5G SECURITY TEST BED™

Securing 5G:

5G Security Test Bed Confirms Mutual Transport Layer Security Is Powerful Zero Trust Enabler for 5G Networks

Fall 2023 mTLS Report Highlights

The 5G Security Test Bed and Its Findings

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. Stakeholders from across the entire wireless ecosystem work together to develop and improve security features for wireless networks and consumers. The wireless industry's 5G Security Test Bed is the next piece of this commitment. The 5G Security Test Bed 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.

Testing CSRIC VII Recommendations for mTLS on 5G Networks

The 5G Security Test Bed's Technical Advisory Committee designed and conducted five tests to verify recommendations from the FCC's Communications Security, Reliability, and Interoperability Council VII (CSRIC VII) around the use of mutual transport layer security (mTLS) on the Service-Based Interface (SBI) between the 5G network functions (NFs).

Key Findings

All five tests were successful, confirming that mTLS can be used for the encryption of data and the mutual authentication of 5G network functions that exchange data across the SBI, enabling Zero Trust in a 5G environment. The tests validated that:

✓ **Additional encryption within the 5G network strengthens security.**
Test 1 confirmed that if a 5G network is breached, information within the network can be vulnerable to exposure. mTLS encryption adds an additional layer of security within the 5G core network itself to protect data from attackers.

✓ **Mutual Transport Layer Security protects 5G networks by:**

- **Encrypting and protecting critical data at both ends of the network.** Test 2 confirmed that mTLS can encrypt critical user, device, and network information via HTTPS, as well as authenticate and authorize both sides of the HTTPS connection through mTLS encryption.
- **Rejecting expired credentials.** Test 3 confirmed that, after implementation of mTLS, expired credentials on one end will lead to a failed SBI connection, keeping out-of-date functions that may have vulnerabilities from attaching to the network.
- **Rejecting invalid credentials.** Test 4 confirmed that, with mTLS, invalid credentials on one end will lead to a failed SBI connection, preventing unwanted functions from joining the network.
- **Cross-authenticating credentials from different vendors.** Test 5 confirmed that a 5G core solution can be implemented securely using different vendors, ensuring that mTLS sessions can be established across different certificate authorities.

Because mTLS can be used at numerous points within a 5G network to constantly authenticate the validity of users and functions attempting to connect, it can serve as a foundational component of the Zero Trust approach to network security. Zero Trust has been recognized by the wireless industry, and recently by the federal government, as a multifaceted and flexible defense against network attacks.

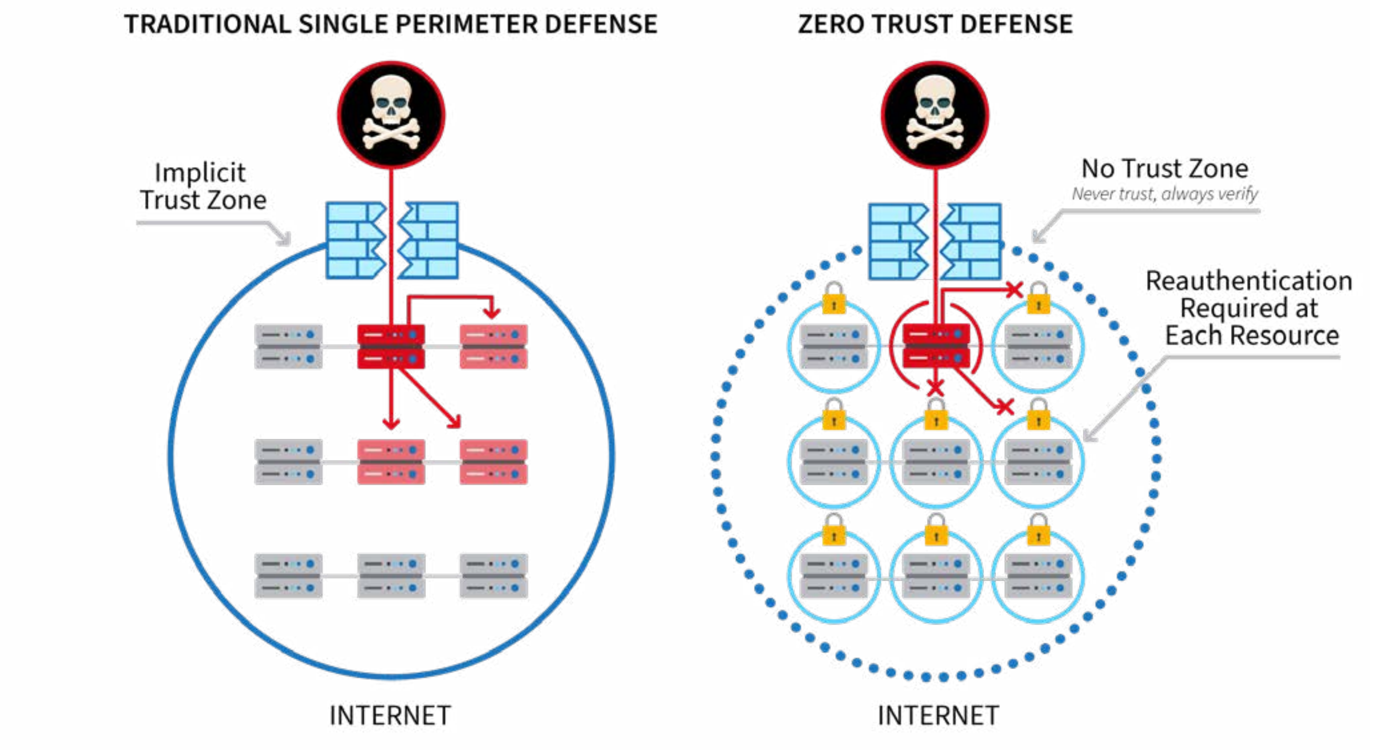
5G Security: Service-Based Architecture, Transport Layer Security, and Zero Trust

5G's Service-Based Network Architectures

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 each NF able to access services from another NF. The nature of 5G network architectures enables greater flexibility, targeted customization, and enhanced security when it comes to protecting the network.

Zero Trust

Zero Trust is a set of principles that significantly strengthens security on these networks by requiring ongoing verification of users, applications, and associated devices even after they have been authorized to enter the network. When Zero Trust principles are implemented, users, devices, and applications are authenticated at multiple points *within* the network as they access different network areas and corresponding network functions. The methods, applications, and components that are implemented to achieve Zero Trust are part of the Zero Trust Architecture.[1]

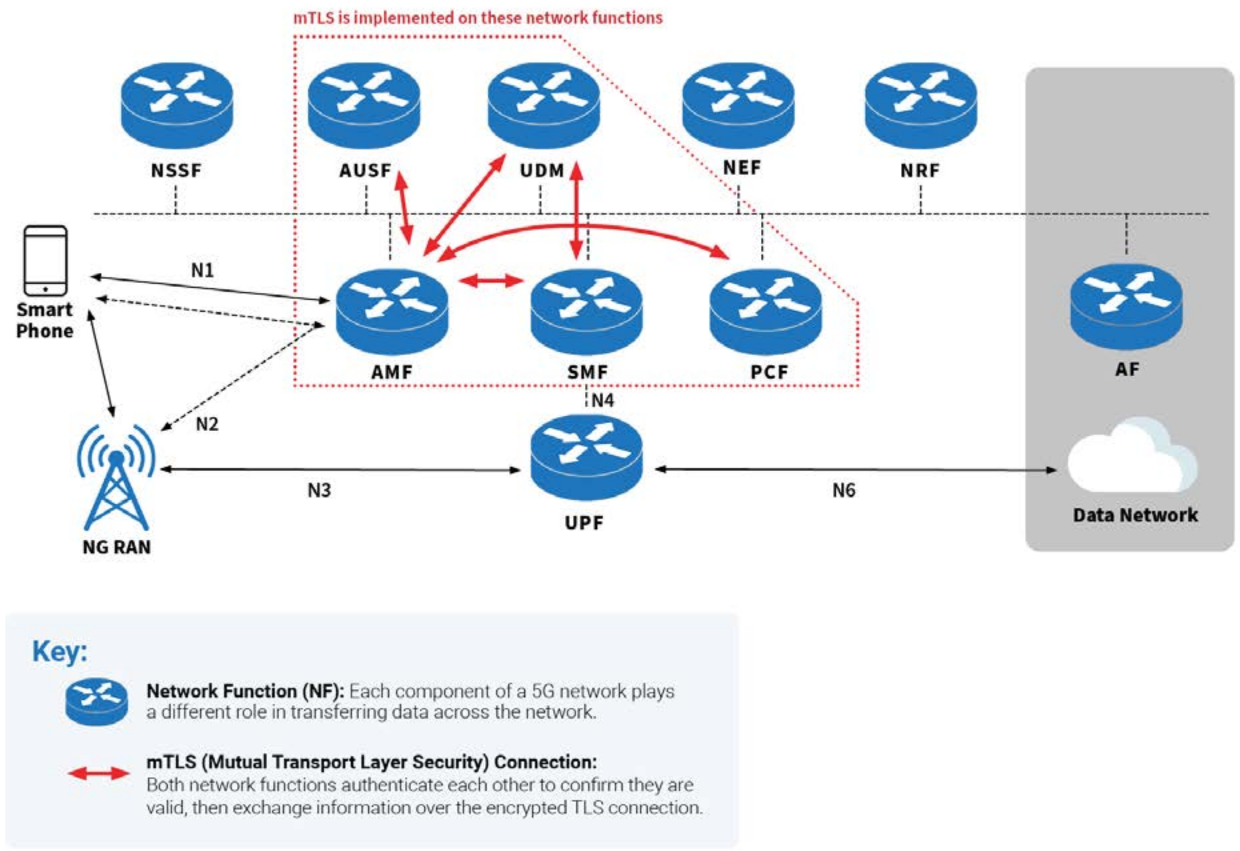

TRADITIONAL SINGLE PERIMETER DEFENSE
ZERO TRUST DEFENSE
Implicit Trust Zone
No Trust Zone
Never trust, always verify
Reauthentication Required at Each Resource
INTERNET
INTERNET

[1] A 2023 CTIA report, *Defining Zero Trust: Industry Approaches and Policy Frameworks for Strong Wireless Network Security*, provides an in-depth overview of Zero Trust, its core principles, and implementation. It is available at https://api.ctia.org/wp-content/uploads/2023/01/Defining-Zero-Trust-White-Paper-2023.pdf.

Mutual Transport Layer Security

Because different wireless networks have different capabilities depending on their structures, equipment, and systems, Zero Trust Architectures inherently differ to meet each network's particular needs. Transport layer security (TLS) is a protocol for securing data that uses cryptography to encrypt and decrypt data exchanged between sender and recipient networks. With mutual TLS (mTLS), the sending and receiving network functions authenticate each other to confirm they are valid, then exchange information over the encrypted TLS connection—providing an additional layer of security. mTLS can be used across a 5G network's SBA interface (SBI) to enable encryption between the various components (known as network functions, or NFs) within the 5G core, requiring authorization for each NF before it exchanges information.

When included in a Zero Trust Architecture, mTLS can serve as a powerful foundational component of Zero Trust.



Key:

Network Function (NF): Each component of a 5G network plays a different role in transferring data across the network.

mTLS (Mutual Transport Layer Security) Connection: Both network functions authenticate each other to confirm they are valid, then exchange information over the encrypted TLS connection.

Testing Transport Layer 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, including a 2021 Executive Order instructing the federal government to "advance toward Zero Trust Architecture" on its networks, along with additional guidance for federal agencies from the Office of Management and Budget. The National Institute of Standards and Technology's (NIST) foundational guidance on Zero Trust also recommends "authenticating all connections and encrypting all traffic" on a network.

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.*[2]

5G Security Test Bed Results: Successful Verification That mTLS Enhances Zero Trust and 5G Network Security

Test Case 1: Understand SBI Vulnerabilities

Test Case 1 was designed to determine if data traveling on the 5G core SBI is vulnerable in the event of a data breach. The test execution consisted of acting as an unauthorized user infiltrating the network, then accessing and capturing the data carried on the SBI, such as user, device, location, and connection information.

- ✓ **Success:** The test confirmed that in the case of a breach, information may be exposed on the 5G core interfaces. The following tests added additional layers of encryption within the 5G network core to confirm that information could be protected, even after a beach, by enabling the implementation of Zero Trust principles.

Test Case 2: Implement Mutual TLS on SBIs

Test Case 2 was designed to demonstrate the ability to encrypt critical user, device, and network information via HTTPS using mTLS, as well as to verify that mTLS can authenticate and authorize both ends of the HTTPS connection. The test consisted of implementing mutual authentication prior to network function communication across the SBI, and then verifying that data is encrypted in transit.

- ✓ **Success:** The test confirmed that with mTLS encryption implemented on transit data, an unauthorized user cannot decode user or device identification information, nor identify network function IP addresses.

Test Case 3: Prevent Network Function with Expired Credentials from Attaching to SBI

Test Case 3 was designed to demonstrate that, with mTLS implemented, expired credentials on one end of the connection lead to a failed SBI connection, preventing any out-of-date, and potentially vulnerable, network functions from attaching to the network. The test consisted of two parts, transmitting data across mTLS-encrypted network function connections before and after their credentials expired.

- ✓ **Success:** The test confirmed that mTLS enables network functions with valid credentials to connect and exchange encrypted data over the SBI; after credentials expired, mTLS terminated the network functions' connections and prevented them from connecting or exchanging data over the network.

[2] 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

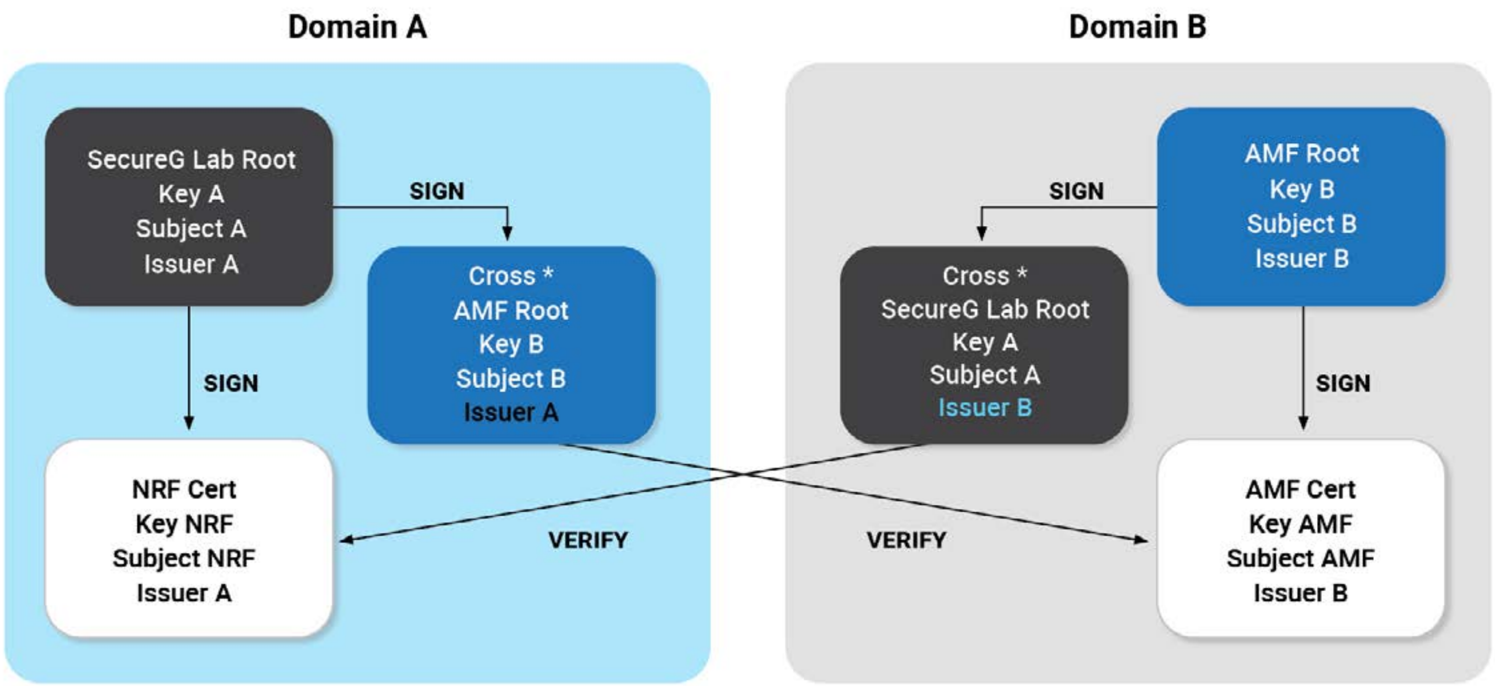
Test Case 4: Prevent Unknown Network Function from Attaching to SBI

Test Case 4 was designed to demonstrate that, with mTLS implemented, invalid credentials on one end lead to a failed SBI connection, preventing any unknown network functions from attaching to the network. For this test, a network function with a certificate valid for its own function was issued a different root certificate from an alternative Certificate Authority (CA). A handshake was then attempted between that NF and another to verify that, because the root certificate was different, it would be deemed invalid on other network functions.

✓ **Success:** The test confirmed that mTLS detects and rejects network functions with invalid credentials, terminating their connection and preventing them from attaching to the SBI.

Test Case 5: Implement Multi-Domain mTLS on SBI

Test Case 5 was designed to demonstrate that mTLS can be securely implemented with certificates from different Certificate Authorities, and that network functions can cross-sign certificates to establish trust across security domains. As with the previous test, a new root certificate was assigned from a different CA—but in this case, the AMF network function was used to cross-sign and verify certificates exchanged between other network functions, establishing the trust that was lacking in Test Case 4.



✓ **Success:** The test confirmed that mTLS works when certificates come from separate root CAs, verifying the authenticity of the participating network functions and enabling protection of the traffic between them.

Key Takeaways

- Together, these tests verify the important role mTLS can play as a Zero Trust enabler. Zero Trust principles dictate continuous validation of users and data traveling on a network, and the five tests successfully demonstrated that mTLS can reliably encrypt and authenticate communications between the network functions that operate on the 5G core interface.
- 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.

This is great news for consumers—mTLS is already being deployed, and implementation will continue to grow as the U.S. wireless industry upgrades its 5G networks from non-standalone (5G networks built on a 4G infrastructure) to standalone (networks designed and built specifically for 5G) nationwide. More than 250 million people are already covered by 5G standalone networks across the U.S., and this number will grow steadily, connecting more people to advanced network security features—like mTLS and Zero Trust—as carriers continue rolling out network upgrades in the coming months.

Next Steps

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 will also conduct additional phases of network slicing tests, and it is 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 at (hpunjabi@ctia.org; (202) 845-5701), or visit https://5gsecuritytestbed.com/.

5G
SECURITY™
TEST BED