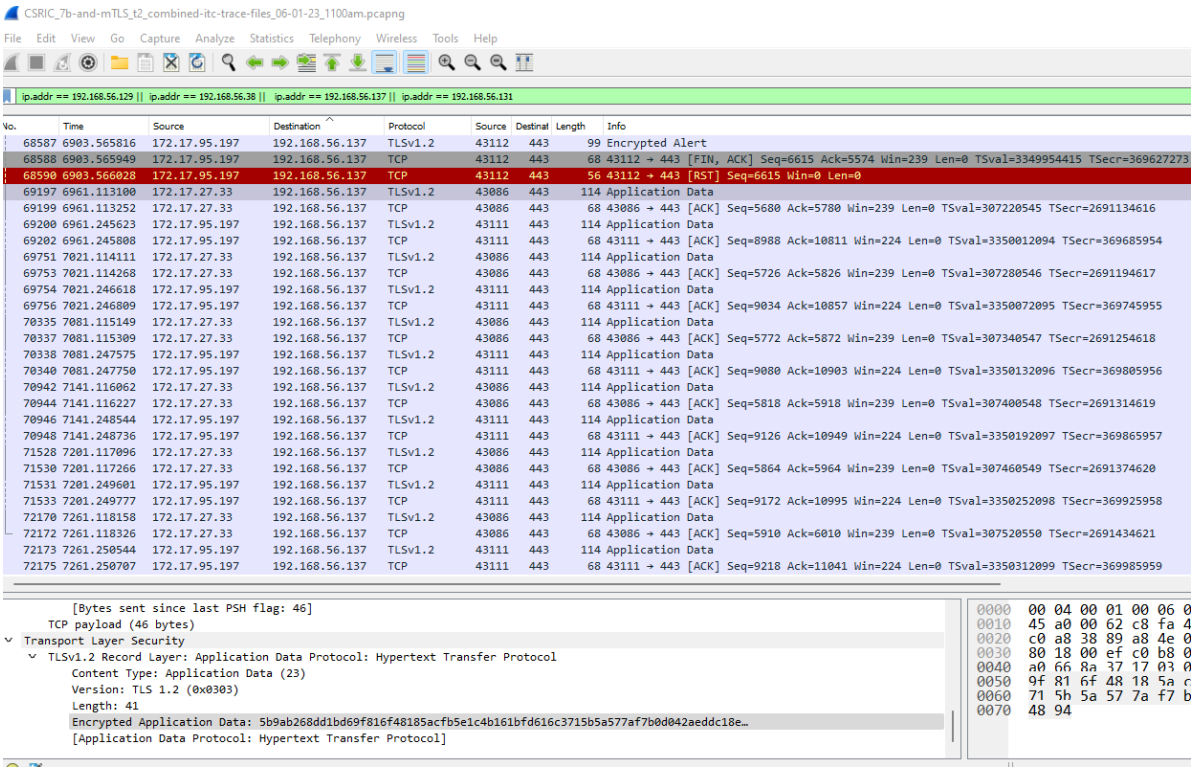

Figure 11: Encrypted mTLS traffic between UDM and AMF

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 SBI communications	Success: Network functions mutually authenticate immediately after TCP session established and before any data exchanged.
Data in transit is encrypted: cannot decode SUPI, IMEI, IMEISV, NR Cell ID; cannot identify network function IP addresses, including AMF, SMF, NRF, and AUSF	Success: All messages are encrypted; cannot read contents to decipher PEI; IP addresses are viewable, but no way to 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.

```
[xxx@fgp-dmc-jump mtls-certs-SecureG-1CA]$ openssl x509 -text -in tc3/SecureG-amf-cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2452505485278308780 (0x22090cbeb3b5e9ac)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=SecureG, CN=SecurG Lab Root CA
        Validity
            Not Before: Jun 22 17:49:00 2023 GMT
            Not After : Jun 29 17:49:00 2023 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)
                Modulus:
                    00:c1:49:86:b7:ec:6f:3e:18:4f:ef:8f:49:dc:9c:
                    82:34:bd:27:b7:7e:7c:82:a2:af:0e:f0:9a:47:a3:
                    ff:f7:d6:ce:1e:6c:08:62:74:6c:3a:97:bd:ed:a4:
                    0a:0d:a6:b1:9a:2b:56:96:dc:30:30:f6:2f:c3:b2:
                    19:e0:a8:6f:a8:4d:c1:fd:dc:ed:20:0b:b4:18:8b:
                    59:0d:40:01:da:a1:7b:62:4c:08:44:9b:94:a6:b1:
                    22:05:62:fb:9f:e3:02:54:01:87:10:d9:80:31:51:
                    77:d6:ca:53:2a:47:cf:0b:64:f2:ae:da:f1:e4:fb:
                    2f:08:20:ce:04:92:62:4d:50:15:2f:3d:13:bd:ce:
                    17:30:ad:12:0f:3f:46:03:14:49:a1:b1:19:e9:e5:
                    96:26:e8:7d:59:96:3e:e2:2d:92:cb:3c:95:99:4d:
                    17:b5:1f:31:90:30:26:62:7f:92:04:17:52:c5:dd:
                    73:19:93:9b:bb:ee:92:6e:c5:3f:b2:6e:8a:f3:3f:
                    ca:5c:94:1d:9a:33:bd:06:86:df:fc:a6:97:5a:04:
                    06:97:3b:e2:c1:fc:12:36:02:40:10:4b:c3:00:9f:
                    f0:68:4e:60:c0:11:93:3b:24:46:5b:73:80:14:0f:
                    22:09:11:43:c5:22:a4:76:af:8d:39:0e:1c:f0:21:
                    ae:61
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                C7:97:3D:A8:66:B6:40:F1:77:94:63:EA:2D:F5:F1:28:98:7D:78:53
            X509v3 Authority Key Identifier:
                keyid:91:6A:C5:35:33:A4:EE:F2:8D:51:6C:5B:4B:AF:B4:66:76:D5:40:C5

            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:mtrdmcamf01.amf.dmc.mnc014.mcc310.3gppnetwork.org
    Signature Algorithm: sha256WithRSAEncryption
```

Figure 12: TC-SBI-03 Certificate Details

```
eccd@control-plane-mtrdmc-cont-mas03-sv03:~/mtls-certs-SecureG-1CA> date; mtls_nrf_status
Tue Jun 27 16:33:10 EDT 2023
AMF
  ea3661f0-d82d-4972-b170-4dee6aea8c66
  - nfStatus REGISTERED
  - namf-comm REGISTERED
  - namf-evts REGISTERED
  - namf-mt REGISTERED
  - fqdn mtrdmcamf01
```

Figure 13: TC-SBI-04 AMF registration status

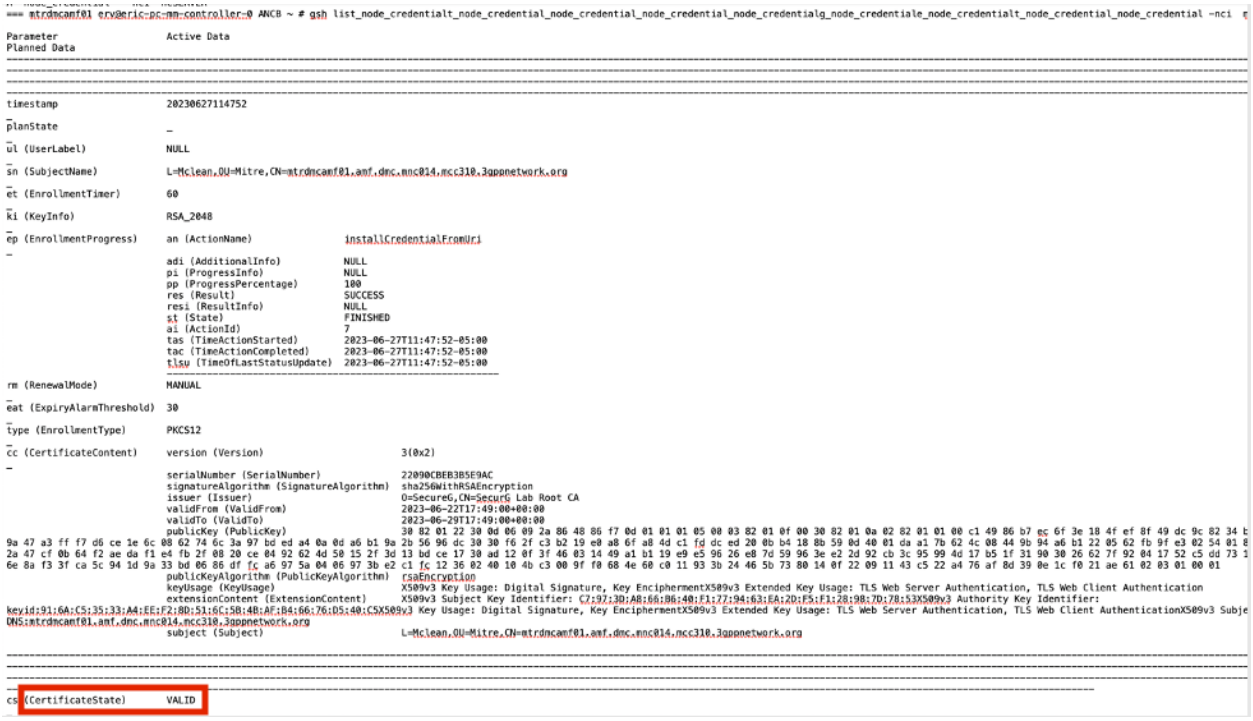

Figure 14: TC-03 Certificate Status During Valid Period

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..

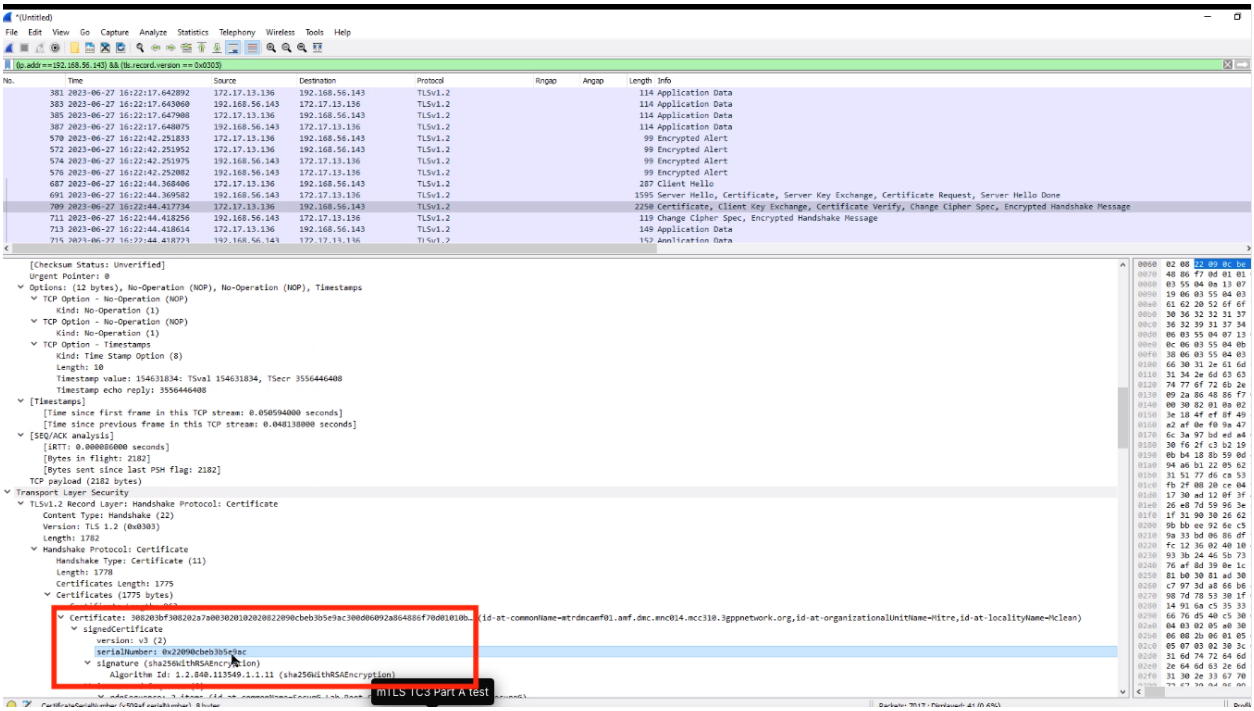

Figure 15: TC-SBI-03 Certificate Handshake Showing Certificate Serial Number

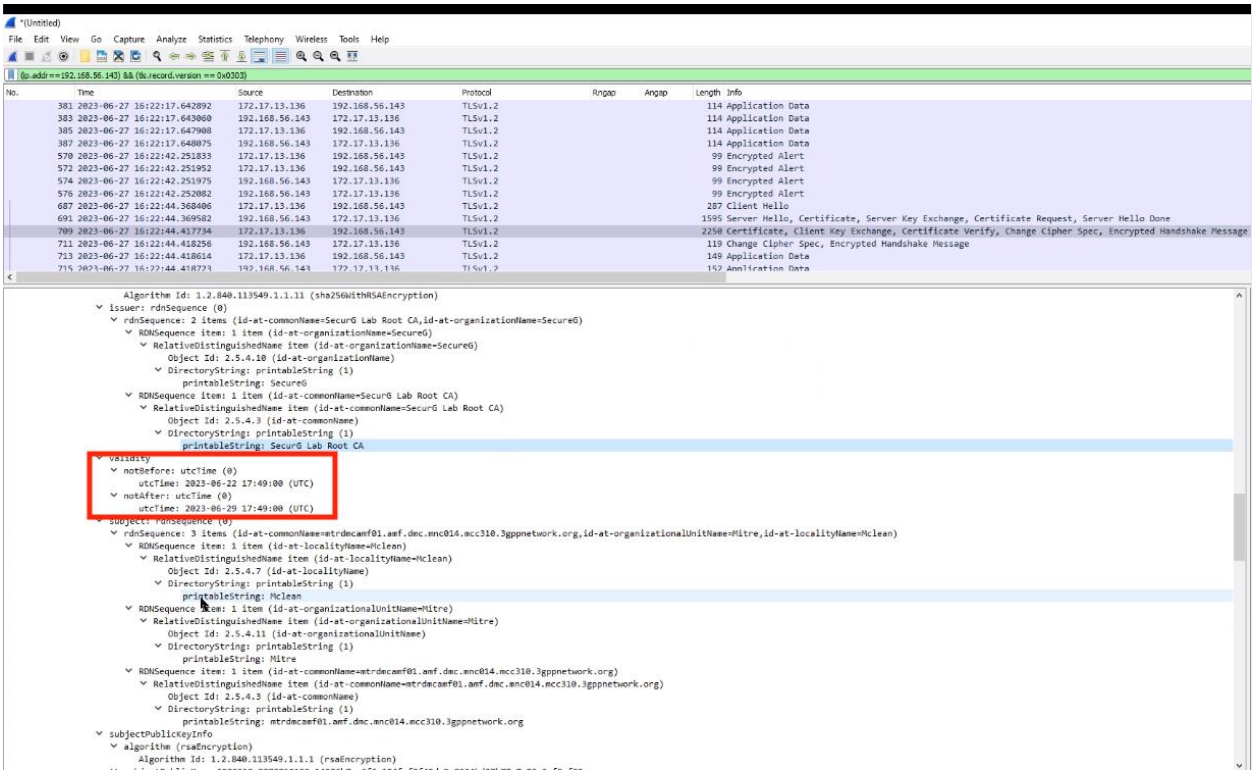

Figure 16: TC-*SBI*-03 Certificate Handshake Showing Validity Period

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.

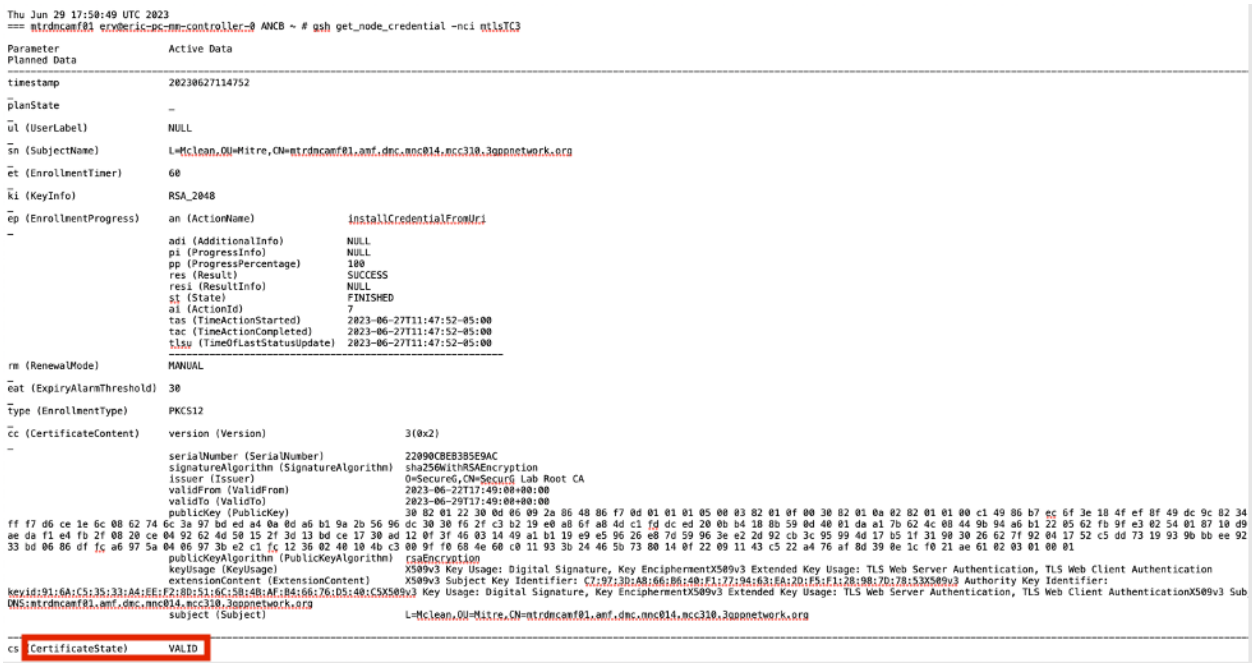

Figure 17: TC-SBI-03 Certificate Details Shortly after Expiration

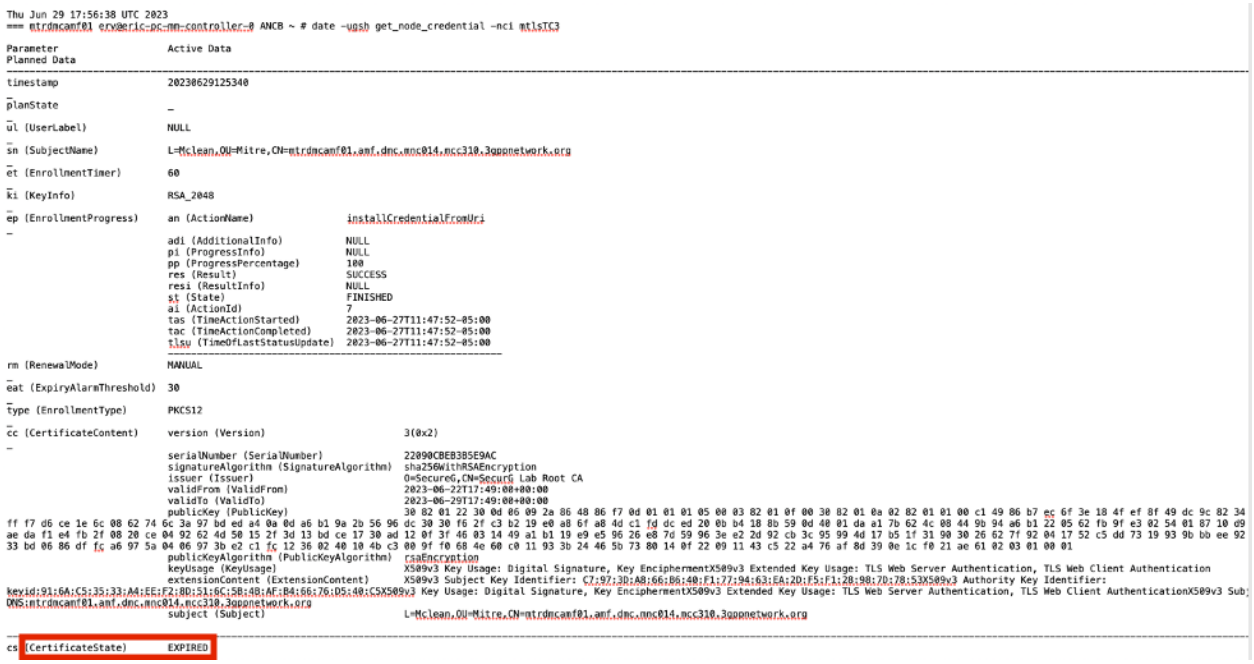

Figure 18: TC-SBI-03 Certificate Details Seven Minutes after Expiration

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

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.

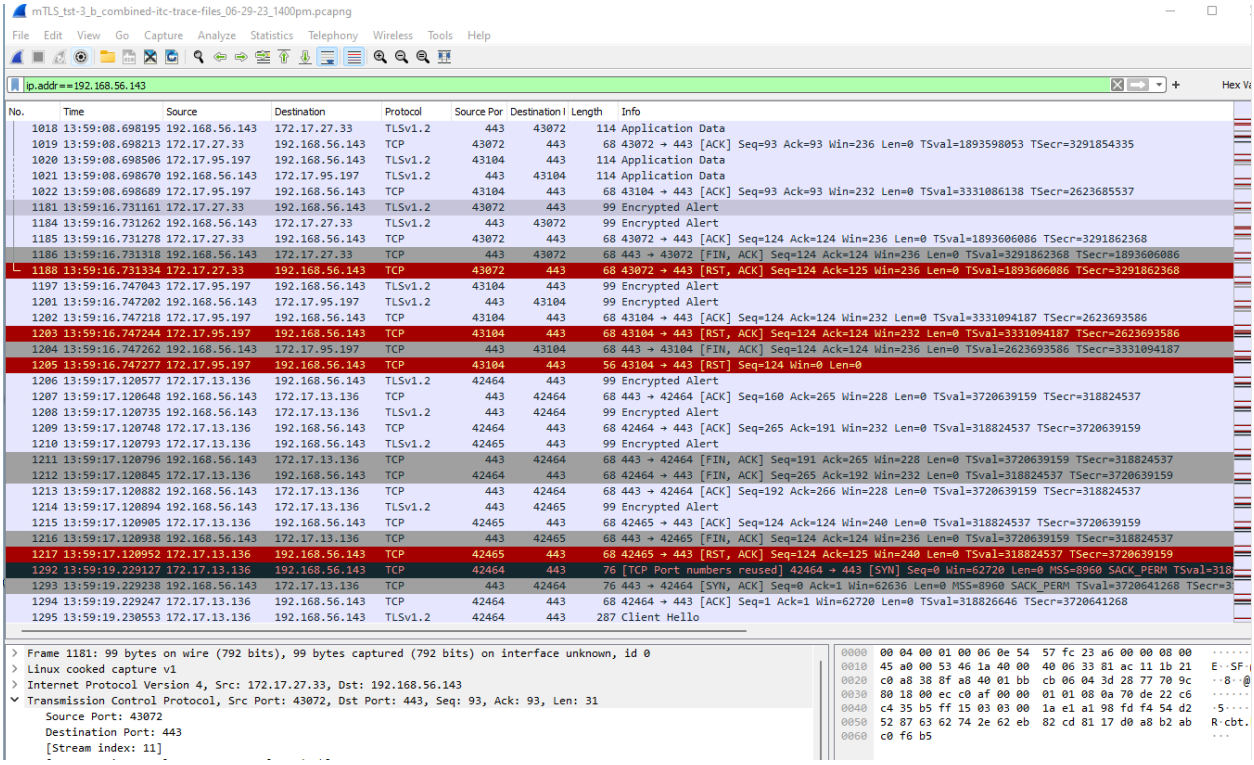

Figure 19: TC-SBI-03 Alerts and [RST, ACK] Messages after Certificate Expiration

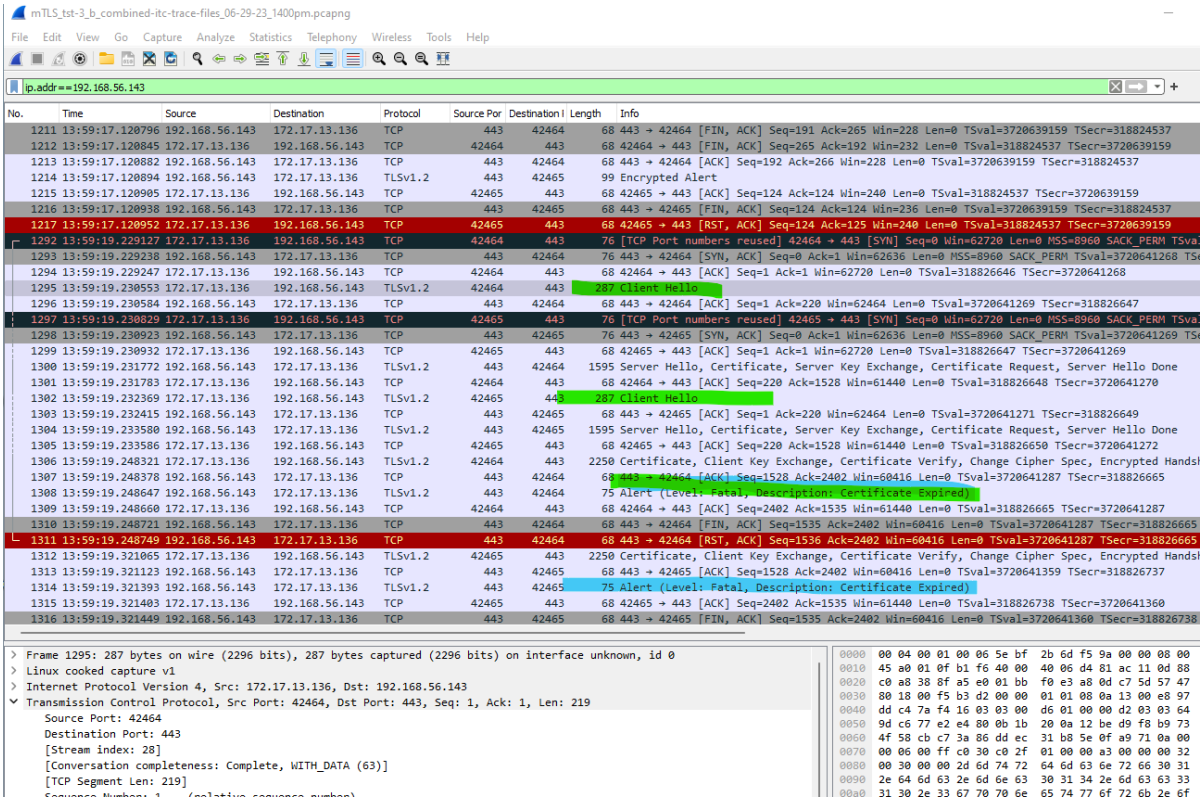

Figure 20: TC-SBI-03 SBI mTLS Client Hello and Fatal Alerts

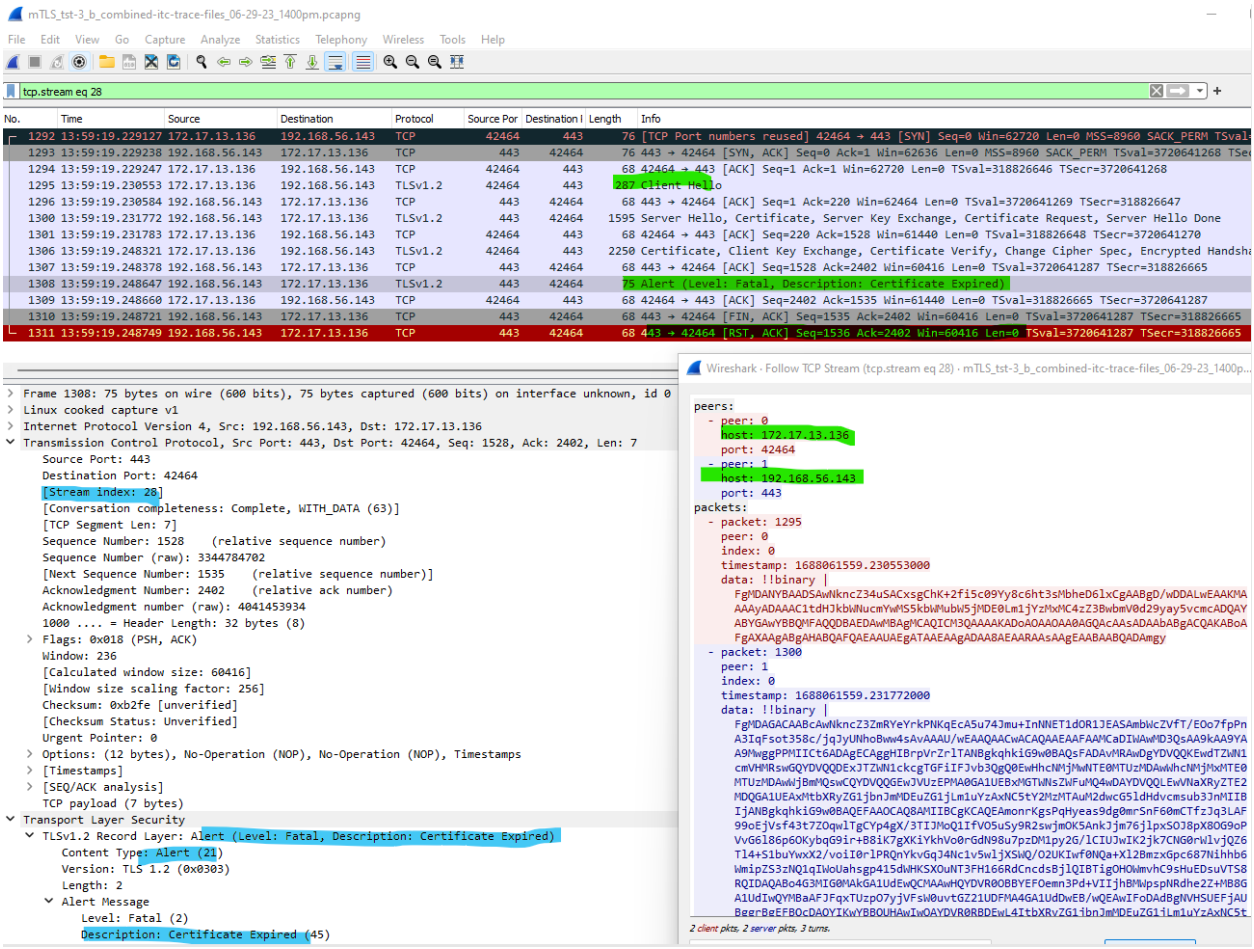

Figure 21 : TC-SBI-03 mTLS Fatal Alert Details

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.

```
eccd@control-plane-mtrdmc-cont-mas03-sv03:~/mtls-certs-SecureG-1CA> date & mtls nrf status
[1] 57676
Thu Jun 29 14:00:29 EDT 2023
AMF
  ea3661f0-d82d-4972-b170-4dee6aea8c66
  - nfStatus REGISTERED
  - namf-comm REGISTERED
  - namf-evts REGISTERED
  - namf-mt REGISTERED
  - fqdn mtrdmcamf01
```

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
  - fqdn 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 credentials to attach on the SBI	Success: Prior to certificate expiration, 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 credentials from attaching on the SBI	Success: After certificate expiration, AMF 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: O=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: O=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:
                    b8:df:2b:4a:63:23:eb:21:01:a1:7d:f5:6a:76:96:
                    51:38:c8:04:e4:cc:e2:cd:bd:42:27:03:74:b6:2c:
                    e0:94:32:f8:50:da:52:ce:49:4e:b0:e9:10:13:98:
                    8c:f0:ef:01:73:11:48:f5:9c:3b:f7:fc:47:e1:a6:
                    fd:32:29:da:72:b5:bf:3a:ba:01:7b:c7:ca:60:a5:
                    be:ae:d0:4b:9f:62:ac:22:71:63:1d:b4:3d:72:27:
                    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

```
_
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_trusted_certificate -cei SecureG-tc4-cacert-root
Parameter                   Active Data
Planned Data
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
timestamp                   20230629211303
_
planState                   _
_
ms (ManagedState)           ENABLED
_
cc (CertificateContent)     version (Version)                       3(0x2)
_
                            serialNumber (SerialNumber)             2B03227A60AFAD89
                            signatureAlgorithm (SignatureAlgorithm) sha256WithRSAEncryption
                            issuer (Issuer)                         O=SecureG,CN=AMF-root-CA
                            validFrom (ValidFrom)                   2023-06-22T17:56:00+00:00
                            validTo (ValidTo)                       2025-06-22T17:56:00+00:00
                            publicKey (PublicKey)                   30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 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 b8 df 2b 4a 63 23 eb 21 01 a1 7d f5 6a 76 96 51 38 c8 04 e4 cc e2 cd
bd 42 27 03 74 b6 2c e0 94 32 f8 50 da 52 ce 49 4e b0 e9 10 13 98 8c f0 ef 01 73 11 48 f5 9c 3b f7 fc 47 e1 a6 fd 32 29 da 72 b5 bf 3a ba 01 7b c7 ca 60 a5 be ae d0 4b 9f 62 ac 22 71 63 1d b4 3d 72 27 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 02 03 01 00 01
                            publicKeyAlgorithm (PublicKeyAlgorithm) rsaEncryption
                            keyUsage (KeyUsage)                     X509v3 Key Usage: Certificate Sign, CRL Sign
                            extensionContent (ExtensionContent)     X509v3 Basic Constraints: CA:TRUEX509v3 Subject Key Identifier: 2E:FD:D9:43:58:B5:17:AA:75:0A:68:92:B7:09:67:B0:1B:A9:04:D4X509v3 Key
Usage: Certificate Sign, CRL Sign
                            subject (Subject)                       O=SecureG,CN=AMF-root-CA

-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
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
            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)
                Modulus:
                    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:d8: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:
                    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:f0:1b:97:49:7e:9d:0b:31:ad:15:
                    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:F1:88:4D: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:mtrdmcamf01.amf.dmc.mnc014.mcc310.3gppnetwork.org
    Signature Algorithm: sha256WithRSAEncryption
```

Figure 26: TC-SBI-04 AMF Certificate Details

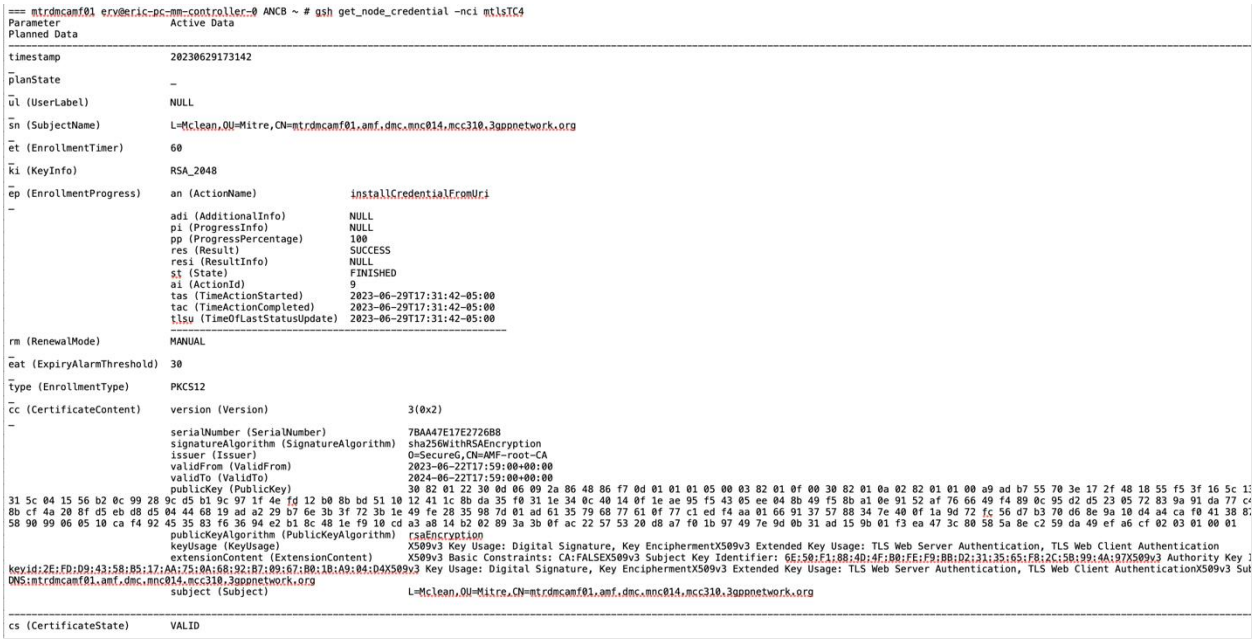

Figure 27: TC-SBI-04 AMF Certificate State

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.

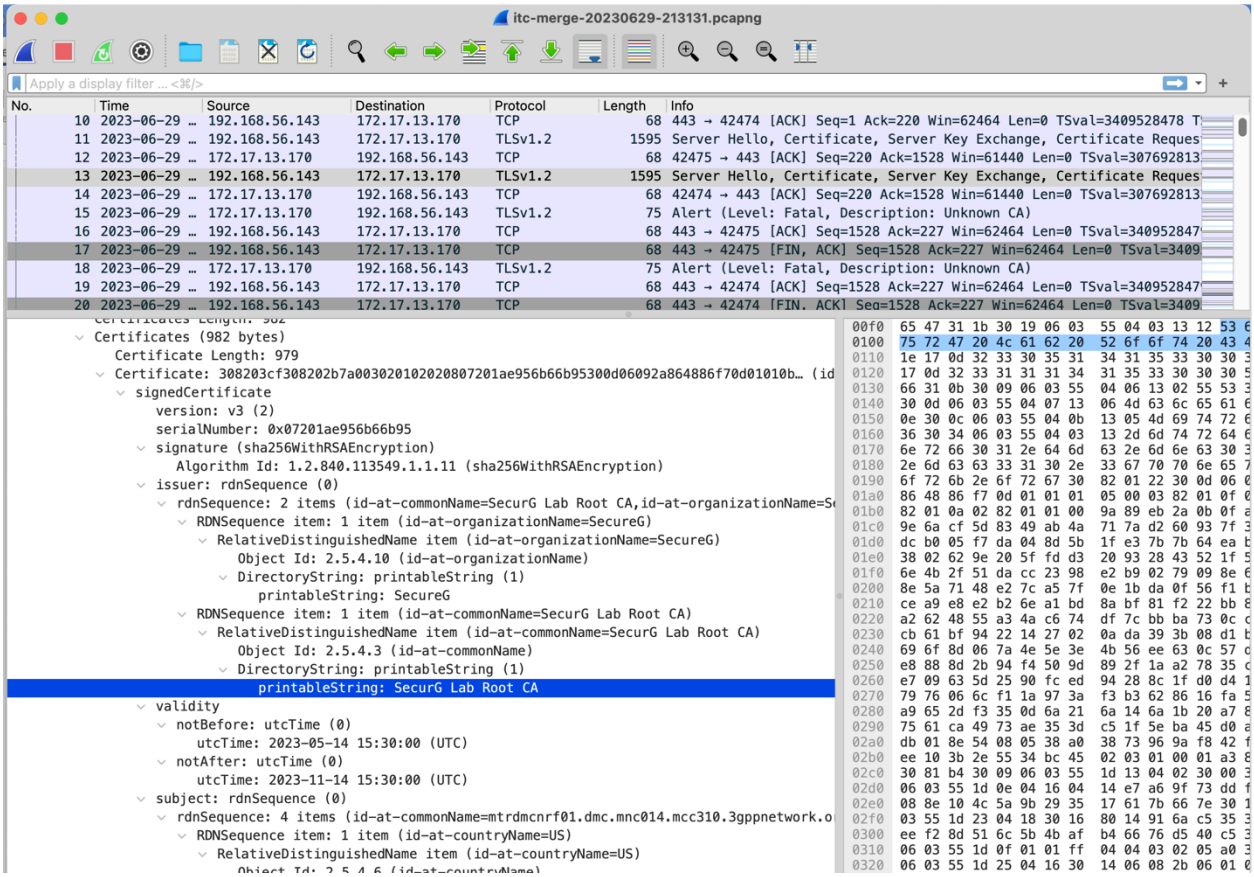

Figure 28: TC-SBI-04 NRF to AMF Key Exchange

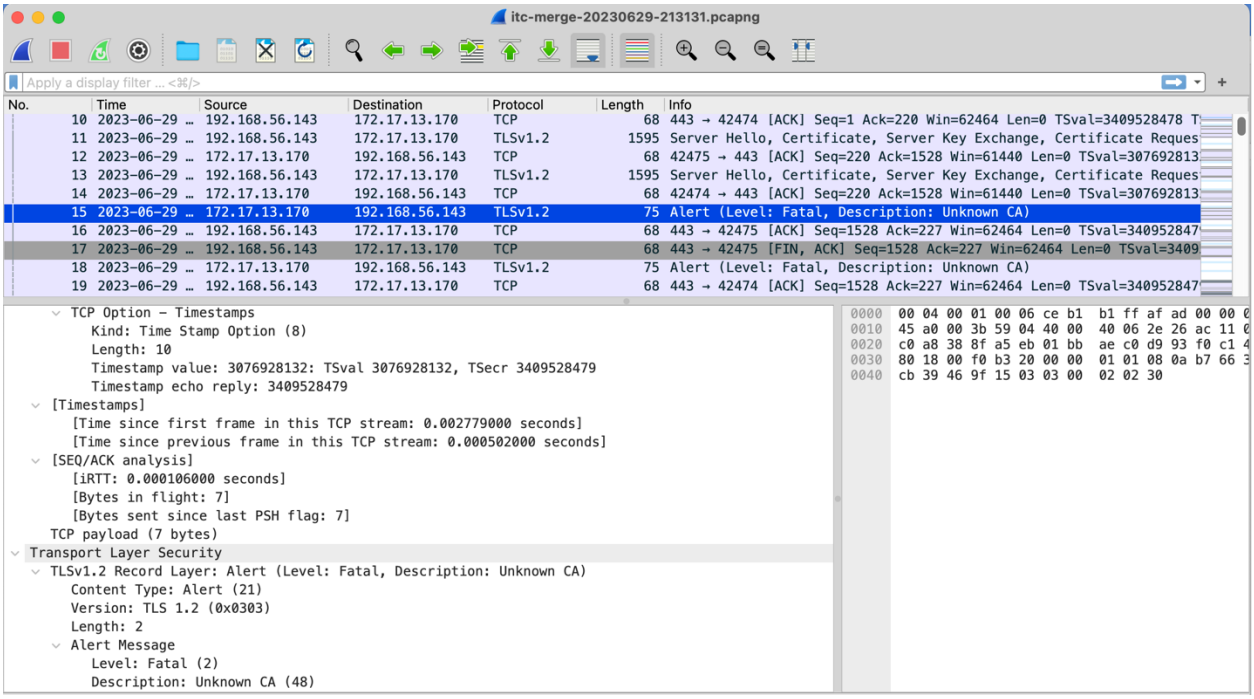

Figure 29: TC-SBI-04 AMF-to-NRF Key Exchange Failure

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	Success – Certificate using "AMF-root-CA" successfully installed on AMF.
Handshake between AMF and NRF fails	Success – 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.

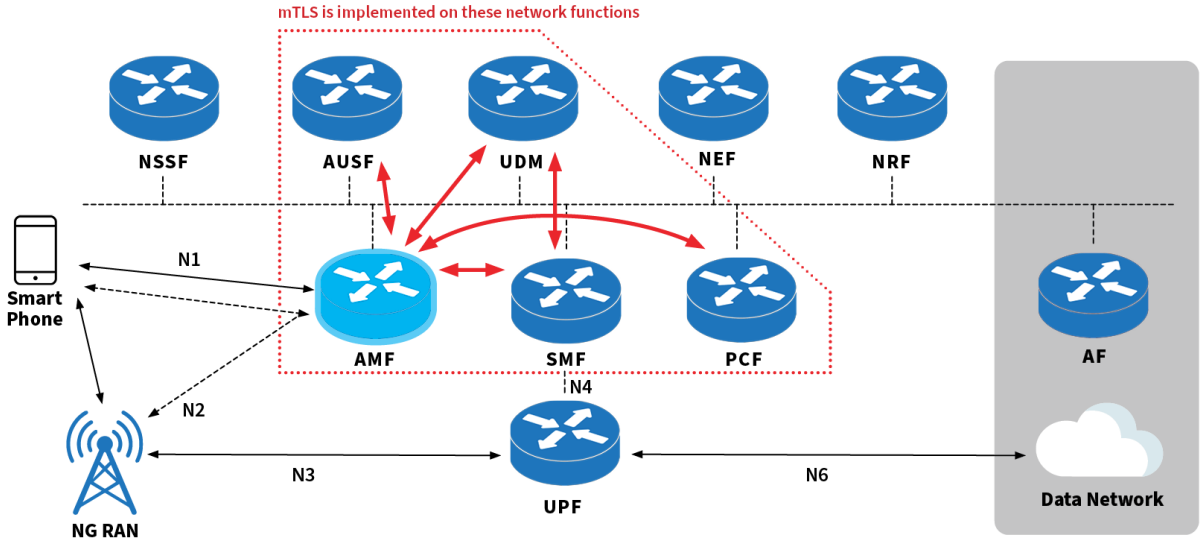

Figure 30: Intra-Network mTLS across Security Domains

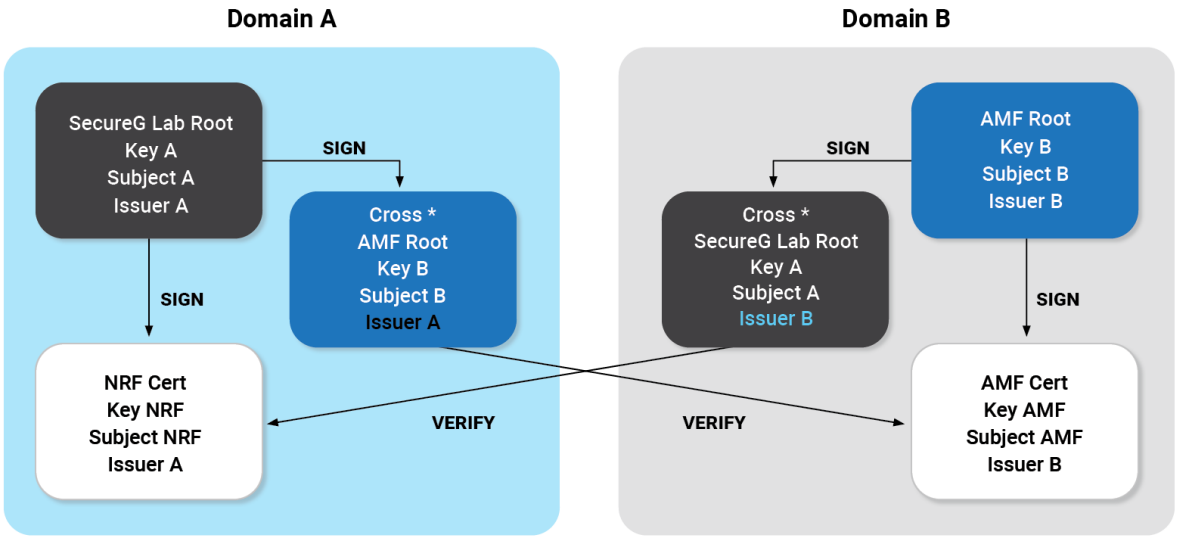

Figure 31: Cross-Signing of Certificates for Intra-Network mTLS

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
        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          _
_
ms (ManagedState)      ENABLED
_
cc (CertificateContent)    version (Version)          3(0x2)
_
            serialNumber (SerialNumber)          2B03227A60AFAD89
            signatureAlgorithm (SignatureAlgorithm)  sha256WithRSAEncryption
            issuer (Issuer)              O=SecureG,CN=AMF-root-CA
            validFrom (ValidFrom)          2023-06-22T17:56:00+00:00
            validTo (ValidTo)          2025-06-22T17:56:00+00:00
            publicKey (PublicKey)          30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 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 b8 df 2b 4a 63 23 eb 21 01 a1 7d f5 6a 76 96 51 38 c8 04 e4 cc e2 cd bd 42 27 03 74 b6 2c e0 94 32 f8 50 da 52 ce 49 4e b0 e9 10 13 98 8c f0 ef 01 73 11 48 f5 9c 3b f7 fc 47 e1 a6 fd 32 29 da 72 b5
bf 3a ba 01 7b c7 ca 60 a5 be ae d0 4b 9f 62 ac 22 71 63 1d b4 3d 72 27 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 02 03 01 00 01
            publicKeyAlgorithm (PublicKeyAlgorithm)  rsaEncryption
            keyUsage (KeyUsage)          X509v3 Key Usage: Certificate Sign, CRL Sign
            extensionContent (ExtensionContent)     X509v3 Basic Constraints: CA:TRUEX509v3 Subject Key Identifier: 2E:FD:D9:43:58:B5:17:AA:75:0A:68:92:B7:09:67:B0:1B:A9:04:D4X509v3 Key Usage: Certificate Sign, CRL Sign
            subject (Subject)              O=SecureG,CN=AMF-root-CA

--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
cs (CertificateState)      VALID
```

Figure 35: AMF Root Issuer and Subject

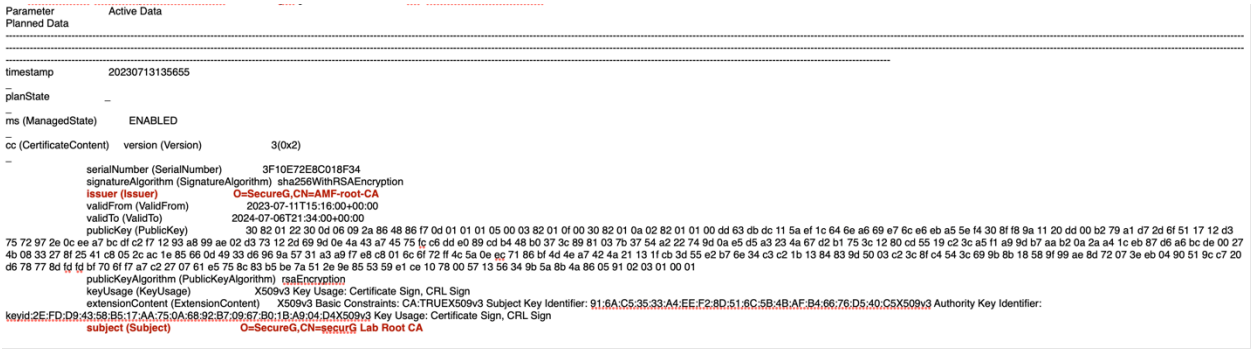

Figure 36: AMF Cross-signing of SecureG Lab Root CA

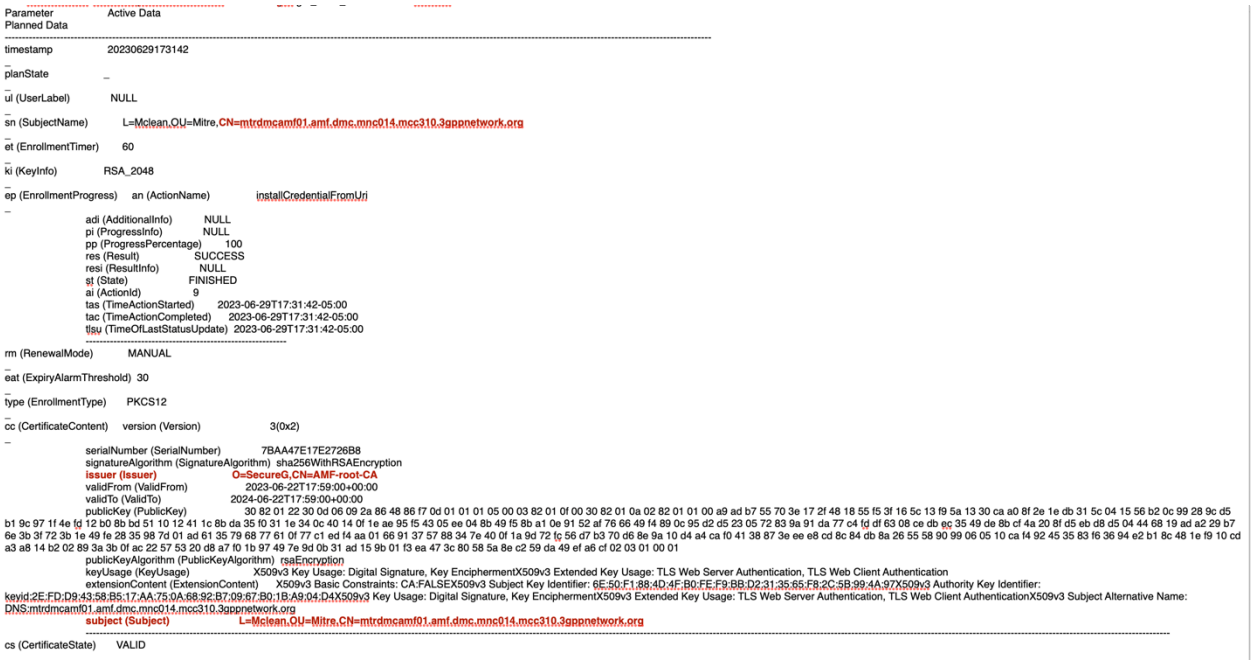

Figure 37: AMF Certificate Signed by AMF-root-CA

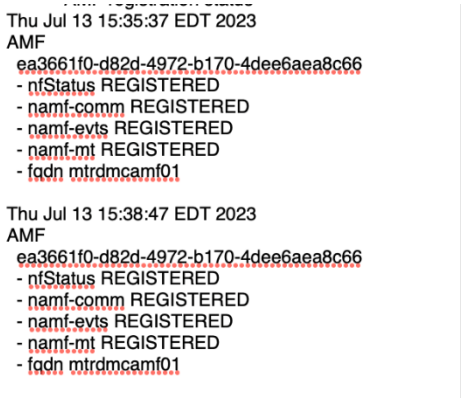

Figure 38: AMF Registration Status

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.

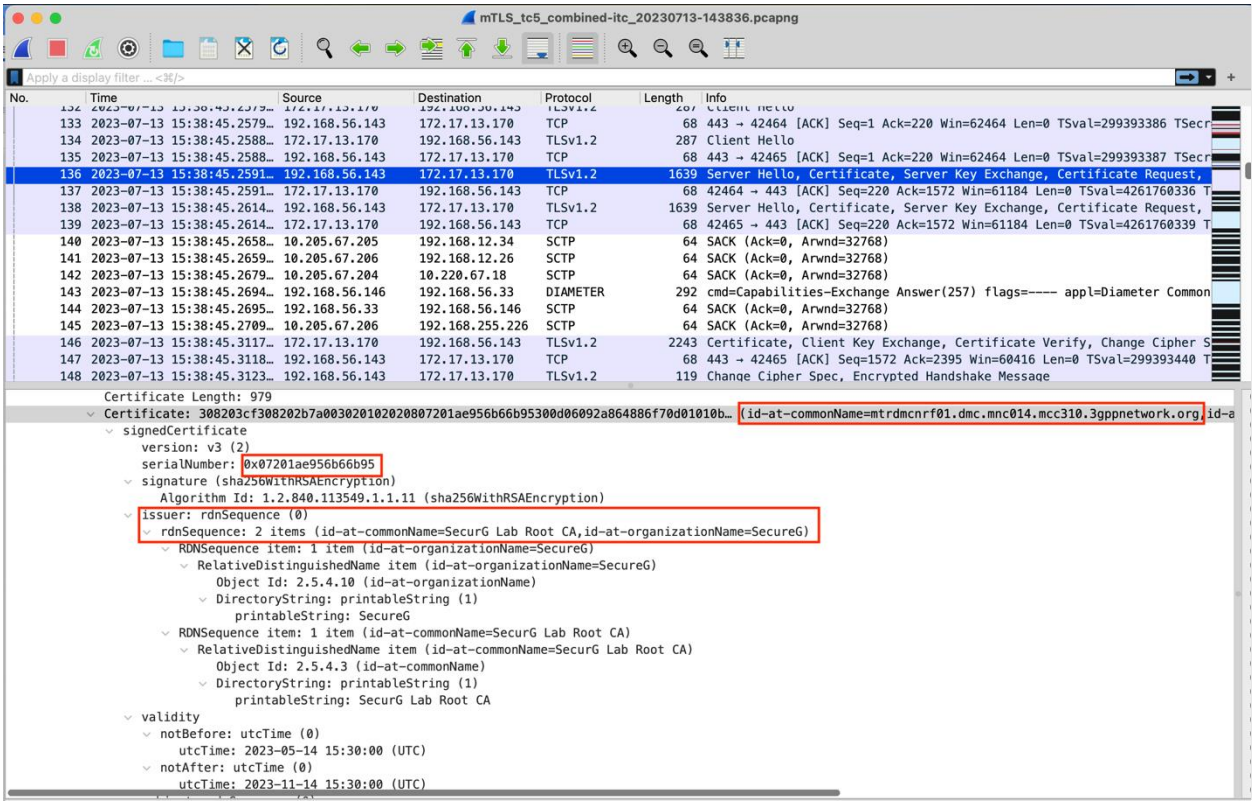

Figure 39: NRF to AMF Server Hello, Certificate Exchange

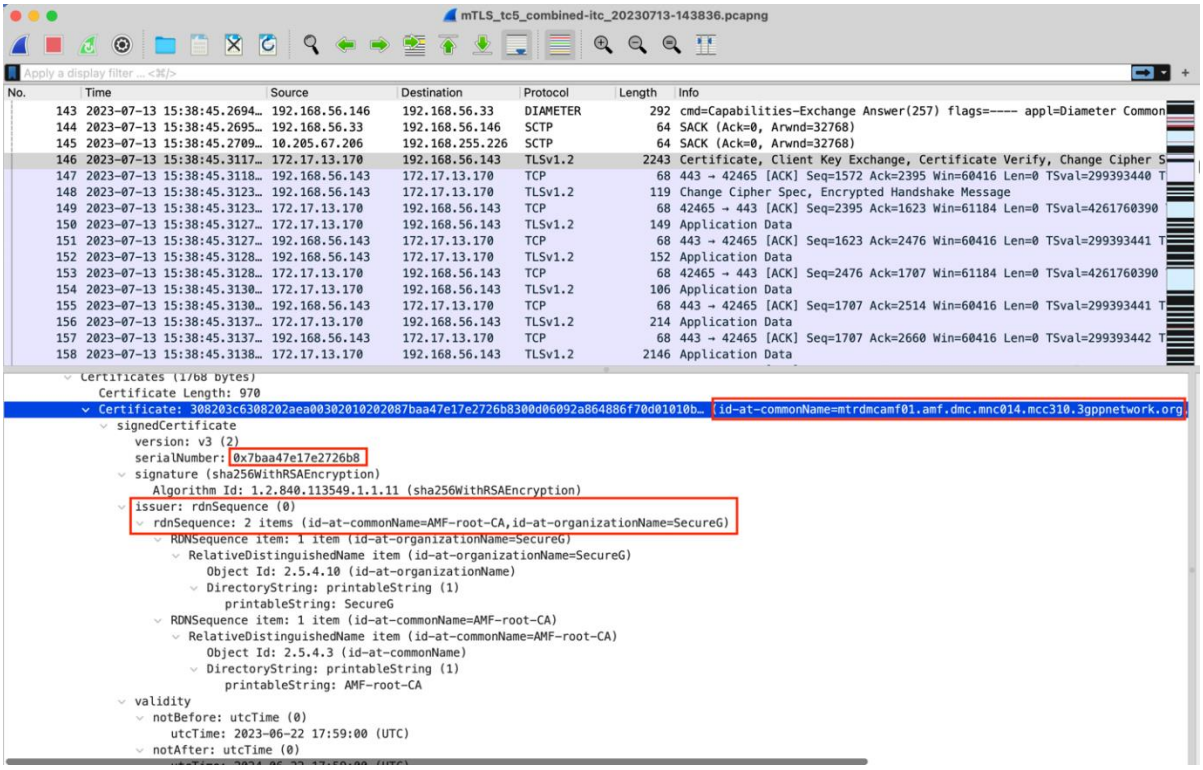

Figure 40: AMF to NRF Certificate Exchange: AMF Certificate

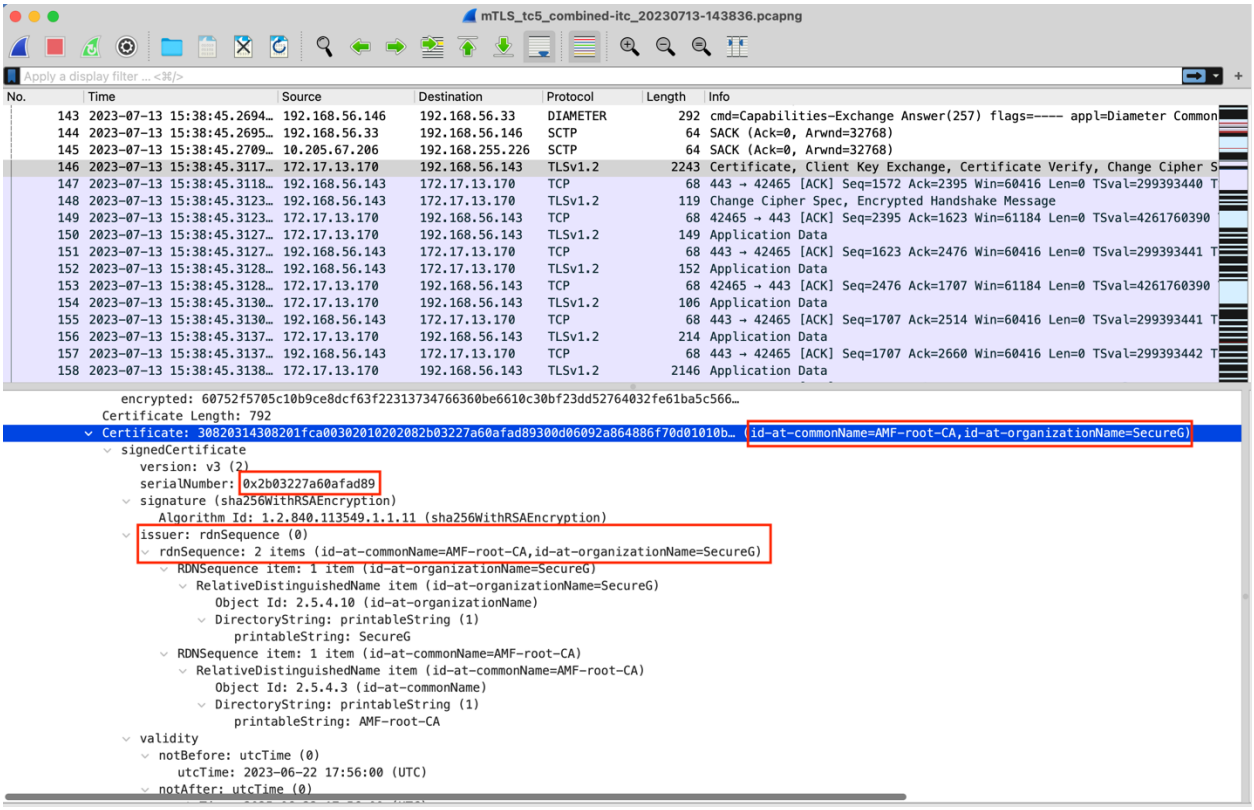

Figure 41: AMF to NRF Certificate Exchange: AMF-root-CA

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

Appendix: Acronyms

3GPP	3rd Generation Partnership Project
5G STB	5G Security Test Bed
AMF	Access and Mobility Management Function
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

TLS	Transport Layer Security
TP	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