Keyfactor for Telecom

Securing modern 5G networks and infrastructure

Establishing trust and compliance in public and private 5G networks with identity-first security.

Our world is more connected than ever; wireless network providers, operators, and OEMs are the beating heart behind it. Now, we want everything connected, all the time, no matter where it is. These are requirements that go well beyond the limits of Wi-Fi, so we turn to 5G networks. What was previously only thought of for cell phones is now being utilized in cars, wind turbines, critical infrastructure monitoring devices, and so much more.

The world relies on communication; security must keep up to scale

5G offers a high endpoint density allowing a single node to connect to a large number of devices, low latency to support time-sensitive network applications, and is not as susceptible to interference from the environment of the base station. This makes it a solid choice not only for the global networks we think of, covering miles and tens of thousands of connected devices, but also the new Industry 4.0 factories with all machines being smart.

While the cell phone market is quite mature, the new market for 5G IoT devices is still coming into its own. With the billions of devices that are set to come online in the next few years, this drastically increases the number of players in the market, and, consequently, the number of attack vectors. Silicon vendors, OEMs, and services providers alike all have a role in securing critical communications, in both public and private 5G networks.

Keyfactor solutions:

Trusted PKI

The foundation for trust in wireless and wireline networks is ensuring that every component is authenticated with a unique and verifiable identity — issued from a trusted PKI.

Secure code signing

Updates are inevitable. Signing and verifying firmware and performing secure updates ensures that only authorized code from legitimate sources can run on network endpoints.

Identity Management

Every identity must be managed to ensure that it can be renewed before it expires or revoked/ updated in the event of a compromised root certificate or a vulnerability in classical cryptographic algorithms.

3 unique challenges of 5G security

01 Scale

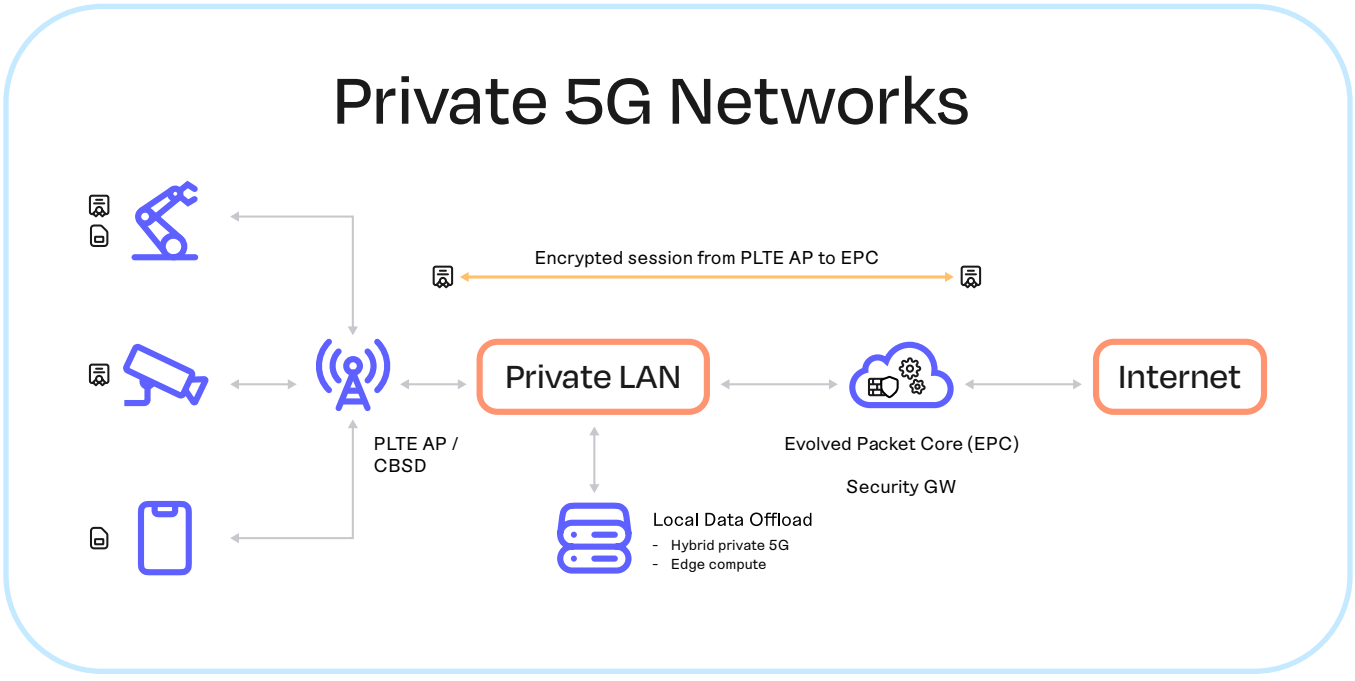
The number of 5G IoT devices is growing at an astronomical rate. Networks must be able to handle not only the increased throughput for each device, but also have proper validation in place to ensure that only valid devices connect to it.

02 Modernizing architecture

In public 5G, OpenRAN and mobile virtual network operators (MVNOs) represent a shift in communication technology and operations. The use of non-proprietary hardware and shared infrastructure opens new opportunities for business, but at the same time, brings new vulnerabilities.

03 Meeting standards

With rapidly evolving technologies come ever-changing standards. New standards and guidelines are continually being developed, like IoT SAFE and regional standards like the Telecommunications Security Regulation/ACT in the UK and the Cyber Resilience Act in the EU. Additionally, previous standards face revisions like the Canadian Telecommunications Act and those from 3GPP.



Protecting 5G networks with identity-first security

Whether working in public or private 5G, the goals are still the same: (1) communication between devices is secure, (2) every device is identified and trusted, and (3) devices can only be updated with authorized code. PKI-based identities and code signing are two proven methods of ensuring security throughout the entire 5G network.

Identity issuance

Every device connecting to a 5G network, and every piece of hardware comprising the network, needs a unique device identity. Not only that but these identities, in the form of certificates, must be standardized enough that different manufacturers can read and validate certificates from other manufacturers. With multiple standards in place, product designers need a solution that is flexible enough to meet all current requirements and stays current with new standards that are being developed, including post-quantum algorithms.

Scaling with the market

The pace of new smart, 5G product development will only increase. Security is paramount, but at the same time it can't be a bottleneck for production. When it comes to PKI, that means spinning up new issuing CAs quickly to meet certificate demands, while staying within budget and maintaining high availability.

Securing updates

Manufacturers and service providers must ensure that only authorized code can run on devices. If transmitted through insecure channels, the code could be intercepted, altered, then pushed down to their smart devices and networking equipment. Unauthorized code can lead to a breach or malicious attack to gain remote control, access data, or push ransomware not just to the device, but any other device on the network.

The Solution:

PKI and machine identity management

With identity-first security from Keyfactor, manufacturers and service providers can protect every device from RANs and eNodeBs to backhaul infrastructure and connected user equipment with a unique and trusted identity. Code signing then enables secure updates for network components and ultimately ensures that devices are secure, updated, and standard-compliant from design to end-of-life. Trusted by some of the largest IoT manufacturers, Keyfactor delivers identity issuance, governance, and operational efficiency at the scale the 5G market demands.

Scalable and flexible PKI

With support for a wide variety of protocols including ACME, EST, and CMPv2, EJBCA Enterprise is a highly scalable and extensible PKI platform for certificate-based identity issuance. 5G network providers and users can issue device identity and SSH certificates at a massive scale, whether during manufacturing, as an update in the field, or short lifespan-session certificates as a replacement for tokens. EJBCA PKI has a flexible architecture and can be deployed within a data center, in the cloud, or as a managed service.

Keyfactor EJBCA Enterprise

Learn more ↗

Secure code signing

Software and firmware updates are inevitable. SignServer Enterprise digitally signs code and validates signatures to ensure only trusted code is executed on connected devices and systems. The solution can leverage existing on-premises or cloud-based hardware security modules (HSM) or use a built-in HSMs with a turnkey hardware appliance.

Keyfactor SignServer Enterprise

Learn more ↗

Certificate lifecycle automation

A single certificate expiration can cascade to cripple an entire network. Keyfactor Command for IoT gives operators and manufacturers complete visibility and lifecycle management of all keys and certificates issued in their infrastructure and on their devices. Security teams can see the status of all certificates, then quickly and easily revoke, renew, and re-issue a single certificate or millions in bulk from a single platform, ensuring identities remain secure over the device's lifespan.

Keyfactor Command for IoT

Learn more ↗

Key benefits of identity-first security from Keyfactor

- Scale easily with rapidly growing demand
- Maintain standards compliance with customizable certificate templates
- Be post-quantum ready with PKI integrating the latest algorithms
- Stay flexible with an HSM-agnostic, multi-tenant capable solution
- One vendor for code signing and certificate issuance, management, and automation

Want more information about Keyfactor for 5G cybersecurity?

Learn more ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1.216.785.2946