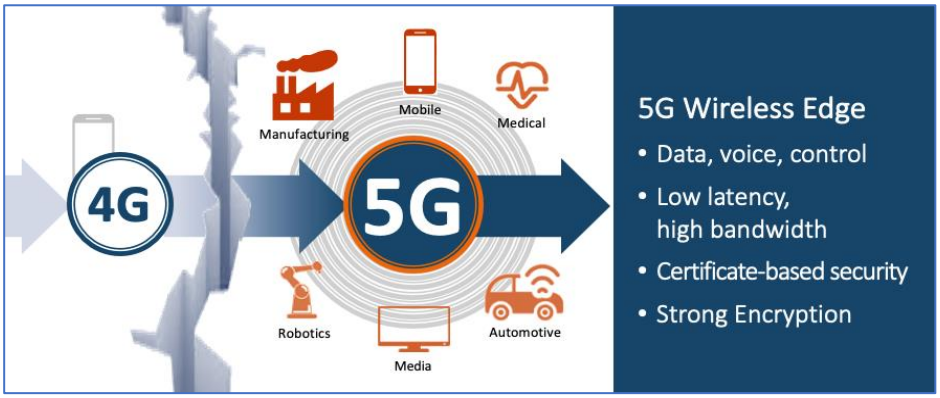
SecureG – The 5G Ecosystem Trust Broker

The 5G Revolution

Previous generations of mobile/ wireless technology represented an incremental ***evolution*** of capabilities and bandwidth. The transition to 5G instead is a ***revolution***, delivering a high bandwidth, low latency network to support the delivery of Industry 4.0 and Industrial IoT applications – smart cities, autonomous vehicles, real-time remote control, smart manufacturing and beyond.



5G Security Built on Certificates

The 3GPP approach to securing 5G communications relies heavily on digital certificates for authentication and encryption in many areas of the 5G ecosystem.

Supply-Chain Awareness

There is no greater risk to the security of a nation than failing to protect critical infrastructure (CI) – the power grid, manufacturing, transportation, financial institutions and more. And that infrastructure, increasingly automated with online access, is anticipating reliance on 5G for next-generation connectivity and control.

Key to protecting CI is ascertaining the *provenance* of the technology that implements it: where was it manufactured and integrated and by whom? When was firmware and other system software last updated? Verifying integrity and availability are essential to trust.

The promise of 5G can only be realized if networks offer a secure and fully vetted supply chain.

Who Does SecureG Serve?

SecureG protects the 5G ecosystem, enabling trusted interoperability between:

- Telecommunications carriers and operators
- Cloud service providers (CSPs)
- Multi-access edge computing (MEC)
- Enterprise networks
- IoT and IIoT devices
- Other networks, end-points and end-users

First to Market with ZT for 5G

What is Zero Trust?

Zero Trust (ZT) is an approach to security that recognizes modern networks no longer have a reliably secure perimeter. Zero trust protection requires:

- Strict device and session authentication
- Least privileged access
- Continuous validation

Why Zero Trust for 5G?

Just as 5G departs from earlier wireless paradigms, 5G networks require rethinking of approaches to cybersecurity:

- Multi-carrier, edge-centric networks have no perimeters
- 5G networks run primarily as virtual functions in the cloud
- Privilege and authentication vary across carriers and service types
- Multi-vendor networks need vendor-specific trust domains
- Certificate-based Identities are central to the 3GPP 5G architecture

Why SecureG?

SecureG, founded with strategic investment from MITRE Engenuity and CTIA, is uniquely positioned to broker trust on advanced 5G networks, offering:

- **Zero Trust** – PKI services to authenticate, authorize and encrypt 5G network systems
- **Ultra-High Reliability** and **Low Latency** – Supporting the stringent performance requirements of advanced 5G use cases
- **Security** – meeting FISMA/FEDRAMP standards for Critical Infrastructure
- **Supply-chain Awareness** – Ensuring control and visibility of network components through secure provisioning
- **Scalability** – Cloud-native PKIaaS that scales for Industry 4.0 and IIoT use cases
- **Interoperability** – Ensuring shared trust across 5G network connections, mobile edge computing, carriers and clouds
- **Design Wins** – U.S. Navy; other DoD, Federal and Enterprise wins in progress

Securing a Clear Path

SecureG enables the trusted machine identities for each step along a 5G system. Designed for high speed, low latency zero-touch deployments, SecureG's solution integrates to serve vendors through the ecosystem from Carriers and Cloud Service providers to IoT device manufacturers.

SecureG Products & Services

Trust Anchor

The SecureG Trust Anchor is built for a level of trust required by national Critical Infrastructure. It is the PKI foundation enabling trust among 5G carriers.

5G Certificate Authority

SecureG is the CA for 5G systems, issuing supply chain-aware enhanced certificates featuring provenance data and Zero Touch Provisioning,

The SecureG Bridge CA will issue the cross-certificates that enable trusted digital transactions. SecureG will also operate an Online Certificate Status Protocol (OCSP) responder for certificate validation data occurring at each digital exchange transaction.

SecureG-issued cross-certificates will secure a massive volume of trusted digital exchanges.

CA Security Operations Center

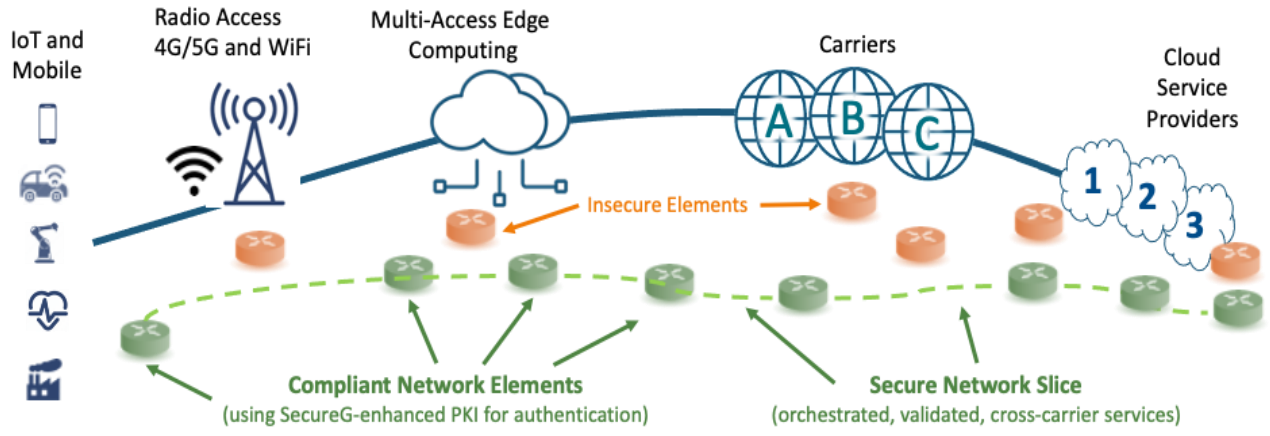
The SecureG SoC will support the full PKIaaS lifecycle including advanced security alerting, monitoring, detection, response, and continuous mitigation for clients of all sizes.

AI/ML Data Analytics

To PKIaaS customers and select third parties SecureG will offer in-depth analytics of transaction data and trends across the 5G network built on advanced AI/ML capabilities.

PKIaaS

SecureG will provide advanced PKI-as-a-Service (PKIaaS) functions featuring low-latency key management operating at the speed and scale needed for Industry 4.0 / IIoT applications.



A 5G secure network authenticated by SecureG digital certificates