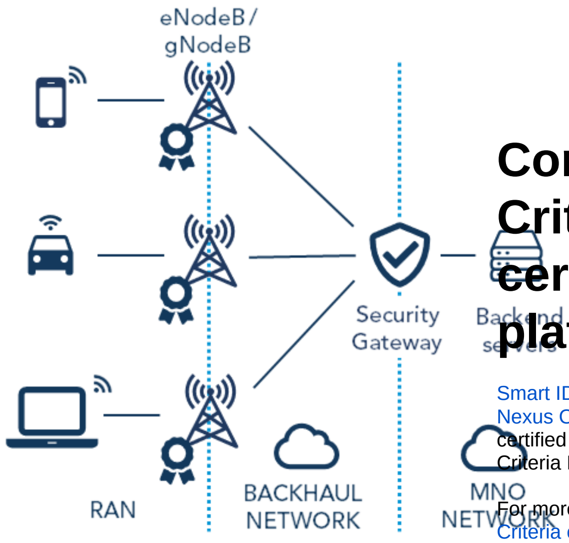
Telecom network PKI



Common Criteria certified PKI platform

Smart ID Certificate Manager (CM) and Nexus OCSP Responder have been certified in compliance with Common Criteria EAL4+.

For more information, see Common Criteria certification.

Nexus' solution for protecting telecommunication 4G (long-term evolution, LTE) and 5G networks with PKI certificates, is a high-security and multitenancy solution with automation features and a solid track record.

Telecom use case

A 4G (LTE) or 5G network is composed of the radio access network (RAN) that connects to mobile network operators (MNOs) via the base stations. Mobile network operators meet many challenges in protecting the telecom infrastructure, and many more challenges will come in the future. Telecommunication companies that want to grow and adapt to the internet of things (IoT), a mature and flexible public key infrastructure (PKI) platform is needed.

Telcos must encrypt the communication on the backhaul if it goes through public networks, and issue certificates to the different network components, as well as the users and servers that are involved, for a solid end-to-end protection of the telecommunication.

Nexus' solution

Nexus' LTE & 5G PKI solution follows the 3GPP standard and is based on Smart ID Certificate Manager and has the following features:

High security

Strong authentication and encryption are crucial to secure the communication between eNodeBs or gNodeBs and security gateways, as well as between eNodeBs or gNodeBs and their operations support systems (OSS). Encryption tunnels using certificate-based authentication, instead of passwords, ensure high security, scalability and automation.

Nexus’s mature and reliable PKI component framework provides the widest range of certificate issuing and management protocols on the market. This means that any standards-based network element, server, personal computer or smart card can get the certificates necessary to establish the highest trust across the mobile network from the base stations and deep into the core network.

Do you want to know more?

Contact us

Using the Nexus PKI platform enables mobile network operators to increase the level of protection and security in their networks. The robustness and readiness of the Nexus software improves the overall availability of the LTE or 5G infrastructure and becomes an excellent tool for providing good governance and efficient security management.

Protection against internal threats

Internal threats to the system also need to be considered. Nexus' PKI platform has functionality to protect from internal threats that most other PKI platforms do not include:

- Multi-person control can be enforced to security-sensitive operations, so that different roles must be involved in security critical operations.
- Out-of-the-box strong authentication is enforced to access the security infrastructure.
- All event logs are digitally signed and therefore protected against manipulation.

Vendor-independence

A PKI solution provided by the telecom equipment vendor could be relevant when the network is limited to single vendor base stations. However, as soon as base stations from various vendors are included in the network, an independent solution is needed. This scenario will become increasingly common.

Nexus' PKI platform is flexible about choice of vendors, and with an independent PKI platform, operators can increase and maintain security today and keep the security platform untouched when technology upgrades are needed.

Nexus' solution already supports multiple LTE devices and the list is continuously growing, to let you stay independent of certain telecom equipment vendors.

LTE equipment that supports SCEP or CMP can request certificates after being registered in CM.

The following devices are explicitly verified:

- Airspan AirHarmony 1000 ENB (CMP)
- Airvana/Commscope OneCell (CMP)
- Alcatel Lucent 9412 (CMP)
- CISCO 7600 Series Routers with SAMI (CMP)
- Ericsson RBS6000 (SCEP)
- Ericsson RBS6201 (CMP)
- Fortinet Fortigate Next Generation Firewall (SCEP, CMPv2)
- Huawei ENB (CMP)
- Huawei Femtocell BTS3202H, 3202E (CMP)
- Juniper SRX (SCEP)
- NEC eNB.
- Nokia Networks ENB (CMP)
- Nokia Networks Flexi Zone micro (CMP)
- XipLink, XS-SCPS TCP accelerator, XO-VPN

Automatic certificate enrollment

Automatic certificate enrollment, instead of doing the work manually, leads to lower costs, less administration and no risk of human error.

Nexus' PKI platform has an automated process for issuing certificates and allows full lifecycle management including device registration, certificate request authentication, certificate renewal, and revocation.

For the auto-enrollment and lifecycle management of the machine certificates, the PKI platform uses the standard protocols Simple Certificate Enrollment Protocol (SCEP) and Certificate Management Protocol (CMPv2) to request and renew machine certificates from the certificates authorities (CA) of the corporate PKI. Several other suitable standards and protocols for Telcos are also supported, such as ACME, 3GPP and EST (Enrollment over Secure Transport, RFC 7030).

Third party devices, clients, servers, and software components with built-in support for standards-based certificate enrollment protocols can benefit from the corresponding server-side support in Certificate Manager.

These are the supported standard-based protocols:

- **ACME** - Automatic Certificate Management Environment, RFC 8555
- **CMP**- Certificate Management Protocol, RFC 4210, RFC 4211
- **CMC**- Certificate Management over CMS, RFC 5273
- **EST**– Enrollment over Secure Transport, RFC 7030
- **EST-coaps**– EST over secure CoAP, IETF draft (draft-ietf-ace-coap-est)
- **SCEP**- Simple Certificate Enrollment Protocol, draft-nourse-scep-23
- **WinEP**- Windows certificate auto enrollment using Windows certificate templates

In addition to the standards-based protocols, listed above, CM provides protocols that offers additional features for customized clients, web front-ends, etc:

- **CM SDK**– CM Software Development Kit, a Java API.
- **CM REST API**- CM RESTful API.
- **C2X REST API**- RESTful API for V2X certificate enrolment.
- **CM WS**– SOAP Web Services

For more information, see Certificate Manager interfaces.

Multiple use cases and multitenancy

Apart from protecting the base stations, there are many other use cases for certificates. For solid end-to-end protection, users and back-end servers also need certificates. Nexus' PKI platform manages these certificates as well. Support for a wide range of certificate issuing and management protocols makes it possible to include any other PKI use case found in corporates, including out-of-the-box integration with internal IT systems such as servers, authentication clients and smart cards.

Multitenancy allows multiple CAs for different client organizations and use cases to run in a single service environment. Nexus’ PKI platform is truly multitenant. Each CA can be managed with separation of individual policies, issuing and maintenance processes, and separate groups of policy administrators in one platform.

Solid track record

Nexus' PKI solution is used in critical, large-scale, multi-CA deployments. The platform scales well in large device volume networks and helps the operator guarantee high availability by supporting automation, local high availability, load sharing using load balancers, and geo-redundancy support for appropriate disaster recovery plans.

An operator can manage certificates for multiple networks and countries in one central and well-managed service, instead of using multiple and less funded local initiatives. Several of the biggest mobile operators in Asia, Europe, and America trust Nexus' PKI platform.

Read more about the following customer case: How Vodafone Turkey keeps its rapidly growing network secure with PKI.