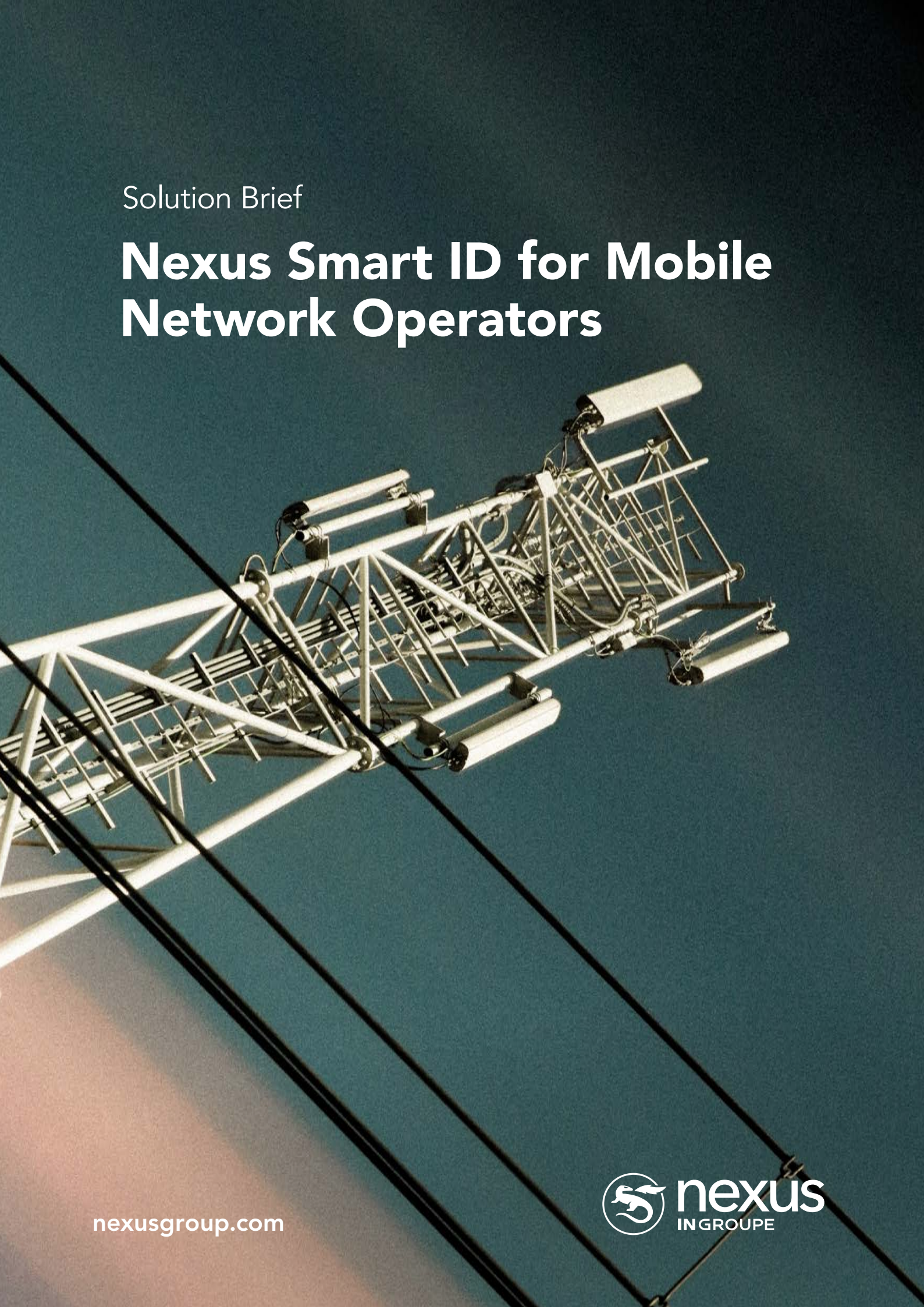
Solution Brief

# Nexus Smart ID for Mobile Network Operators



nexusgroup.com

nexus
IN GROUPE


# Introduction

Mobile networks constitute critical infrastructure and are essential to protect to prevent cyber security attacks from malicious parties and to conform with regulations and telecom standards.

Many mobile network elements rely on a Public Key Infrastructure (PKI) to protect the communication between the different machine components. Like people need trusted credentials, e.g., passport or smartcards, to prove their identity, machines use digital certificates to authenticate themselves. Trusted, unforgeable identities provisioned to each device in an M2M application, are the foundation for trusted and secure communication. PKI-based digital certificates constituting such identities enable authentication, data integrity and data confidentiality and have been used for decades to protect various systems and applications.

**Backhaul protection**
Backhaul refers to the insecure link between the e/gNodeB, connecting User Equipment (UE) via its radio interface to the operator's core network, and the SeGW (Security Gateway), a network element at the border of a security domain of the operator.

The link between e/g NB and Security Gateway (SeGW) shall provide a secure communication tunnel based on a PKI (as specified in 3GPP specification (TS 33.320)

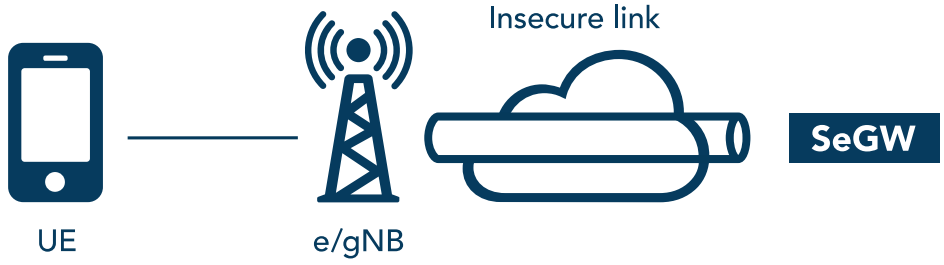



***Figure 1.*** *PKI protected backhaul link*

In addition to backhaul protection, PKI provides key values for other telecom use cases:

- **Network Management Systems**
  Protection of the connection from Network Management Systems, e.g. Nokia NetAct, Ericsson ENM, to e/gNodeBs.

- **VNF communication**
  Implementation of the TLS based mutual authentication and transport security between the Network Functions (NFs) in the Service-Based Architecture (SBA) as prescribed by 3GPP 5G specification TS 33.501.

- **Virtualization Platforms PKI**
  Use of external Certificate Authority (CA) in the SBA virtualization platforms, e.g. Kubernetes.

- **Open RAN security**
  Communication on interfaces E1, Xn, midhaul (F1) and open fronthaul (M-Plane) is based on IPSec/(D)TLS.

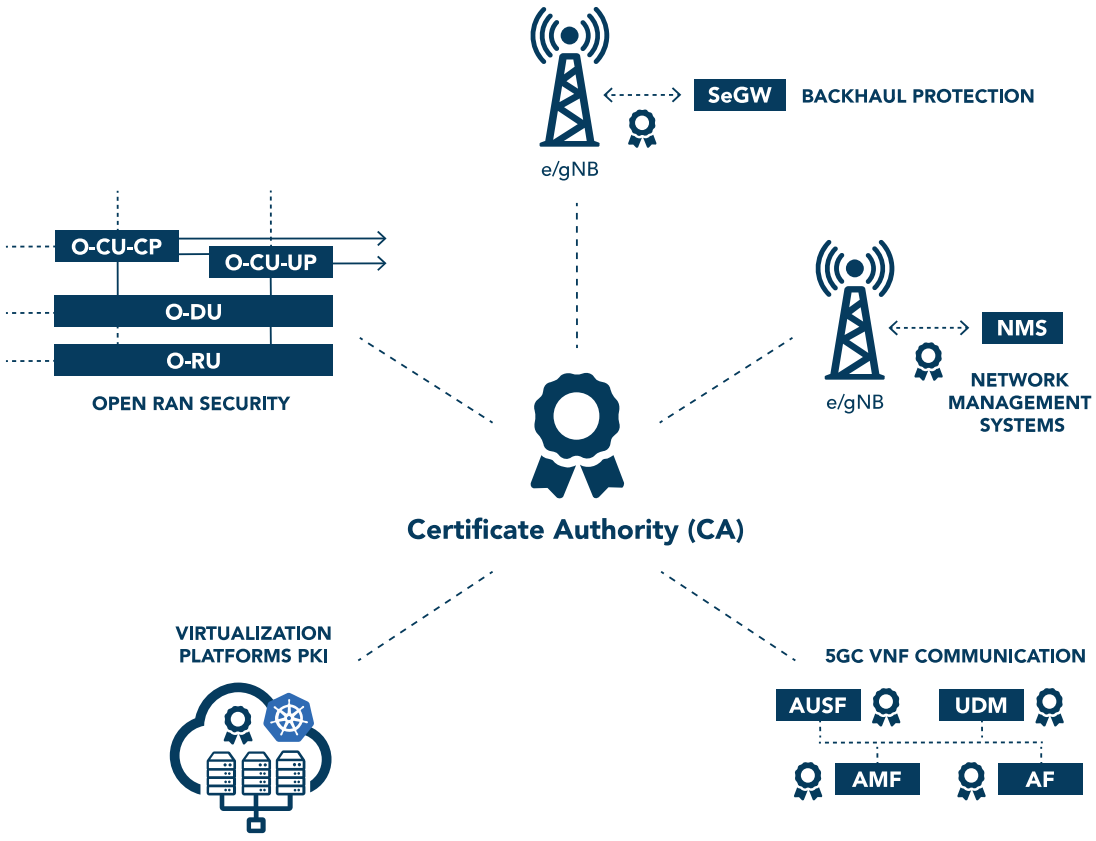



***Figure 2.*** *Telecom PKI use cases*

Solution Brief

# Nexus Smart ID IoT

## – The solution for Mobile Network Operators

Nexus Smart ID IoT is a Certificate Authority (CA) product enabling a Public Key Infrastructure (PKI) that constitutes the foundation for trusted and secure Machine-to-Machine (M2M) communication.

**Nexus Certificate Manager**
The core component of Nexus Smart ID IoT, Certificate Manager, is a generic, mature, reliable, and high-performing CA platform. The software is serving hundreds of customers globally and has issued >1 billion certificates. It offers multi-tenancy and multi-CA possibilities and provides easy CA management and vast integration possibilities supporting multiple certificate formats, crypto algorithms and HSM vendors/models. All standard certificate management protocols are supported, and a flexible REST API is available in addition.

Certificate Manager software is Common Criteria (CC) EAL4+ certified and supports delegated, approval-based device onboarding.

# Nexus Certificate Manager mobile network integration

Nexus Certificate Manager enables:

- Issuing of certificates to all radio network devices, independent of vendor, for backhaul protection based on the CMPv2 certificate management protocol.
- Support for SCEP and EST protocols enabling enrolment of network devices that do not comply with the CMPv2 standard.
- ACME protocol available allowing integration with virtualization platforms, like Kubernetes, Ansible, Terraform, Docker, Openstack, etc.
- Use case scalability due to multi-tenancy: different use cases can be completely separated though still served by a single CA platform. This allows flexibility to extend the platform to future IoT use cases or even corporate IT use.
- Nexus Certificate Manager can be easily deployed in a virtual environment based on Docker containers and in single-node, high-availability, or geographically redundant configuration. It can integrate to any Hardware Security Module (HSM) based on standard interface.

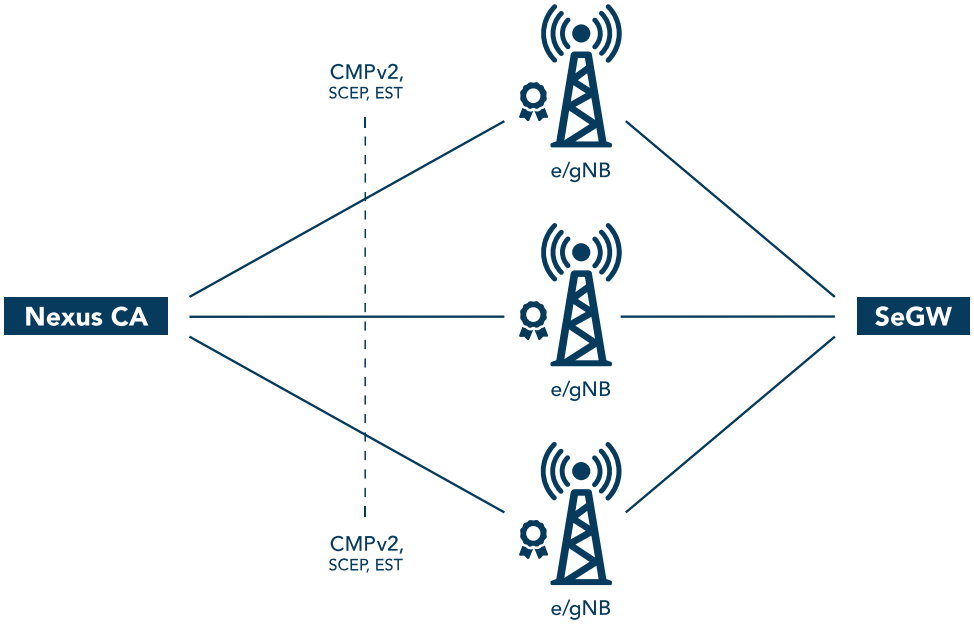



***Figure 4.*** *Nexus CA backhaul protection integration*

**Customer references**
Nexus Smart ID IoT and Certificate Manager is deployed with multiple MNOs on a global basis and in addition with hundreds of customers for various other PKI purposes.

Nexus furthermore has a broad partner network, that can enable broader turnkey solutions where requested.

Solution Brief

# Nexus Smart ID IoT for Mobile Network Operators
## **Your benefits in summary**

- 4G and 5G backhaul protection
- Interoperable with all standard e/gNodeB devices independent of network vendor
- Extensive certificate management protocol support for use in additional use cases
- Multi-tenancy enabled, enabling complete separation of PKI use cases
- Supports any standard HSM
- Highly secure solution, including CC EAL 4+ certified software
- Supports deployment in virtual, container-based environment
- High-availability and geographically redundant deployments enabled
- Market proven due to various global PKI backhaul protection deployments in operation with numerous mobile network operators
- Broad partner network enabling any required form of turn-key solutions towards customers´ needs

Please contact us for a joint alignment on how Nexus Smart ID IoT can serve your specific targets and requirements regarding secure digital identities within your network/infrastructure: contact@nexusgroup.com

**Do you want to know more? Contact us!**

https://www.nexusgroup.com/contact/

# nexusgroup.com