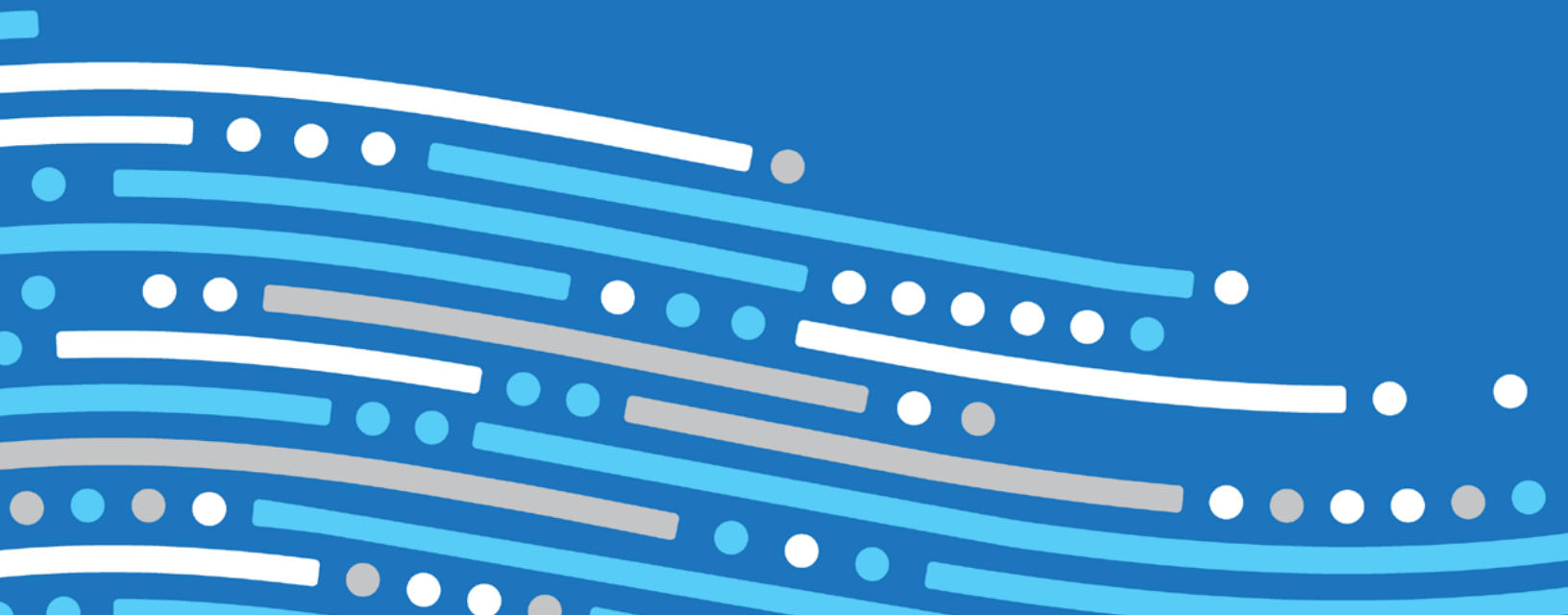
5G SECURITY™ TEST BED

Securing 5G:

5G Security Test Bed Confirms Network Slicing Works Securely to Enhance 5G Network Efficacy

2023 Q1 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 new 5G Security Test Bed is the next piece of this commitment.

Real-World Testing: A First of Its Kind

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. 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 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 3GPP Technical Specifications for Network Slicing

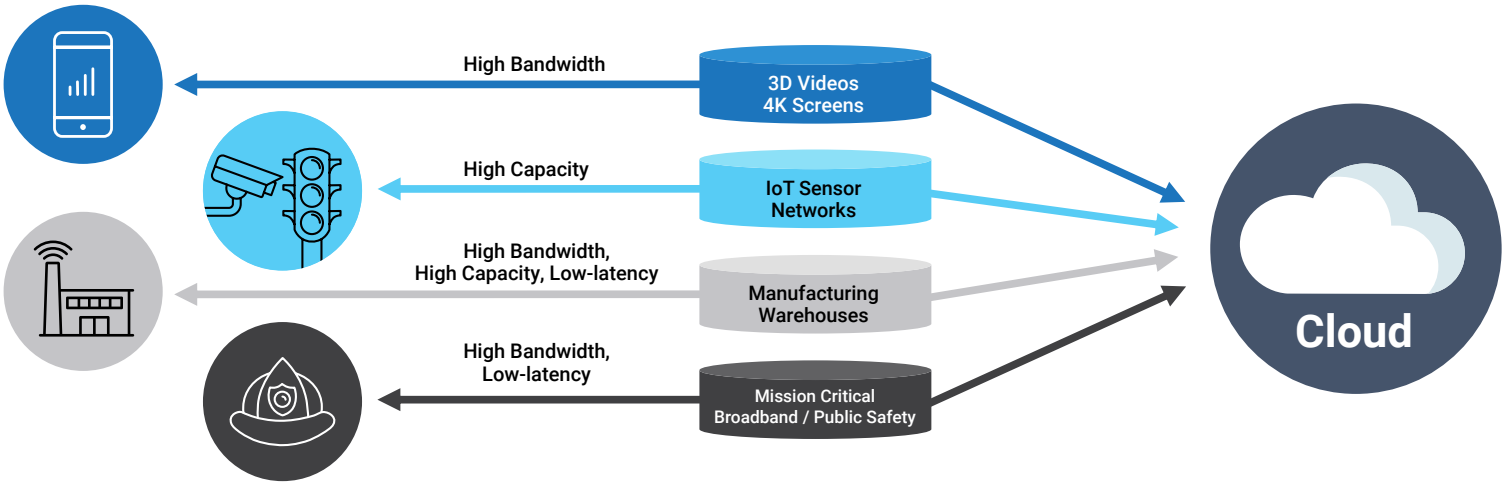
For this round of tests, the 5G Security Test Bed set out to evaluate and verify the security components of the Third Generation Partnership Project's (3GPP) technical specifications for 5G's advanced security capabilities, along with select measures recommended by the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) VII Working Group 2 report. The tests represent a first-of-its-kind validation of 5G network slicing. Specifically, the tests assessed standards for network slicing found in 3GPP TS 33.401 and 33.501, by investigating the security features associated with 5G network infrastructure and the devices that can access a 5G standalone (5G SA) network.

What Is Network Slicing?

A major new feature of 5G networks is network slicing, which enables operators to provide fine-grained, customizable services to meet the diverse needs of a variety of customers and applications, such as in public safety, transportation, or security contexts.

Network slices are a form of wireless network management whereby network segments are separated virtually across the same physical infrastructure. These network slices enable network operators to more efficiently support the needs of various users, enabling stronger security and higher capacity throughout the network.

Example applications include dedicated low-latency connections for connected cars, high capacity for smart cities, or multi-layered security for mission-critical operations. More examples are depicted below.



Key Findings

The 5G Security Test Bed successfully tested various properties of networks partitioned through network slicing, including authentication, segmentation, security, and data integrity, validating that:

✓ **Each user device and its data are authenticated and isolated to a specific slice.**
This test confirmed that the network properly authenticated each user device and registered it to the correct slice. Each network slice was completely segmented, and no data or traffic could flow between them, protecting the slices and user data from unauthorized access. This helps strengthen network security by ensuring bad actors cannot access other parts of the network if one slice of the network were compromised.

✓ **Additional security (IPsec encryption) can be added to individual slices.**
This test confirmed that IPsec encryption could be added to a specific network slice while maintaining isolation between the slices. This verifies that individual slices can meet the security needs of specific use cases without impacting other slices on the network—a factory worker using augmented reality may need a low-latency slice to ensure quick responsiveness, while a slice with additional encryption can be used to transfer login credentials without the need for lower latency.

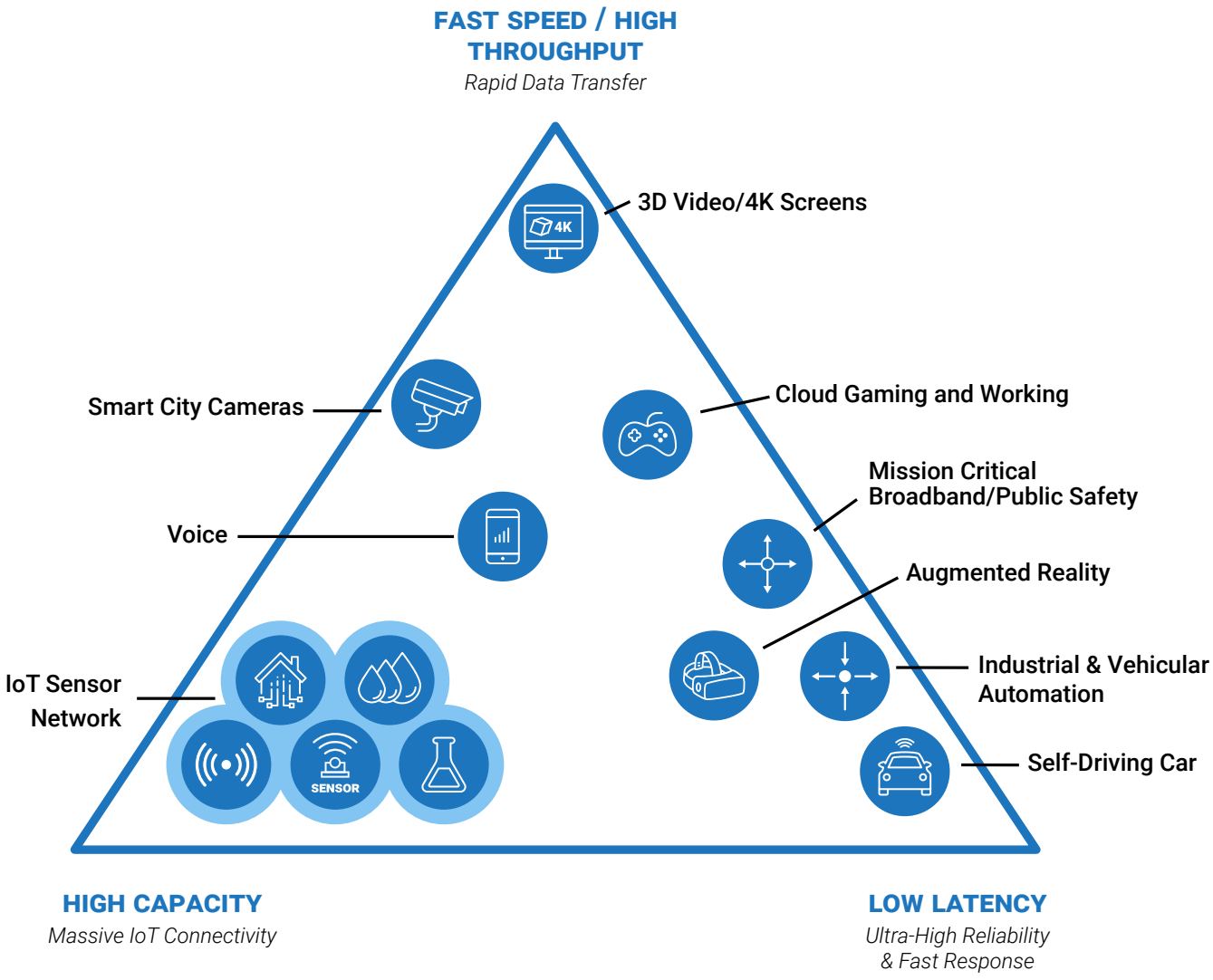
✓ **Overlaying two layers of encryption does not result in data loss.**
This test confirmed that two additional layers of encryption could be added to the 5G network's existing layer of encryption—for a total of three layers of encryption—to a specific slice, without negatively impacting its ability to effectively transfer data. This is important for networks that need highly secure segments, such as in national security use cases.

5G Security Test Bed Test Results: Successful Validation of Network Slicing Technical Specifications

This round of testing successfully verified the efficacy of implementing network slicing, and multiple layers of security in a commercially relevant 5G standalone configuration. It also showed that the security specifications and procedures outlined in the relevant 3GPP specifications are feasible and effective for network slicing.

Each of the three tests incrementally increased the level of security, from basic slice isolation in Test 1, to the addition of an encrypted tunnel on one slice for greater security in Test 2, to the addition of an end-to-end virtual private network (VPN) over the secure slice in Test 3.

NETWORK SLICING APPLICATIONS: NETWORK EFFICIENCY FOR FLEXIBLE USES



Test Case 1: Network Slice Authentication and Segmentation Security

Test Case 1 focuses on assessing whether devices on the network can authenticate and be assigned to the correct network slice, and that the network slices are completely segmented such that no traffic flows between them. The test network (transport network) was configured with two slices, and two devices were connected to the network. This test case demonstrated the following key findings:

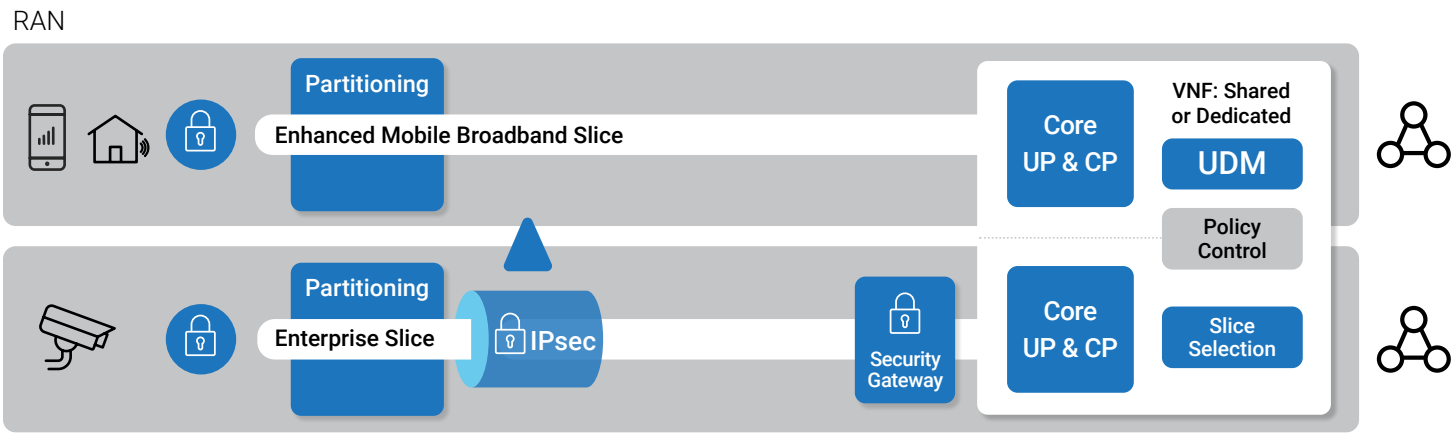
- The network properly authenticated each device.
- Each device registered to the correct slice.
- The two slices were completely segmented from each other across the virtual network.
- No data associated with one slice was visible from the other slice.

Test Case 2: IPsec Transport Protection for Highly Secure Slices

To protect both user and control traffic from eavesdropping or manipulation, carriers can put it in a secure tunnel (called an IPsec tunnel) while it traverses an untrusted link between a user device and the 5G core network. Test Case 2 builds on Test Case 1 by demonstrating the use of an IPsec tunnel to encrypt the data transmitted through one of the slices, creating an additional layer of security for that slice. The test demonstrated the following key findings:

- Both devices were properly authenticated and isolated on each slice.
- The IPsec tunnel was implemented on one slice with no errors or warnings.
- The IPsec tunnel successfully encrypted all of the traffic traveling through its network slice.

TEST CASE 2: NETWORK SLICE CONFIGURED WITH IPSEC TUNNEL ENCRYPTION.



Key: ▲ = Test Point in Device or Location

CP: Control Plane
eMBB: Enhanced Mobile Broadband
IPsec: IP security (encrypted tunnel)
UDM: Unified Data Management
UP: User Plane
VNF: Virtualized Network Function

Test Case 3: Multiple Layers of Encryption within a Network Slice

Test Case 3 builds on Test Cases 1 and 2 by assessing whether the addition of another two layers of confidentiality on top of the 5G network encryption compromises user application performance. In addition to the IPsec tunnel and the 5G network layer encryption, Test Case 3 added a layer of VPN encryption. The test demonstrated the following key findings:

- The device was able to connect to the highly secure slice with three layers of protection.
- Data loss during data transmission was negligible, indicating no impact on user application performance.

Why Test 3GPP Technical Specifications?

In the decentralized and virtualized networks that will make up 5G, advanced security measures should be considered in order to support ongoing security enhancements. 3GPP, which unites seven telecommunications standard development organizations, advances 5G work that utilizes security models that take a new and different approach to individual, endpoint, and core security.

3GPP has produced technical specifications covering a range of wireless network technologies and 5G network features. It continues to develop specifications that support security and privacy, that reflect the changing wireless network landscape, and that enable more efficient wireless network management.

What Is 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, and academia, created with a sole focus on testing and validating 5G security recommendations and use cases from government agencies, standards bodies, 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's founding members are wireless providers AT&T, T-Mobile, and UScellular; industry partners Ericsson, CTIA, the MITRE Group, and SecureG; and academic partner the University of Maryland, which also serves as the Test Bed Administrator.

The 5G Security Test Bed is guided by a Technical Advisory Committee (TAC) made up of the Test Bed's founding 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.

How the 5G Security Test Bed Advances 5G Security: A First-of-Its-Kind Approach

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 reflects the industry's collaborative approach to 5G security—it was created by the CTIA Cybersecurity Working Group (CSWG), an industry initiative that convenes the country's leading telecom and tech companies to assess and address the present and future of cybersecurity. The 5G Security Test Bed further builds on the work of a broad array of government agencies, policymakers, international standards bodies, thought leaders, and partners in the telecommunications and information technology sectors. These groups include 3GPP, the Alliance for Telecommunications Industry Solutions (ATIS), 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.

More specifically, 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.

Next Steps

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.

Future 5G Security Test Bed reports will cover additional phases of network slicing test cases and Phase 1 5G SA test cases, including CSRIC recommendations. Development is in progress for test cases focusing on false base stations and roaming security on 5G standalone networks. Additional anticipated test case topics include Open RAN, IMSI privacy, and new trust anchor solutions.

The Test Bed members and administrator welcome engagement from stakeholders with an interest in the mission of the 5G Security Test Bed, and we expect to develop more and diverse test cases along with new participants. To learn more about the 5G Security Test Bed or membership, read the full report, or view and download the report one-pager, visit www.5Gsecuritytestbed.com.


5G
SECURITY™
TEST BED