How to choose the right security for LTE infrastructures

Whitepaper

Release date: 2017-01-26

Introduction

The wireless communication standard Long-Term Evolution (LTE), also known as 4G, provides lower latency, higher throughput, ubiquity, and better security than its predecessors do. LTE networks are already available in more than 150 countries and offer connectivity for a variety of devices from smartphones to vehicles.

Global and national mobile operators are adjusting their business models to meet the needs of the internet generation. GSMA estimates that in 2020, 70% of the mobile connections will be over mobile broadband (3G, 4G and 5G technologies). Mobile users are accustomed to having broadband access wherever they are, using their smartphones to browse the internet, connect to social networks, send and receive e-mails, publish photos and films, and stream various online services. LTE networks are becoming a public infrastructure as critical as other infrastructures like railways, aviation or energy transport. The data transported over mobile networks is also increasingly sensitive and valuable, now that bank transactions and private information on social media is commonly handled via mobile devices.

Due to the requirements of higher throughput and the increasing number of connected devices supporting 4G (and soon also 5G), base stations need to be more closely spaced. This means that they have to be placed in easier to reach locations, in offices, public buildings, and homes, for example. Therefore, it is vitally important to protect LTE network elements from both remote cyber-attacks and physical tampering.

This paper covers how to choose the right protection for LTE infrastructures. We believe our public key infrastructure (PKI) platform Nexus Certificate Manager is the right choice in many cases, and we will explain why.

Background

An LTE network is composed of the radio access network (RAN) that connects to mobile network operator's (MNO's) via the base stations.

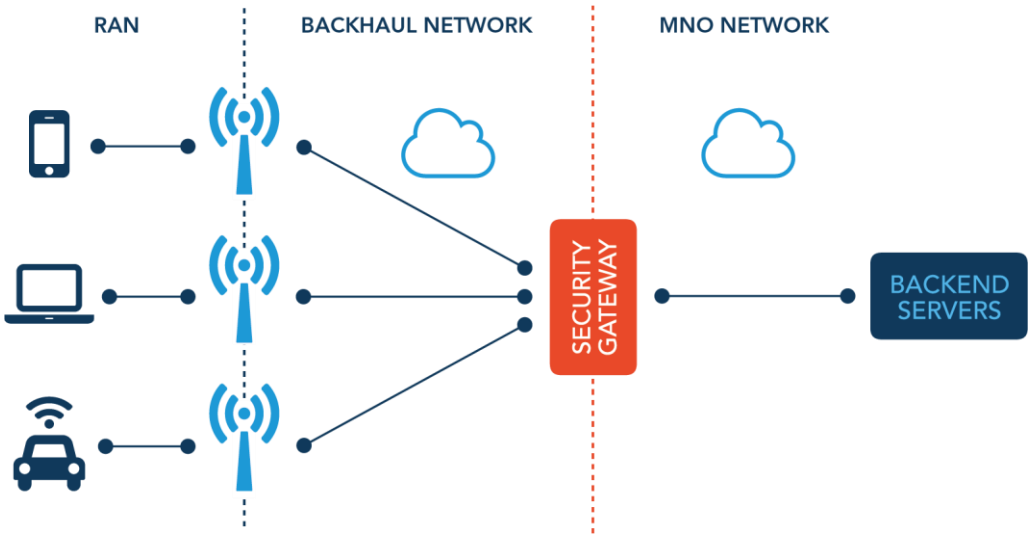

Figure 1. LTE network setup.

LTE networks face threats like device tracking, call interception, frequency jamming, physical base stations attacks, and flooding. Mobile network operators have to mitigate those risks to protect their assets and their reputation, and to guarantee their customers' privacy, confidentiality of exchanged data, and constant access to the mobile network.

To establish trust, the LTE network elements, such as the base stations (eNodeBs) and security gateway (SeGW), ensure confidentiality and system integrity by encrypting the link between the base station and the core network using IPSEC tunnel routing.

Tunnel peers will authenticate each other and negotiate keys to encrypt the traffic. There are two ways to authenticate: using shared secrets or X.509 certificates. Shared secrets offer short-term gains, as the technique is easy to implement, but have the same issues as passwords. That is, they are hard to generate, distribute, renew, and manage in other ways. Moreover, there is no guarantee that there is no register of the keys somewhere on the network. The problem with shared secrets is in the name: can a shared secret really be a secret?

X.509 certificates are a more secure solution. Every device has its own key and there are no shared secrets that can be hacked. There can however be issues with how to handle the X.509 certificates if they are not managed in a well-suited certificate management system. Manual administration of certificates is difficult and time-consuming. Several different security systems can be required to secure equipment from different vendors. With 5G and IoT, the number of network elements and vendors is likely to grow, with an expected increase in complexity and operational risk as a result.

Security will also become increasingly important, as a countless number of products could connect to the backhaul in future IoT projects.

How to choose the right security for LTE infrastructures

There is much to gain by carefully choosing the right security system for the LTE infrastructure.

To avoid the various issues raised in the previous section of this whitepaper, these aspects are the most important considerations (we will expand on each of them below):

- High security
- Protection against internal threats
- Vendor-independence
- Automatic certificate enrollment
- Future-proof
- Scalability, manageability and availability
- Multiple use cases and multi-tenancy
- Good track record

High security

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 for that matter) can get the certificates necessary to establish the highest trust across the complete mobile network from the base stations and deep into the core network.

Using Nexus Certificate Manager enables mobile network operators to increase the level of protection and security in their LTE networks. The robustness and readiness of the Nexus software improves the overall availability of the LTE 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 Certificate Manager 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

When choosing an LTE network security solution, it is important to consider the need for a vendor-independent security solution. 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.

In addition, to reduce project risks and costs when changing vendors, the security solution needs to be in place throughout the process.

Nexus Certificate Manager already supports LTE network devices from Airspan, CommScope, Alcatel Lucent, Cisco, Ericsson, Fortinet, Huawei, Juniper, and Nokia networks, and the list of supported vendors is continuously growing.

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 Certificate Manager 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, Certificate Manager uses the standard protocols Simple Certificate Enrollment Protocol (SCEP) and Certificate Management Protocol (CMPv2). These protocols are used to request and renew machine certificates from the certificates authorities (CA) of the corporate PKI.

Future-proof

When the IoT wave comes, there will be billons of unrelated devices that need to be securely identified. Only a highly scalable PKI can do the job.

Smart homes, smart cities, and smart transport is on everyone’s lips. 5G will arrive soon, with an ambition to cover all the possible IoT scenarios. Even if not yet fully standardized by 3GPP, 5G will connect the IP-based backhaul to a constantly increasing number of devices. Security will be a key focus. Nexus is an independent PKI vendor that strictly adheres to industry standards to guarantee the interoperability of involved devices from various vendors today and in the future.

The support for the EST protocol (Enrollment over Secure Transport, RFC 7030) in Nexus Certificate Manager is another concrete example of the Nexus vision, since this protocol is expected to play an important role in future IoT projects.

Scalability, manageability and availability

A mobile network operator wanting to grow does not want to be limited by a constrained PKI solution delivered from network equipment vendors. Scalability of the system is important. Nexus Certificate Manager is used in critical, large-scale, multi-CA deployments. The platform scales well in large

device volume networks. 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.

Another critical issue for mobile operators is to guarantee a high level of availability. Network outages caused by expiring certificates need to be avoided. Nexus Certificate Manager helps the operator to guarantee high availability by automation of manual processes and by its design. Certificate Manager is made to support local high availability, load sharing using load balancers, and geo-redundancy support for appropriate disaster recovery plans.

Multiple use cases and multitenancy

Apart from protecting the base stations, there are many other use cases for certificates. Users and back-end servers also need protection. A Nexus Certificate Manager installation also handles these types of certificates 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 Certificate Manager 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.

Good track record

Some of the biggest mobile operators in Asia, Europe, and America trust Nexus Certificate Manager. A large number of organizations are also trusting Nexus Certificate Manager for other use cases than mobile network security. For almost two decades, security conscious customers like banks, governments and trust-centers have relied on Nexus Certificate Manager to reduce risk and secure assets.

Certificate Manager is a flexible and scalable CA software platform, used to issue electronic identities (eIDs) to people, software and things. It can manage the full life cycle of all kinds of digital certificates used to ensure the trustworthiness of the issued eIDs.

When it comes to people, there are three main scenarios for PKI usage: enabling trusted identities for workforce members, online customers, and citizens. The trusted identities are used for everything from enabling contracts to be signed online, to granting secure access to physical and digital resources.

Certificate Manager is already used to secure IoT and as certificate-based security standards are adapted to low power IoT networks, it becomes important to choose an independent PKI vendor.

Conclusion

Mobile network operators meet many challenges in protecting the LTE infrastructure, and many more challenges will come in the future. For the operator that wants to grow and adapt to future possibilities with IoT and 5G, a mature and flexible PKI platform is needed. Certificate Manger creates flexibility 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.

As shown in this whitepaper, Nexus Certificate Manager meets all the needs, offering CA functionality, as well as support for the EST, SCEP, and CMP protocol services. It is not limited in terms of number of CA's or certificate templates which makes it ideally suited to be the foundation of a global or national PKI service for a mobile operator.

How to contact us

For more information, please send an email to contact@nexusgroup.com or go to www.nexusgroup.com.

References

GSMA Mobile Economy, http://www.gsma.com/mobileeconomy/
RFC 7030, Enrollment over Secure Transport, https://tools.ietf.org/html/rfc7030