Nokia Siemens Networks LTE transport security

Executive summary

Securing LTE transport effectively

Executive summary

1. Market trends, challenges and opportunities

Security is a ‘must’ to take full advantage of LTE

When talking about LTE we usually associate enhanced user experience through high speed, fast reaction and extended broadband coverage in rural areas. LTE also stands for higher efficiency provided by simplified and flattened architecture, all IP transport and high efficient radio technology providing higher data rates at reduced cost. LTE also opens up manifold opportunities for new revenues by offering new services and finding new business models and partners. First LTE networks are already in commercial operation today and others are going to start in 2011. But to fully exploit the opportunities also security has to be ensured. In particular, the flat all IP architecture requires special attention on security.

In 2G and 3G all transferred data are encrypted from the user device to the Radio Network Controller, which used to be physically protected and located inside a trusted building. With LTE the encryption is terminated already in the base station. Modern technology and miniaturization has reduced size and energy consumption of the base stations drastically and enabled installations increasingly in public places. This exposes base stations to unauthorized access.
In addition, the high bandwidth provided by LTE requires an efficient all IP transport network, which is by nature more open than traditional transport networks and might also be shared with other parties. Therefore the data transfer from the base station to the core network needs to be specifically secured with IP security (IPSec).

Threats are manifold and the business impact can be dramatic. For example: eavesdropping of voice and data can damage the trusted customer relationship between CSP and customers and force the customers to churn. Unauthorized access to the core network can cause denial of service or even corrupt the CSP’s systems e.g. the billing systems.

Why 3GPP compliance matters

In order to provide the same level of security as for 2G and 3G the standardization bodies have issued technical specifications for network domain security, authentication framework and security architecture. In order to secure the LTE transport effectively, it is important that the IPSec tunnel between base station and security gateway is setup between trusted network components to ensure that only authorized components get granted access to the network. According to 3GPP a strong authentication using certificate authority as in Public Key Infrastructure (PKI) is required. Some vendors provide authentication using shared keys. But this is only doing it by halves. Using one shared key for all eNodeBs is dangerous. If the key is compromised, all eNodeBs are compromised. Using different keys for each eNodeB would not be manageable. Therefore, only using certificate authorities according to PKI provides comprehensive security in a manageable way.

Benefits of LTE transport security:

Customers can enjoy all the advantages of LTE with the same high level of security they are used to in 2G and 3G networks. CSPs protect their reputation and their infrastructure as a sustainable basis for new business models and business partners.

2. Solution/Product overview

Our LTE transport security offering comprises:

3GPP compliant certificate authority and IPSec based solution

- Consulting
- Architecture & Design
- Implementation
- Support

and includes as Hardware/Software Components:
- Certificate Authority
- Security gateway with Firewall and VPN

3. Why is Nokia Siemens Networks your best partner?

Our LTE Transport Security solution is today (December 2010) the only 3GPP compliant certificate authority and IPSec based solution for LTE transport in the market.

We are currently the only vendor who provides a complete end-to-end security solution for LTE transport networks with a live deployment experience. Our end-to-end solution includes built in IPSec in our eNodeBs with high throughput ensuring highest performance.

Our solution is pre-validated against our NSN LTE RAN technologies as well as RAN from other leading vendors

Our solution enables efficient operation through fully automated certificate life cycle management for both eNodeB and Security Gateway.

Our solution provides strong and automated authentication of eNodeB's and Security Gateway's by using certificates and a Certificate Authority

We deliver pre-validated integration into the CSPs Operations Support Systems