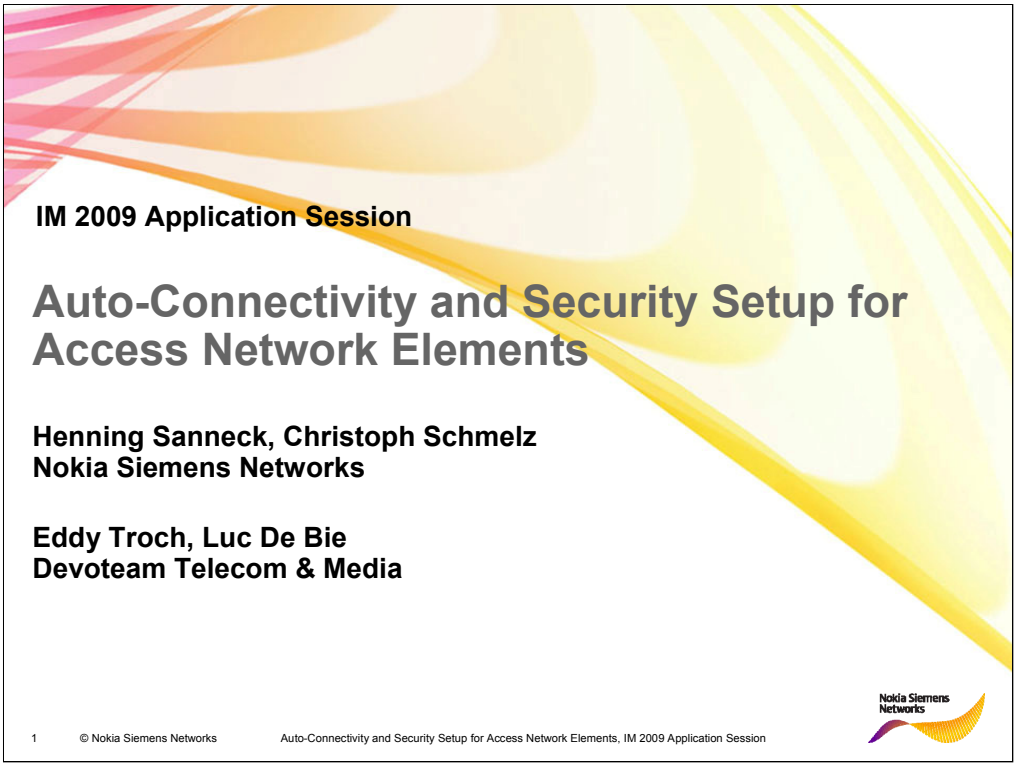
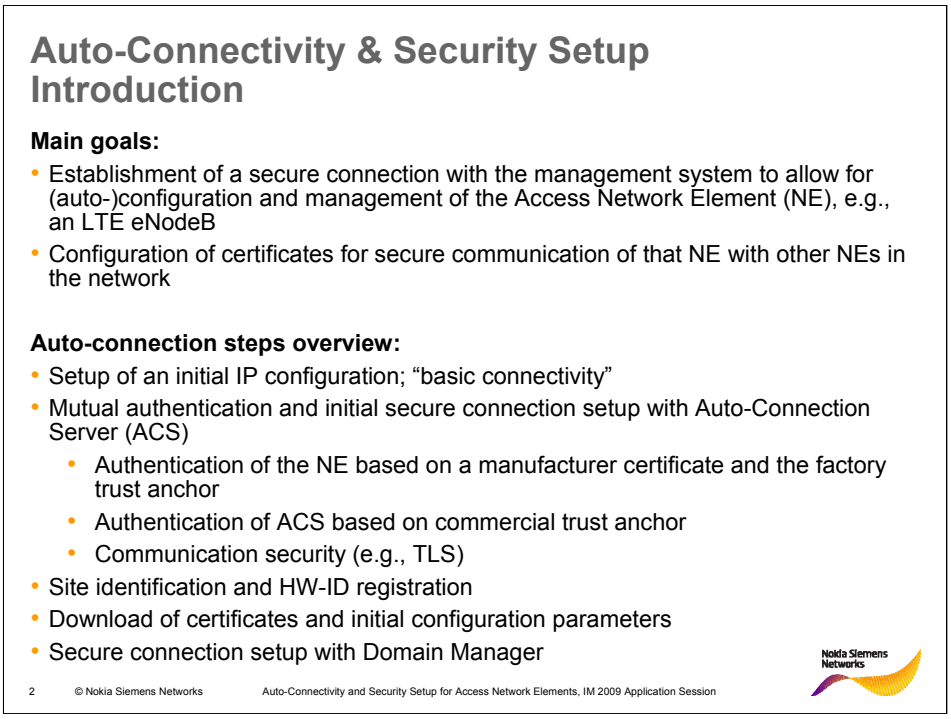


Abstract:

In access networks, the roll-out of new network elements (NE) or changes to the NE HW and SW cause considerable overhead. The total number of NE is significant and is increasing for new radio access technologies like Long Term Evolution (LTE) due to the decreasing cell size. Furthermore for network scenarios like femto access points / home NEs conventional network deployment and management approaches where the network is fully planned and NEs are tightly managed cannot be followed any more. Furthermore the increased security requirements by operators for such network deployments have to be observed.

An auto-connectivity scheme which incorporates the NE's security setup is proposed which tries to balance the trade-off between automation (avoiding any manual intervention) and security. This is achieved by shifting manufacturer and operator activities to a preparation (rather than the actual roll-out) phase and eliminating any interaction between them as much as possible. The NE is delivered only with an "off-the-shelf" software & configuration installation. Only at the point in time when the NE is placed on site, the NE hardware-to-site mapping happening is executed. Together with mutual authentication between NE and the Operation, Administration and Maintenance (OAM) system it is possible to enable a very flexible and secure roll-out process.



The automated establishment of OAM connectivity aims at reducing the need for costly on-site personal to enter initial configuration parameters. This is achieved by having the access Network Element (NE), e.g. a base station for the LTE radio access network called "eNodeB", to acquire the initial parameters from a DHCP server and an Auto-Connection Server (ACS) in following consecutive steps:

• **Setup of basic connectivity**: the NE acquires an initial IP configuration for communication with the ACS by means of the Dynamic Host Configuration Protocol [1]. The initial IP configuration may be replaced by a permanent OAM IP configuration during a subsequent auto-configuration step.

• **Initial secure connection**: it is assumed that security will be based on public keys for authentication, integrity protection and confidentiality protection. The NE will use a certificate for its communications with other NEs. This certificate is generated by the operator's Certification Authority (CA) and needs to be downloaded to the NE. Furthermore the NE needs an operator trust anchor (root certificate) for verifying the certificates received from other NEs while in normal operation. Since initially the operator anchor certificate is not available, it is proposed that the NE uses temporarily a trust anchor of a public CA (e.g. Verisign**,** GlobalSign etc.) to communicate with the ACS. When an NE is purchased, a manufacturer certificate is handed over to the operator and stored at a Certificate Database. During auto-connectivity setup the NE includes the manufacturer NE certificate with the TLS handshaking, allowing the ACS to verify whether the dedicated NE can be authorised to attach to the mobile network.

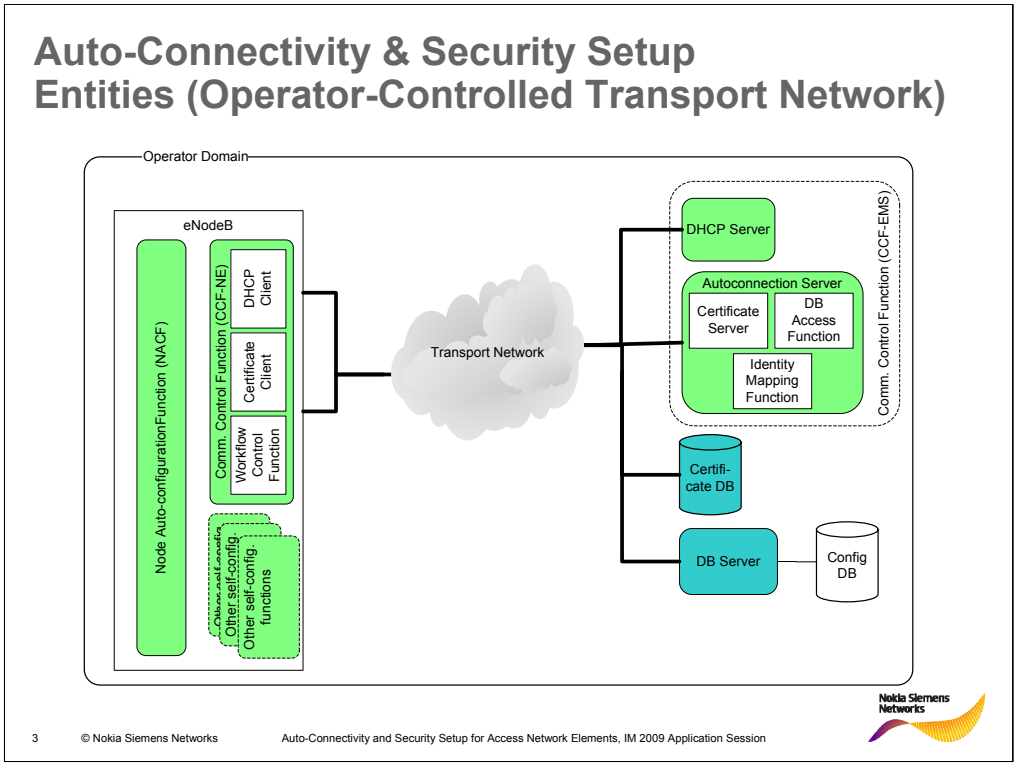
• **Site identification** is required to define which off-line prepared configuration data shall be used for the NE. Typically dedicated configuration data for every site is required.

• **HW-ID registration** makes the new equipment visible in the network topology database.

• **Downloading of certificates and initial parameters**: in addition to the certificates the NE is provided with addresses and parameters for further (auto-) configuration and management.

• **Secure connection setup with Domain Manager**: the temporary TLS connection with the ACS is torn down and a new secure connection is established, now using the certificates downloaded in the previous step. This connection may be protected by TLS or IPsec according to the operator's preference.

The described process can be seen as a concrete "self-configuration" or "self-establishment [2] concept for the network build phase, thereby realizing a part of the overall "Self-Organizing Networks" (SON) vision [3]. This work is based on an earlier IM application session contribution [4], significantly extending the concept presented there by enabling security establishment and site-to-HW-mapping.



The auto-connection and security setup is performed by a Communication Control Function (CCF) residing both at the NE and the NE's Element Management System (EMS). Components of the CCF at the NE retrieve initial configuration data from components at the EMS, orchestrated by a Node Auto-Configuration Function (NACF). The NACF may control additional self-commissioning functions of the NE such as software downloading, configuration database downloading, self-testing etc., but these functions are out of scope for this presentation.

The components on the NE side fulfil the following functions:

• **DHCP client:** retrieval of the initial IP configuration;

• **Certificate client:** establishment of a secure TLS connection and retrieval/storage of the NE certificates;

• **Workflow control function:** retrieval and storage of parameters for self-commissioning.

On the Element Management System side the EMS-CCF includes the components to which the NE communicates directly; the other components are needed to supply their information indirectly via the Auto-Connection Server:

• **DHCP server:** supplies the initial IP configuration and the Auto-Connection Server address;

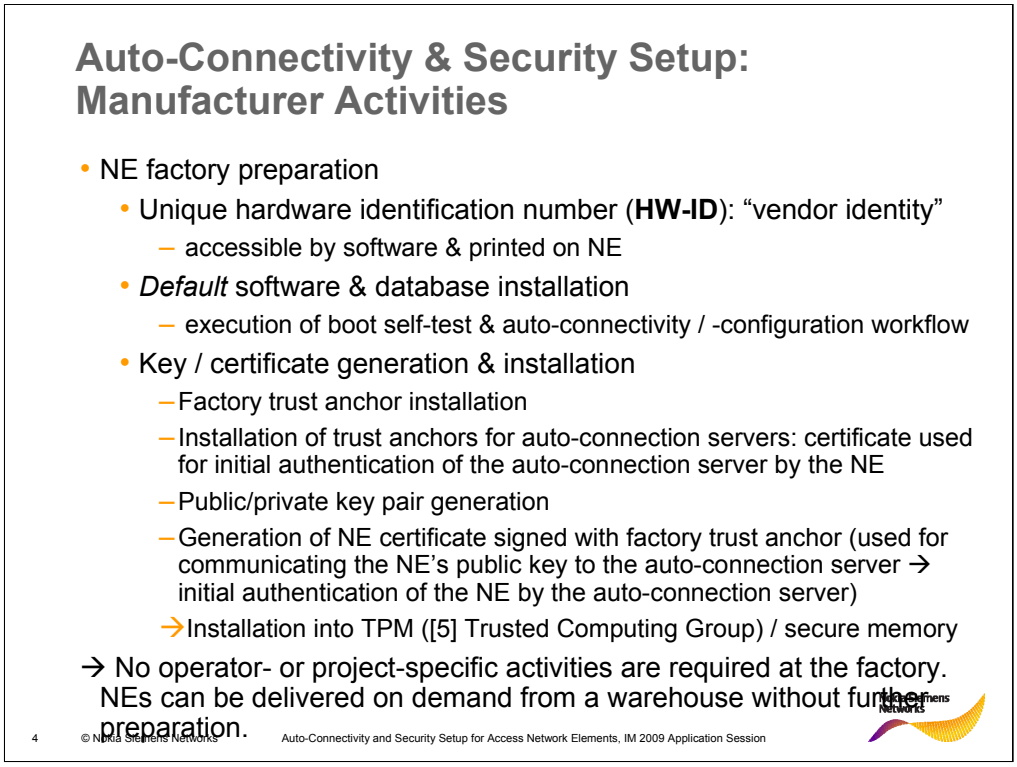
• **Certificate Server:** TLS connection peer, NE authentication and Certificate provisioning;

• **Certificate Database:** holds the operator trust anchor and the NE certificates created by the operator Certification Authority for all NEs purchased;

• **Identity Mapping Function:** determines the identity of the radio site where the auto-connectivity setup is originated from;

• **Database Access Function:** supplies the initial configuration data and registers the hardware identity of the installed NE;

• **Database Server:** a Configuration Management database function of the Domain Manager (EMS) for extracting configuration data from planning files, registering the hardware identity of a site and updating the network topology.



In order to support the auto-connection process some pre-configurations are needed by the manufacturer and the mobile operator.

Preparation activities by the manufacturer:

The proposed concept for auto-connection has been carefully designed to avoid pre-configuration of the NE from the factory with any operator or installation site specific parameters or software. This simplifies the manufacturing processes and allows an NE to be shipped to any customer and site.

• The NE is assigned a hardware identity (HW-ID) which is a serial number used by the manufacturer to identify the NE for purchasing and service purposes. In addition the HW-ID is used as a basis for creating NE certificates. The HW-ID is in principle assigned for the lifetime of the NE and cannot be altered.

• NEs shall be shipped from the factory with an initial software and configuration data supporting the initial booting, the auto-connectivity and security setup and the (auto-)configuration. All other software packages – dependent on the hardware configuration and the mobile network where the base station is installed – shall be downloaded on-site as part of a subsequent auto-configuration or manual commissioning step. This is feasible for LTE since the available transport bandwidth is much higher as compared to 2G and 3G networks.

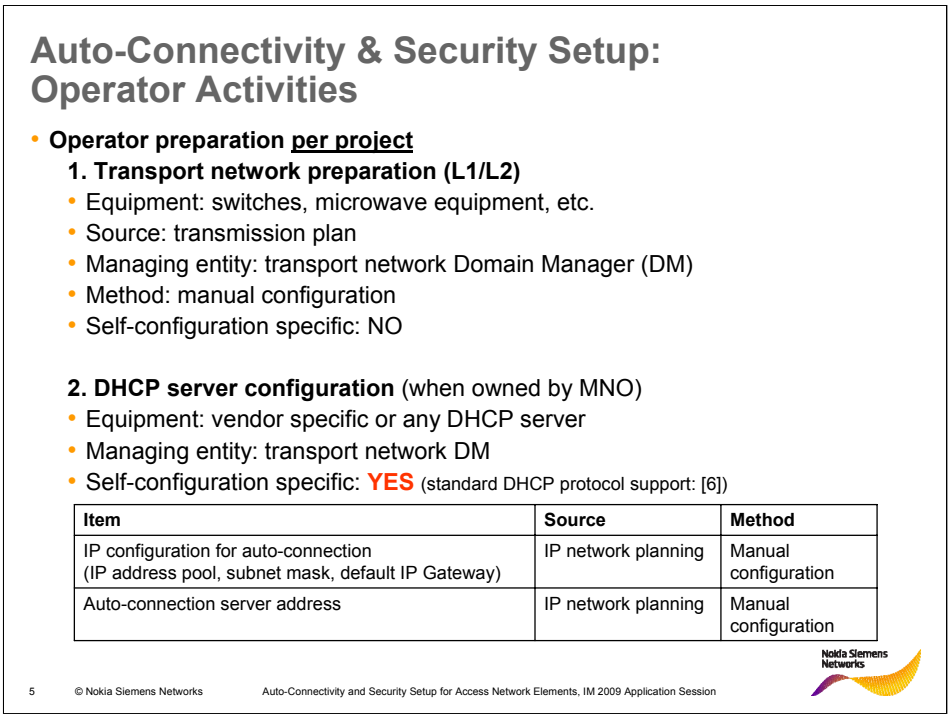
• Key / certificate generation and installation:

The factory trust anchor is needed for software and license integrity verification purposes.

A set of trust anchors from public Certification Authorities is installed to allow for the initial TLS connection setup with an auto-connection server. The operator can decide which CA will be used by the ACS for creating the ACS TLS certificate.

For optimal security, an NE should generate its own public/private key pair during the manufacturing process, such that the private key does never need to be revealed outside the NE. The NE then requests a certificate for its public key to the factory CA and stores the certificate locally. When the NE is sold to an operator, the factory signed NE certificates are handed over to the operator.

For the generation of keys and secure storage of the keys and certificates the NE may be equipped with a Trusted Platform Module (TPM), standardised by the Trusted Computing Group.

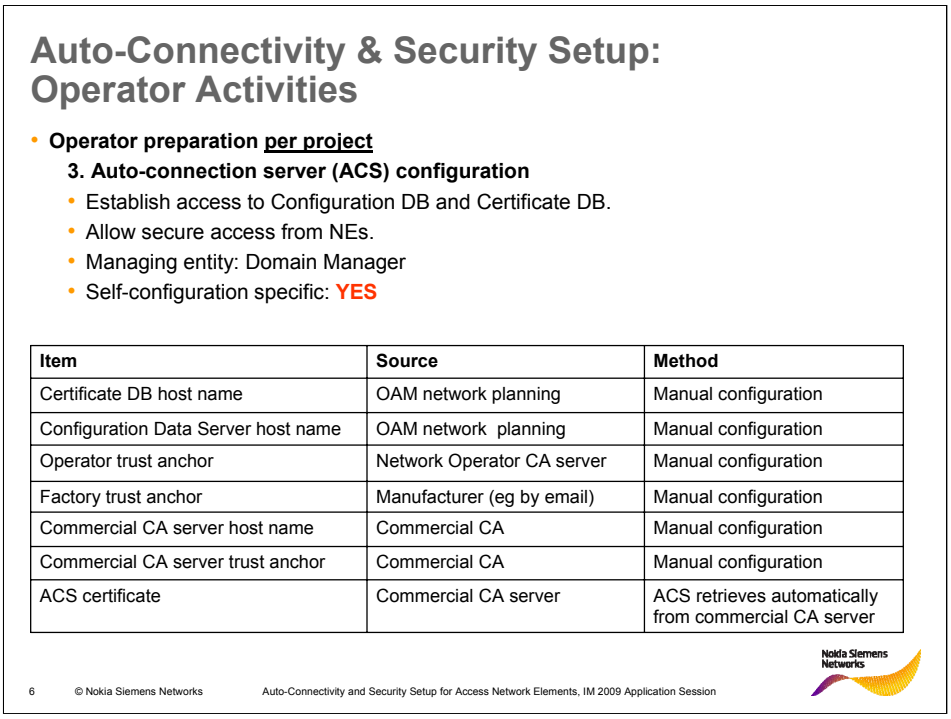


The operator preparation activities need to be split in tasks that are needed per project and per NE. A project could involve e.g. the rollout of a set of new base stations to improve radio coverage or network capacity. Per project preparations need to be executed only once for the auto-connection of a large number of NEs. Only few additional preparation activities need to be introduced for the auto-connection feature. These preparations are replacing the configuration activities that would otherwise be performed by installers and remote commissioners. The operational costs for the additional preparations are negligible in comparison to the operational cost savings of the site installers and remote commissioners.

Operator preparations per project:

• **Transport network preparation** deals with the configuration of microwave equipment in the "last mile" of the transport access network, as well as the configuration and traffic engineering of virtual LANs and Virtual Private Networks in the aggregation and core transport networks. Where the operator deploys third party transport networks this preparation activity is outsourced to the corresponding service provider.

• **DHCP server configuration** entails the provisioning of the initial IP configuration and auto-connection server (ACS) address to be used by the NEs during an auto-connection/ self-configuration. The ACS address is a vendor specific DHCP option which is only interpreted by NEs with the auto-connectivity feature implemented. Most commercial DHCP servers allow for the configuration and distribution of vendor specific DHCP options.



Auto-Connection Server configuration:

Addresses and certificates are configured to enable access to and from the ACS.

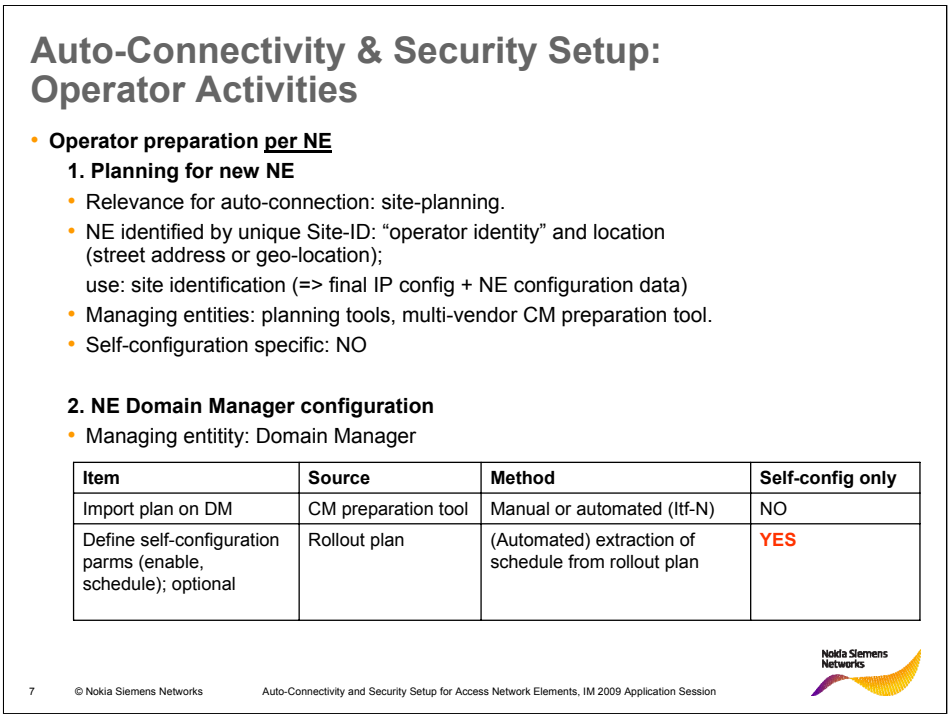
Access to the Configuration Database is needed for retrieving auto-configuration data and updating the network topology.

Access to the Certificate DB is required to retrieve the certificates for an NE.

The operator trust anchor is used by the ACS for distribution to the NEs.

The factory trust anchor is used by the ACS for authenticating the NE and ciphering the TLS connection.

The commercial CA server host name and trust anchor are needed by the ACS to securily retrieve an ACS TLS certificate.



Operator preparations per NE:

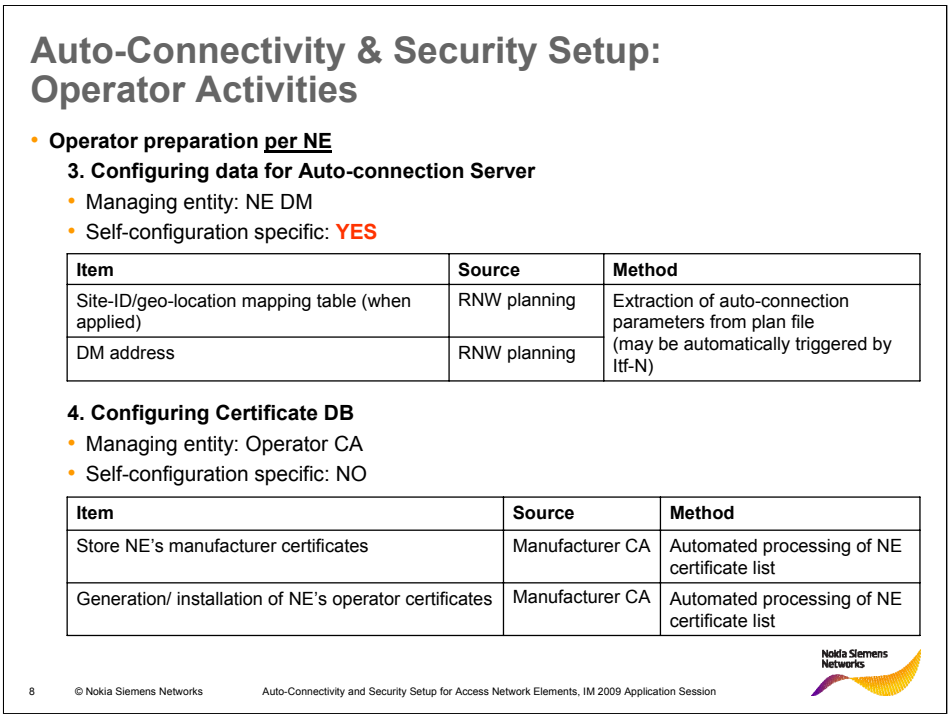
For the insertion of new NEs in a network a transport and radio network planning needs to performed prior to the installation. This is not different when auto-connection will be deployed.

Access Network Element planning is an activity of the operator's planning department supported by specialised planning tools. For the planning process, operators identify NEs by means of the "Site-ID". A Site-ID identifies the unambiguous planned (geographic) location of an NE, and is used as identifier for the NE configuration data. The Site-ID has an operator specific format and is therefore defined as a string data type. It may contain a postal address in conjunction with further location designations, e,g, "Site: Claudiusstr.1, 10557 Berlin Rack:x", or may even include GPS coordinates.

The auto-connection process may require the output of the site planning (part of the network planning) for the site identification task. With the Site-ID it is then possible to find the permanent IP configuration and further configuration for the NE. But before this can happen the planning output must be transferred from the planning tools to the Domain Manager. In many cases this is handled by a multi-vendor configuration management preparation tool. The operator may need to start a task on the Domain Manager to retrieve the planning files, or the Domain Manager may be ordered via a standardised interface to download the files.

The operator may also configure the Domain Manager to enable auto-connectivity setup or schedule the auto-configuration tasks according to an NE rollout plan.

In particular the Site-ID is important for base stations in a mobile network as it refers to the geographic location and thus is inherently part of the radio planning done by the mobile network operator.



Operator preparations per NE:

• Auto-connection Server preparation:

After the Domain Manager has stored the radio network (RNW) planning files a subset of the data shall be extracted and transferred to the ACS. In case the planning files are received by means of the 3GPP bulk Configuration Management IRP (Integration Reference Point), this function can be automatically invoked. This way the data is readily available at the ACS for processing auto-connection requests.

• Certificate Database preparation:

Each time a set of NE is purchased and manufactured the operator shall receive a list with NE certificates from the manufacturer, typically via e-mail. The operator Certification Authority verifies and signs the NE certificates received from the manufacturer. The operator CA shall store both the manufacturer certificates and the operator certificates at the Certificate Database, ready for retrieval by the ACS. Depending on the capabilities of the operator CA, the processing of NE certificate lists may be automated by means of a dedicated application or a generic workflow engine triggering a series of low-level commands.

Auto-Connectivity & Security Setup: Site identification & HW-to-Site mapping

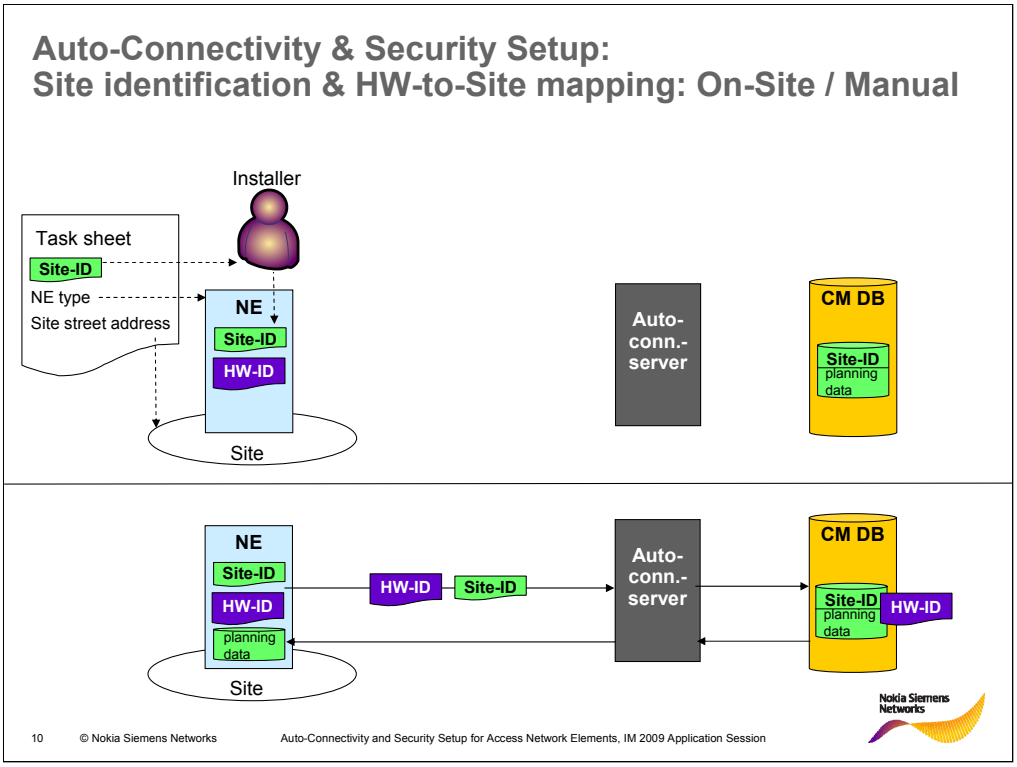
Info insertion	*Manual*	*Semi-automated*	*Automated*
*On-site***	Planned Site-ID entered manually by installer	Measured Site Location using mobile GPS receiver (PDA) plugged into NE via Eth	Measured Site Location using fixed antenna mounted GPS receiver
Remote	HW-ID & planned Site-ID received in human-readable form via paper or phone call from installer, HW-ID entered manually into database	HW-ID read with barcode scanner into PDA, Site-ID entered into PDA, received from installer via SMS / Web interface, HW-ID entered automatically into database	n.a.

** The matching / mapping of the IDs is always done at the server side obviously (matching of a measured location against the planned ones yielding a Site-ID, mapping from HW- or Site-ID to the correct planning data)

The site identification task of the ACS involves the determination of the exact site where an auto-connection is being issued. Once the site has been identified the hardware identity of the installed NE is linked with the Site-ID in the configuration database. This is further referred as “HW-to-Site mapping”.

Several mechanisms can be used for the site identification, ranging from solutions with some human assistance up to a fully automated one:

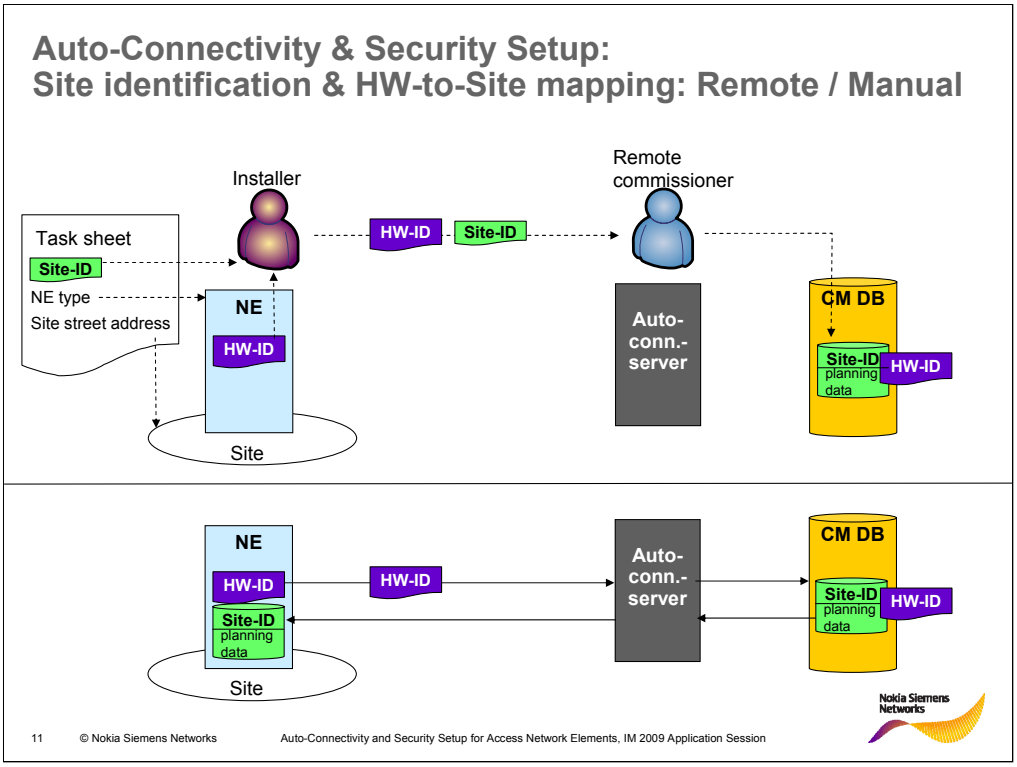
- Before the auto-connection process is started the Site-ID is entered manually by the installer and is then transferred with an auto-connection request to the ACS.
- Before the auto-connection the installer informs a remote commissioner about the HW-ID and Site-ID of the new NE. The remote commissioner then enters the HW-ID/Site-ID correlation in the configuration database of the Domain Manager. During the auto-connectivity setup the ACS queries the configuration database with the HW-ID to find the corresponding Site-ID.
- Semi-automated variant of the previous solution: the installed HW-ID is collected on-site from a sticker by means of a PDA with integrated bar code reader. Installer then also enters the Site-ID and initiates an SMS, e-mail or web session for updating the configuration database. In contrast with the previous solution there isn’t any remote commissioner support needed.
- The installer collects the geographic coordinates of the site by means of a handheld GPS receiver and transfers them to the NE via a proper interface (e.g. Ethernet). The ACS maps the GPS parameters to the Site-ID by means of a geographic matching algorithm.
- The site coordinates are automatically captured by means of a fixed antenna mounted GPS receiver. This solution is cost effective when a permanent GPS receiver is needed at the base station for radio synchronisation purposes.



Site identification entered by installer:

- NE is installed on the site.
- Installer connects a laptop or PDA to the NE, reads the Site-ID from the installation task sheet and enters the Site-ID in the NE database.
- Installer starts the auto-connectivity setup at the NE.
- NE establishes a secure connection with the ACS and sends an announcement message, including the HW-ID and the Site-ID.
- ACS accesses the configuration database to check the plausibility of the Site-ID, to enter the HW-ID in the database record related with the Site-ID, and to retrieve a subset of the planning data related to the site. The planning data subset is then forwarded to the NE.
- NE can perform an auto-configuration on the basis of the parameters received.

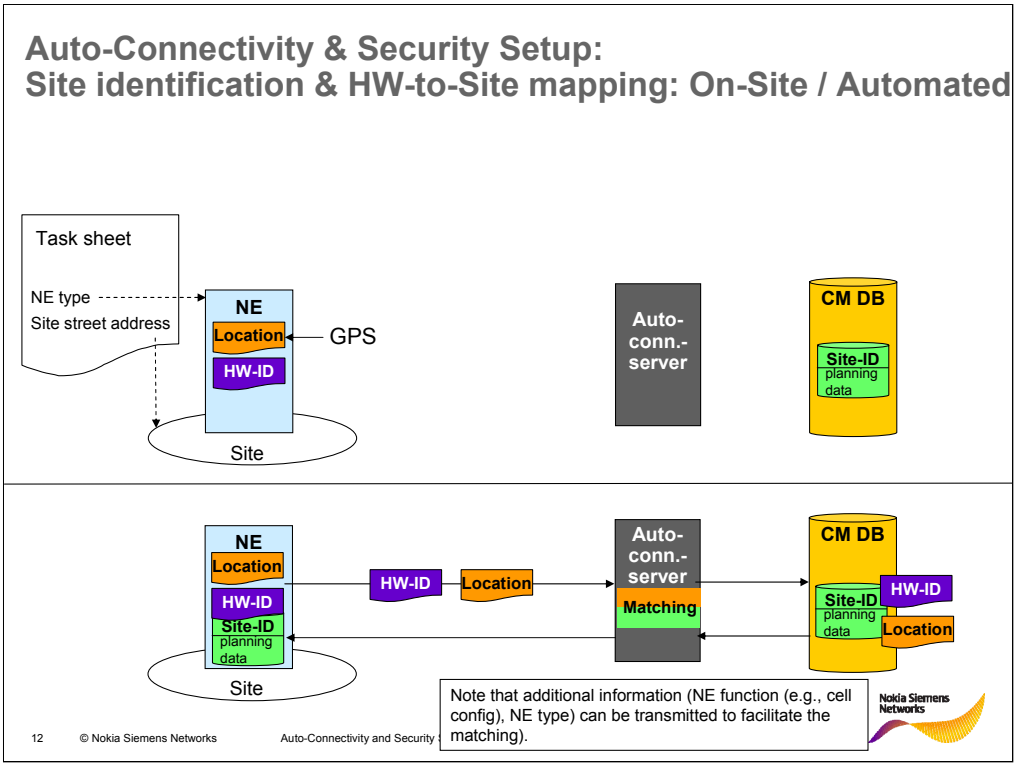
With this solution the benefit of the auto-connectivity and security setup feature is largely reduced, since the installer needs to carry and connect a laptop/PDA and be sufficiently skilled to configure the Site-ID.



Site identification entered by remote commissioner:

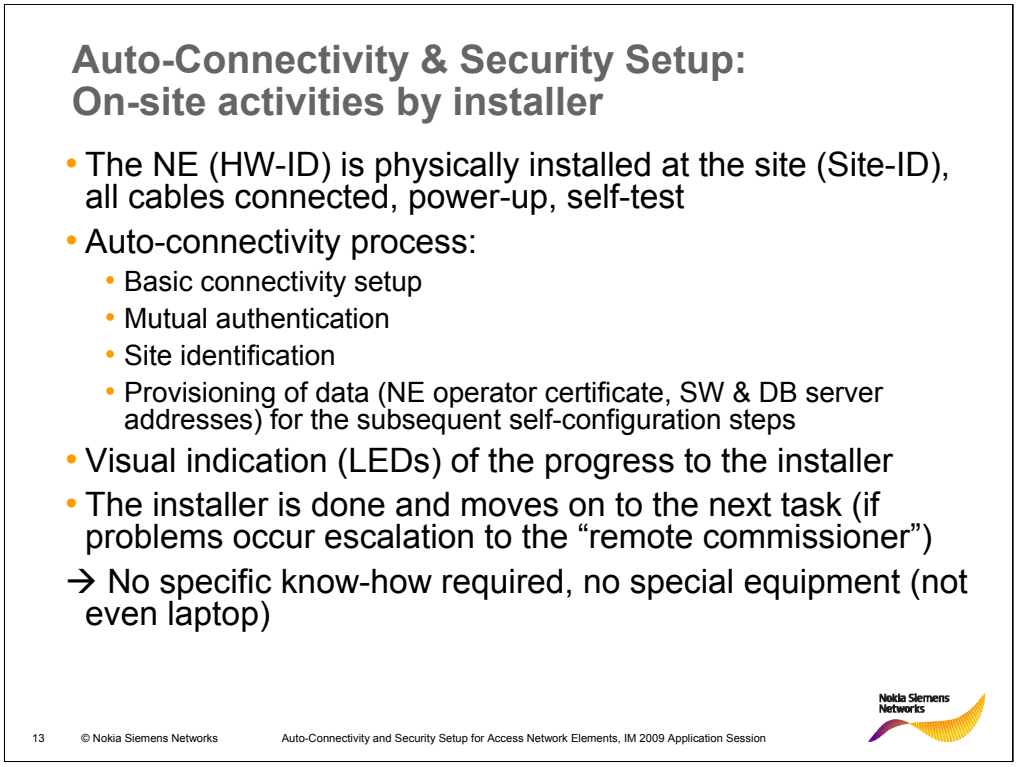
- NE is installed on the site.
- Installer reads the Site-ID from the task sheet and the HW-ID from a sticker on the NE cabinet.
- Installer makes a call to the remote commissioner help desk, informing the remote commissioner about HW-ID and Site-ID of the NE. Remote commissioner enters the HW-ID in the configuration data record related to the planned Site-ID.
- Installer starts the auto-connectivity setup at the NE.
- NE establishes a secure connection with the ACS and sends an announcement message, including the HW-ID.
- ACS queries the configuration database to retrieve the Site-ID and a subset of the planning data related to the site, which are then replied to the NE.

This solution requires expensive help desk support and is error-prone. The semi-automated method whereby the installer reads site-id and HW-ID with a bar code scanner and updates the configuration database remotely is better suited.



Automated site identification with an on-site GPS receiver:

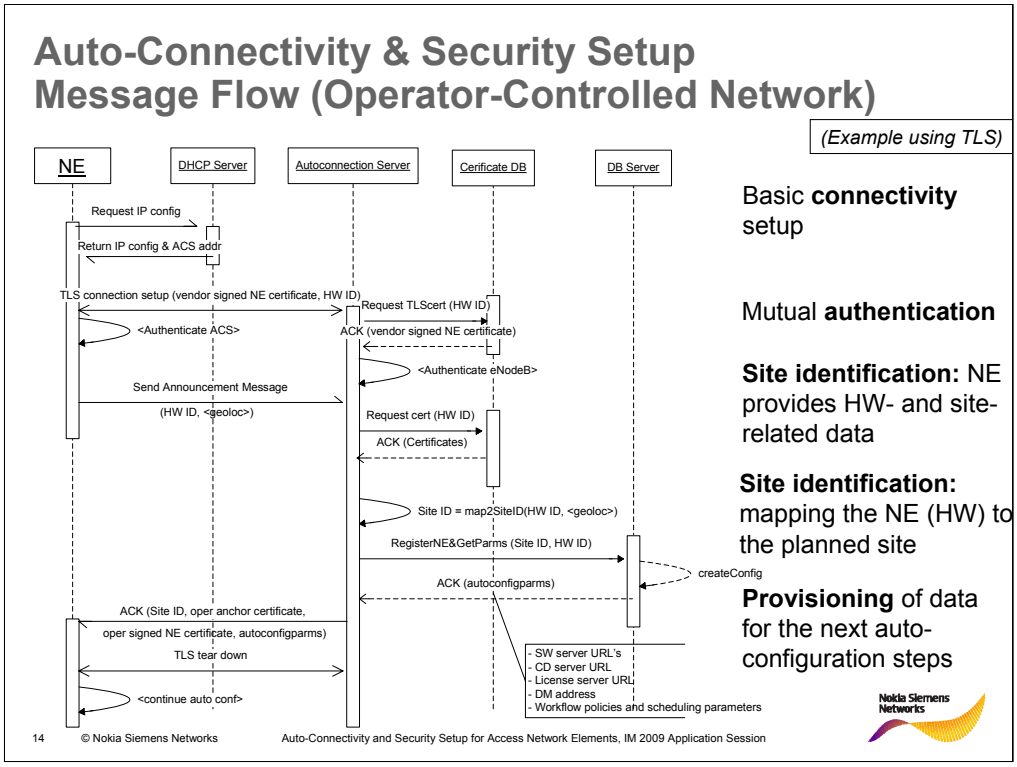
- NE is installed on the site.
- Installer starts the auto-connectivity setup at the NE.
- NE queries the GPS receiver for the site coordinates.
- NE establishes a secure connection with the ACS and sends an announcement message including the GPS coordinates, the HW-ID and possibly additional parameters that distinguish the NE from nearby NEs (e.g. NE type, detected hardware module types etc.) .
- ACS uses a geographic matching algorithm and the geographic site plan of the planned NEs to determine the Site-ID related to the received GPS coordinates. The algorithm shall include a tolerance radius around the planned site locations for coping with uncertainties of the GPS measurement and the GPS receiver location. When there is ambiguity between multiple sites (e.g. in case of co-located NEs of the same operator), the additional information of the NE and/or the rollout time may be used to determine the actual Site-ID.
- ACS accesses the configuration database to enter the HW-ID in the database record related with the Site-ID, and to retrieve a subset of the planning data related to the site. The planning data subset is then forwarded to the NE.



On-site activities by the installer

The main tasks left for the installer are the hardware installation of the racks and the connection of the NE to the antenna’s, the transport network and the power feed. Then the installer powers-on the NE and monitors from the LED indications on the system module whether the auto-connectivity setup proceeds successfully. When this is not the case, the installer shall call for assistance from the remote commissioner for analysing the problem (very likely a preparation task has not been properly executed). Otherwise the installer can leave the site. Further configuration of the NE is handled by the remote commissioner or automatically by an auto-configuration feature.

There is no longer a need for a skilled commissioner to travel on-site, connecting a laptop and entering the initial configuration parameters.



This simplified message flow illustrates the steps of the authentication and security setup, more specifically for the case with automated site identification.

Basic connection setup: when powered-up by the installer and after a self-test the NE starts the auto-connection process with a DHCP request. An appropriate DHCP server assigns an IP address from a reserved pool of addresses and replies to the NE with the initial IP configuration and ACS address.

Mutual authentication: NE starts a TLS handshaking with the ACS. The ACS verifies the vendor signed NE certificate using the factory trust anchor and checks whether the certificate is also available at the Certificate Database. The latter verification guarantees that the NE belongs to the mobile network operator and is authorised to access the mobile network. During the handshaking the NE also verifies the ACS supplied TLS certificate by means of the commercial trust anchor. After mutual authentication TLS client and server start encrypting/decrypting all messages over that connection.

Site identification: NE sends and announcement message to the ACS including the HW-ID and measured GPS coordinates of the site. ACS retrieves the certificates related to the HW-ID from the Certificate Database. The actual site identification is performed at the ACS by the geographic matching algorithm. Then the ACS communicates with the Domain Manager for storing the HW-ID in the on-line configuration database related to the Site-ID, for updating the network topology database with the new NE and for retrieving some parameters for the further (auto-)configuration.

Provisioning of data: ACS supplies the Site-ID, the certificates and the auto-configuration parameters in a reply for the announcement message. NE then tears down the secure TLS session and establishes a secure TLS or IPsec connection to the Domain Manager. The NE is now ready for the actual commissioning.

Summary & Conclusions

- The deployment of numerous access network elements (NE), e.g., radio base stations, causes considerable overhead
- The roll-out process can be facilitated by NE self-configuration
- The most critical part of the process is the initial connection establishment to the OAM system („auto-connectivity“)
- In this phase also the integration of the NE into the secure network environment needs to be performed
- The presented concept balances the tradeoff between automation and security requirements by
  - shifting manufacturer and operator activities to a preparation (rather than the actual roll-out) phase, eliminating any on-site activity as much as possible
  - eliminating any interaction between manufacturer and operator as much as possible
  - the NE is delivered only with an "off-the-shelf" software & configuration installation, facilitating the manufacturing process
  - only when the NE is placed on site, basic connectivity has been established, and mutual authentication between the NE and the OAM system has been done → network site is identified and the actual NE hardware is mapped to it
  - Then the NE can be easily configured to perform the role planned for that site

→ Thus a very flexible and secure roll-out process from both the operator and manufacturer perspective is enabled.

References & Abbreviations

[1] R. Droms, Dynamic Host Configuration Protocol, RFC 2131, IETF, March 1997.

[2] H. Kasinger, B. Bauer, H. Sanneck, C. Schmelz A Management Automation Framework for Mobile Networks in *Proceedings of the 17th World Wireless Research Forum,* Heidelberg, Germany, November 2006

[3] 3GPP TS32.501, Self Establishment of eNodeBs (SEe);Concepts and Requirements(Release 8), 2008.

[4] Henning Sanneck, Christoph Schmelz, Thomas Baumgarth, Konstantin Keutner, Network Element Auto-configuration in a Managed Network´, IM Application Session 2007, Munich, Germany

[5] Trusted Computing Group, https://www.trustedcomputinggroup.org

[6] S. Alexander, R. Droms, DHCP options and BOOTP vendor extensions, RFC 2132, IETF, March 1997

LTE	3GPP „Long Term Evolution“
OAM	Operation, Administration, Maintenance
TLS	Transport Layer Security
NMS	Network Management System
DHCP	Dynamic Host Configuration Protocol
DM	Domain Manager
TPM	Trusted Platform Module
URL	Uniform Resource Locator
CA	Certification Authority