Ensuring cyber-security

for utility mission-critical communications

A Nokia eBook

NOKIA

The cyber-security threat

Utility communications networks are more vulnerable to threats now than ever before as global cybercrime grows in size and sophistication, and as nation-states emerge as potential threat agents.

Utilities must protect themselves from malicious or accidental incidents in operations, substations, along the network and at endpoints such as meters or sensors.

Deliberate threats—sabotage, vandalism, espionage, terrorism, theft or denial of service—can be perpetrated by hacktivists, cybercriminals and nation states, all of whom are evolving in sophistication, and have significant financial and intellectual resources at their disposal. Employees of the utility company itself, as well as entities in the supply chain, can also be threat agents.

This eBook provides an overview for how utilities can protect their mission-critical networks by identifying, addressing and mitigating these threats with best practices and methodologies centered on the ITU-T X.805 security framework using Nokia security capabilities. This multi–layer, in-depth approach, combined with Nokia's expert guidance, will deliver the recommended level of protection.

Power companies and utilities around the world expressed a six-fold increase in the number of detected cyber incidents over the previous year.

Source: PWC 2015 Global State of Information Security Survey

6x

A solutions path:

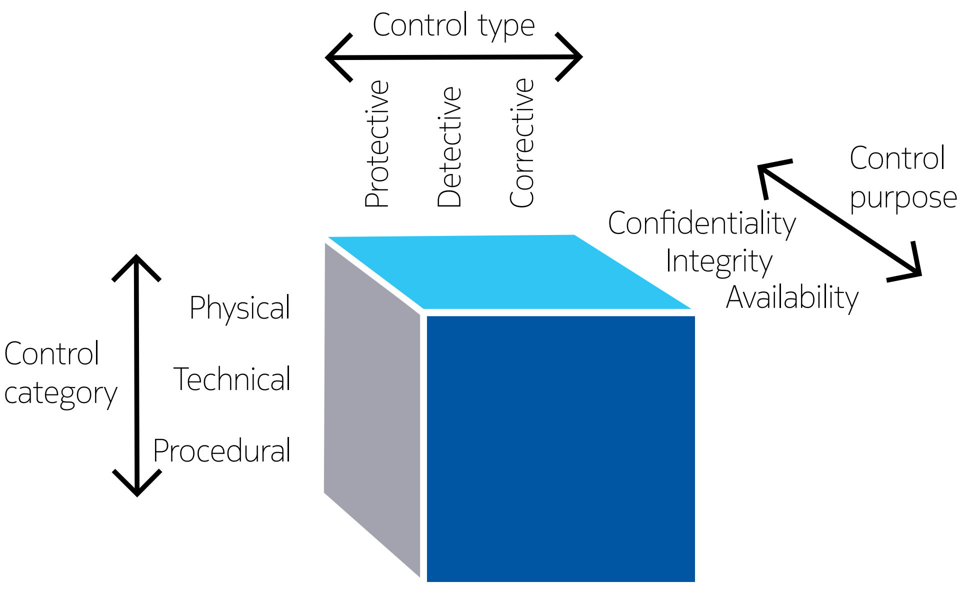
The ITU-T X.805 security framework

The ITU-T X.805 provides a comprehensive security architecture for communications networks. It outlines a security framework with a streamlined, simplified high-level threat model that can be aligned with best practices across different working groups within an organization. It enables utilities to improve network security and eliminate potential threats in complex environments, and it can be applied across network operations and management.

Structured threat mitigation

Utilities should think about security controls not only in terms of the properties they seek to protect – the confidentiality, integrity and availability of data – but also in terms of their category and type. Controls can be protective, detective or corrective, and can be mapped into a three-dimensional matrix in terms of their purpose, category and type. X.805 allows utilities to flexibly define comprehensive security policies, incident response and recovery plans, technology architectures and technical requirements to counter different security vulnerabilities on three defined security layers and planes.

Example controls

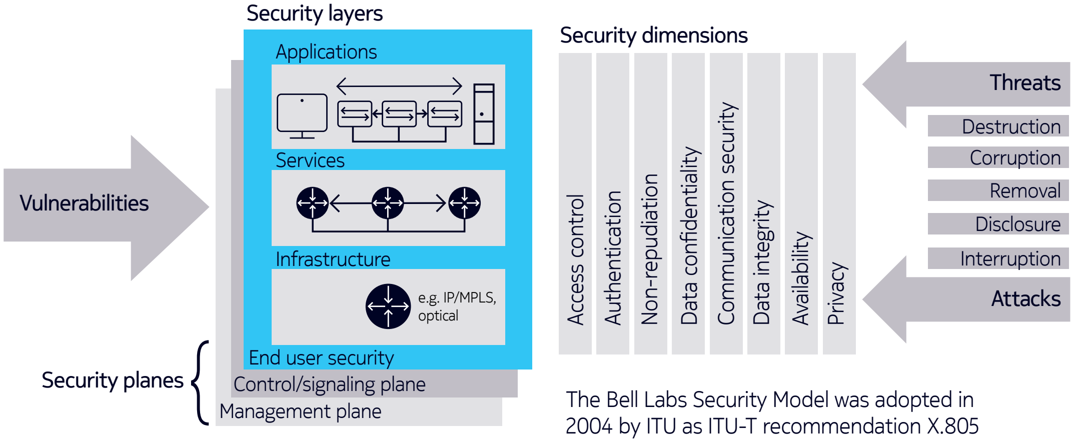


Control	Category	Type	Purpose
Firewall	Technical	Protective	C, I
Door locks	Physical	Protective	C, I, A
Encryption	Technical	Protective	C, I, A
Logging	Technical	Detective	C, I, A
Anti-DoS	Technical	Protective	A
Employee vetting	Procedural	Protective	C, I, A

X.805 security dimensions

The X.805 security framework contains a total of 72 security perspectives encompassing three layers (infrastructure, services, applications) used across three planes (management, control and end user) through eight security dimensions:

1. access control
2. authentication
3. non-repudiation
4. data confidentiality
5. communication security
6. data integrity
7. availability
8. privacy



The Bell Labs Security Model was adopted in 2004 by ITU as ITU-T recommendation X.805

Defense in depth

The X.805 security framework achieves the well-established principle of defense in depth—layers of controls that work together at various levels to protect all assets through a mix of procedural and technical controls.

A structured approach is required to choose the right level of investment in security, and to choose the right set of overlapping controls in the context of this principle. Certain technical controls—such as encryption, security zoning, and remote device security—are foundational for secure network design, deployment and operation.

Applications layer	Applications protocols SCADA, AMR/AMI, DA, teleprotection
Services layer	AAA, DNS, DHCP, VPNs
Infrastructure layer	Network nodes, servers, communications links [e.g. IP/MPLS]

Defense in depth encompasses a layering of security controls to protect assets

Unified identity and access management

Access control has become increasingly difficult in complex, multi-vendor environments spanning different types of networks and technologies. Existing equipment that support only a single user and password that multiple personnel are authorized to access compounds the problem.

Nokia offers a solution that provides unified identity and access management with single sign-on and centralized policies across multi-vendor, multi-technology networks and applications. The Nokia NetGuard Identity Access Manager is a single application that can be seamlessly integrated with existing identity management systems to automate and centrally manage passwords across all physical or virtual network functions. As a result, policies, such as Role Based Access Control (RBAC), can be automated by centrally defining roles, privileges, and controlling access or the password aging policy across a multitude of devices.

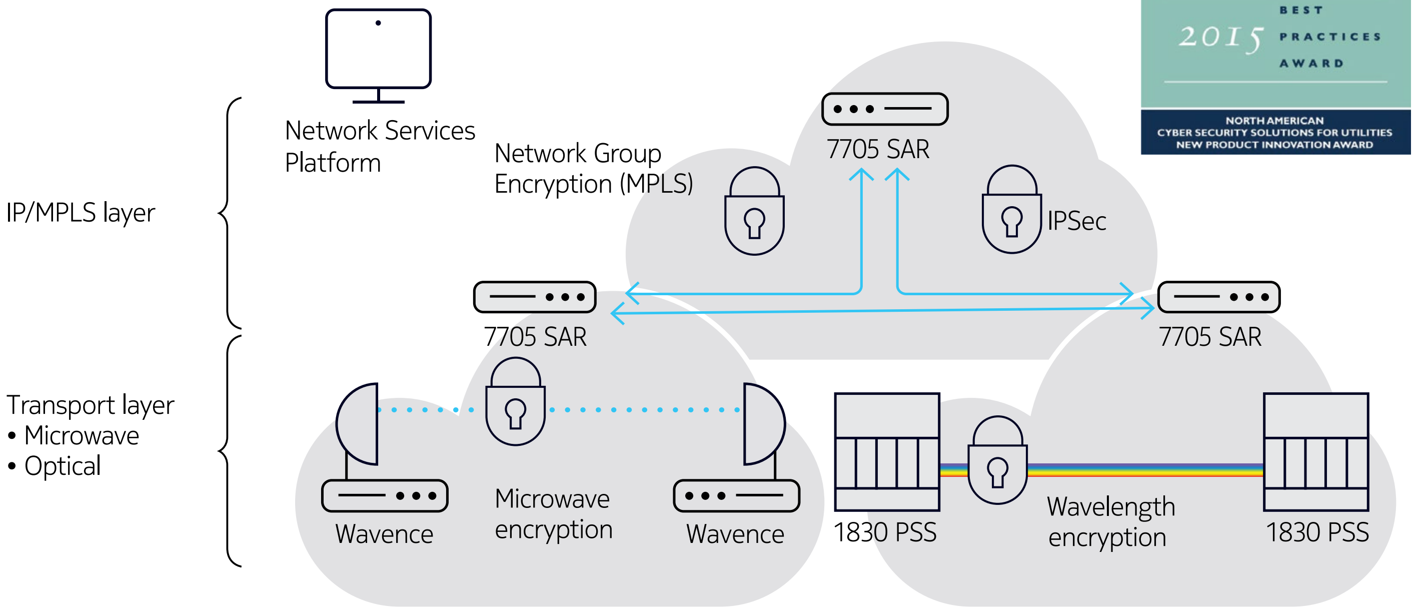
This approach also prevents the need for shared accounts in order to jump hosts for access to older assets. Instead, many-to-one account mapping is used to manage access to these assets that support only a single user and password.

The Nokia NetGuard Identity Access Manager provides comprehensive audit trails with logging and user activity replay, addressing regulatory and compliance reporting requirements, as well as forensic investigations.

Data sheet: Nokia NetGuard Identify Access Manager

Using encryption

Encryption is a key element in cyber-security for utilities to address data confidentiality, authentication and data integrity. Nokia offers a comprehensive multi-layer encryption solution – IP/MPLS layer and transport layer using optical and microwave systems. With this solution utilities can pick the right encryption component using a best fit approach based on the network architecture deployed.



FROST & SULLIVAN
2015 BEST PRACTICES AWARD
NORTH AMERICAN CYBER SECURITY SOLUTIONS FOR UTILITIES NEW PRODUCT INNOVATION AWARD

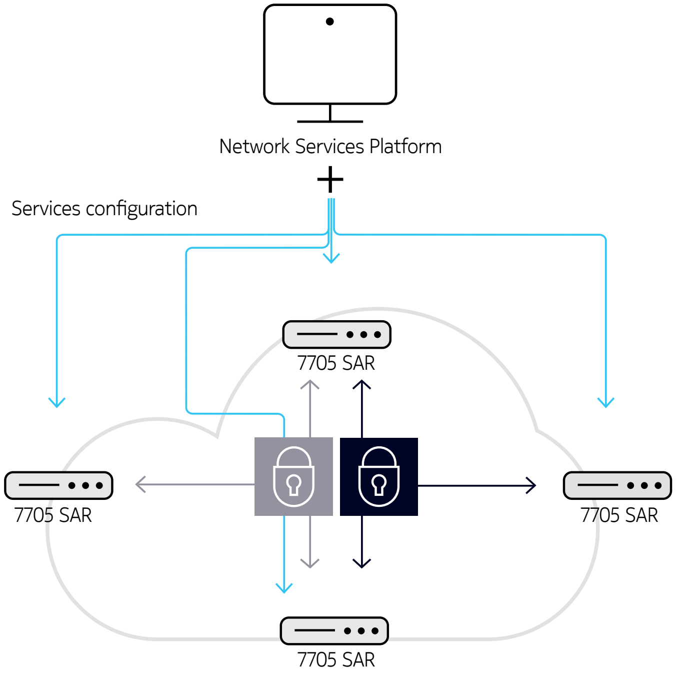
An award-winning solution Nokia's multi-layer encryption for IP/MPLS, optical and microwave won Frost & Sullivan's 2015 New Product Innovation Award for North American Cyber-security Solutions. Its 7705 SAR Network Group Encryption was named a 2016 Smart Grid Product of the Year by IoT Evolution World, and received the Smart Grid, Metering and Infrastructure Security Award during European Smart Energy Summit 2016.

Video: Secure optical transport with Nokia

Video: Network Group Encryption secures IP/MPLS networks

Network Group Encryption (NGE)

The Nokia service router supports end-to-end communications using IP/MPLS. It provides a comprehensive suite of security features, including NGE, which allows IP, as well as non-IP TDM and Ethernet traffic riding over MPLS services, to be encrypted end-to-end. This is accomplished without needing to convert all traffic to IP-routed packets and establish and manage meshes of IP security (IPSec) tunnels between nodes. NGE riding atop MPLS is not limited to Layer 3 services in a P2P configuration, as with IPSec, but also provides seamless encryption for multipoint configuration for L2 and L1 services. In addition, NGE also safeguards network control plane traffic, the foundation of an IP/MPLS network.



NGE benefits

- **Seamless operation over IP/MPLS.** NGE can be applied on top of an operational IP/MPLS network, maintaining operational consistency before and after NGE is applied. Live traffic can be selected by the operator and encryption applied in real time without service interruption.
- **Maximum availability.** NGE-encrypted traffic is maintained under any circumstance. If the encryption manager is out of reach, encrypted traffic keeps flowing. If a router reboots after a power outage, encrypted traffic flow is restored immediately—no waiting for key negotiation.
- **Universal encryption.** Encrypts all P2P, multi-point to multi-point services and sensitive IP/MPLS network control traffic end-to-end without compromise. Using Nokia's Network Services Platform, utilities can easily determine which nodes require which keys to be used in a security domain.
- **Maximum deployment flexibility.** NGE can be used in a variety of network models, over leased line or carrier layer 2 and layer 3 VPN services, or leveraging broadband cellular networks or Wi-Fi to extend encryption to remote locations.

Application note:
Network Group Encryption

NGE's universal approach leaves no traffic vulnerable while traversing the network. Utilities can flexibly deploy an end-to-end solution to support a range of services and applications such as SCADA, teleprotection and other critical operations at remote devices and throughout the distribution and transmission grids over a single, converged network.

Encrypted teleprotection: Teleprotection demands extremely low latency and jitter, and must be transmitted securely with appropriate authentication and data encryption. Tests conducted by The University of Strathclyde in Glasgow successfully demonstrated that critical teleprotection services can be encrypted in real-time with negligible impact on performance.

Video: Reliable teleprotection over IP/MPLS with Nokia

Report: Validating secure and reliable IP/MPLS communications for current differential protection

Zone-based service-aware firewall

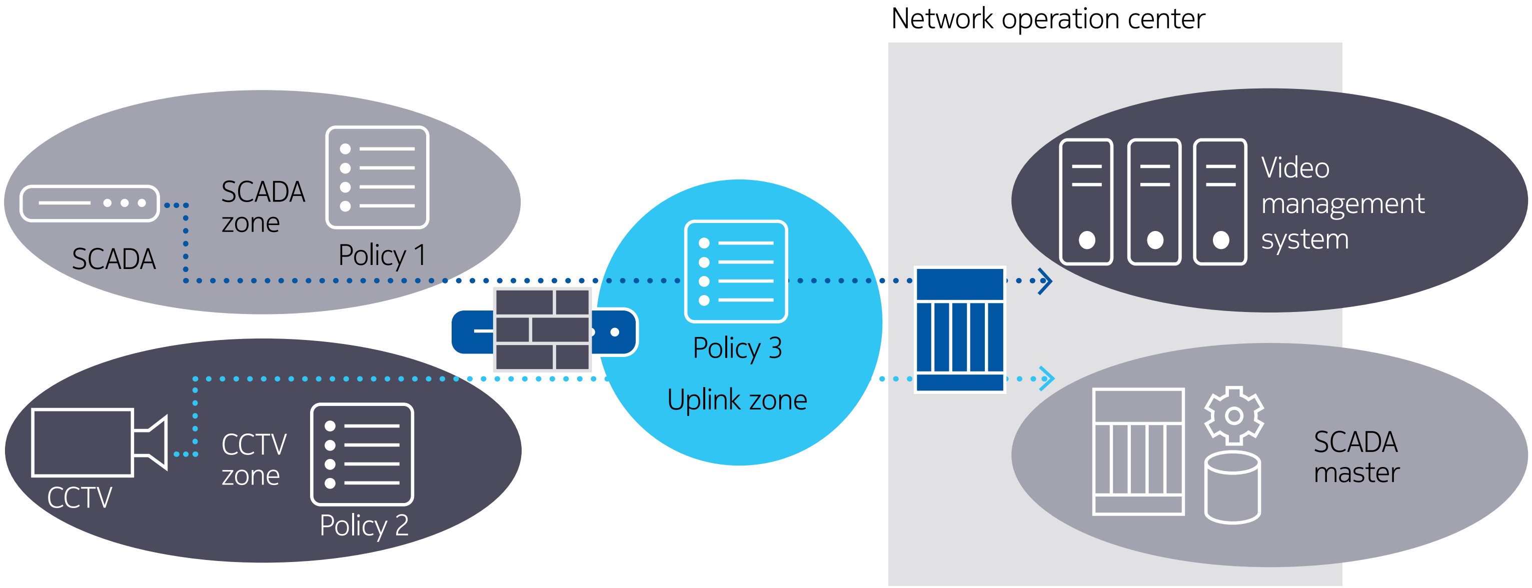
The X.805 access control security dimension is addressed through the use of a zone-based service-aware firewall. A zone specifies the security needs in the form of security policy, defining the rules to specific actions performed on IP traffic. Any IP interfaces that share the same need can be put into the zone. This approach significantly improves efficiency and flexibility when applying a firewall.

Key operations applications that involve communications between the operations center and substations are segregated into their own logical zones—for instance, a "substation zone" and a "SCADA zone."

As grid applications are typically placed into different IP VPN services, it is crucial for the firewall to be service aware so that it inspects packets pertinent to IP VPNs, as well as those for Internet services.

Application note: Nokia 7705 Service Aggregation Router security overview for utilities

Article: Protecting the smart grid amidst a cyber security evolution



Anomaly detection to protect remote devices

Existing grid devices which have limited or no security capabilities, such as Remote Terminal Units (RTU) need protection. New and future Internet of Things (IoT) devices for automation and new business models deployed in the distribution grid may also include limited security capabilities in order to minimize their cost and quicken their time to market. These endpoints will also need to be protected.

Endpoint security

Nokia NetGuard Endpoint Security monitors traffic and compares it to baseline values. It uses analytics that monitor and analyze traffic, as well as search for patterns consistent with malware behavior, protocol anomalies, and deviations from normal traffic profiles. Reports of anomalies automatically generate alerts to initiate an appropriate response to conduct forensics or stop the traffic completely.

Growing deployment of IoT devices giving attackers an expanding number of vectors and surfaces to target.

Managing IoT Cybersecurity Threats in the Energy Cloud Ecosystem Report

Navigant Research

Solution sheet: Nokia NetGuard Endpoint Security

Report: Nokia 2017 threat intelligence report

Assuring device security

Intelligent machine-to-machine (M2M) devices serving utilities in a mission-critical IoT environment require remote management. Nokia’s Intelligent Management Platform for all Connected Things (IMPACT), gives utilities a secure platform on which to scale new IoT services lifecycle management.

M2M security requirements

- A secure “immutable identity,” the key to establishing the device’s credentials when it connects to the network. Managing device identity — authenticating or validating the identity of the device, authorizing or registering the device for access, and managing the specific privileges and services available to the device — is a critical first step to ensuring the security of that device in the field.
- Establishing a secure M2M communication channel for device management. This must provide a means to authenticate the device’s identity, ensure the confidentiality of the data going to and from the device, protect the integrity of the data going to and from the device, and ensure device availability.
- A trusted software environment to ensure the ongoing security of the M2M applications that use, drive, and run on the device. A secure firmware package running at the lowest level of the software stack is the mechanism used by nearly all computing devices, phones and consumer electronics in the field today. Secure device firmware, signed by an immutable device identifier and securely delivered to the device over a secure communication channel, provides the most secure trusted software environment for M2M devices.

Strategic white paper: M2M security: Ensuring device security for the Internet of Things devices

White paper: Using light device management to secure endpoints in the Internet of Things

Solution sheet: Nokia IMPACT

Leading Lights AWARDS 2017 Winner

Most Innovative IoT/M2M Strategy (Vendor) with a solution of IMPACT, NetGuard Endpoint Security and IoT Community

Automated regulatory compliance

Report preparation using data from multiple systems for a security audit can significantly increase a team's workload for weeks or even months. That's because detecting and monitoring compliance violations has become increasingly difficult in complex, multi-vendor environments spanning different types of networks and technologies. Tracking changes, authorization flows, and access controls, as well as the trails of who did what and when — comprehensively and reliably — requires time and effort and is undeniably prone to human mistakes and malicious behaviors

Nokia NetGuard Audit Compliance Manager automates the audit and analysis of all the parameters in the physical and virtual networks. It can be integrated into existing control databases and ticketing systems to centrally track all changes, required authorizations, as well as log and report them.

The Audit Compliance Manager provides a complete audit trail against actual baseline values for each monitored device. By means of continuous and real-time scans of device parameters, the NetGuard Audit Compliance Manager can generate all required compliance reports, efficiently and automatically. Furthermore, it is highly flexible and supports a rich set of features to address any vendor's audit criteria.

Data sheet: Nokia NetGuard Audit Compliance Manager

Enhanced situational awareness and actionable compliance insights

Having visibility of the security posture of the critical infrastructure of a growing network and being able to use data analytics to prevent, pinpoint, and address security threats before they result in breaches is critical. This has become increasingly difficult in complex, multi-vendor environments spanning different types of networks and technologies.

The Nokia NetGuard Security Management Center (SMC) integrates and correlates data from existing security systems, as well as from those that lack single dashboard management platforms. This approach helps to assess business risks, improve quality of decision making, and overall response time to reduce potential recovery costs.

It also includes integrating policy violations from the NetGuard Identity Access Manager and tracking changes identified by the NetGuard Audit Compliance Manager — changes, which are consistent with, or an exception to the baseline. The Security Management Center also correlates critical information, such as traffic anomalies, detected by NetGuard Endpoint Security, which enables the identification of potential attacks, as well as defective or misconfigured devices.

This process also helps the analyst to investigate root causes and protect facilities effectively. Moreover, its analytics and reporting capabilities improve situational awareness and operational efficiency by automating and guiding responses to threats.

Data sheet: Nokia NetGuard Security Management Center

Conclusion

The operational environment is which utilities operate is evolving in terms of threats, technologies and compliance. As communications technologies evolve from TDM to packet, protecting critical grid communications required a layered defense-in-depth approach, employing a range of security controls from physical, technical and procedural categories based on the ITU-T X.805 security framework. This structured approach will leverage the robust foundation of standards guidelines and best practices.

The Nokia NetGuard Security solution for utilities combines unified identity and access control with trailing of user activities, automated auditing of network parameters with centralized management of baselines, and powerful traffic and data analytics from multiple sources, using a single pane of glass perspective. The solution also automates and improves situational awareness, guides threat responses, and simplifies reporting for regulatory compliance for utilities. These capabilities along with encryption and zone-based firewalls are key foundational elements in the Nokia grid communications security solution, designed and tested with end-to-end security in mind.

As communications are extended to remote devices with a wireless FAN solution, and IoT strategies are deployed, additional control with a Nokia solution to secure and lifecycle manage the growing number of remote devices becomes critical. These solutions bring together best-in-class technology and services from Nokia's certified security professionals to keep the gird secure.

What Nokia Delivers

A solutions path based on the ITU-T X.805 security framework

Nokia offers utilities a comprehensive security solution that maps to X.805's multi-layer / multi-dimensional framework with layers of controls that work together at various levels to protect all assets with a defense in depth approach.

Reliable MPLS security

Nokia IP/MPLS products provide strong mechanisms which securely protect the management, control, and data planes of mission-critical utility communications networks.

7705 Service Aggregation Router (SAR)

The 7705 SAR provides a comprehensive suite of security features for all management, control and data planes associated with the network infrastructure and virtual private network (VPN) services, along with additional security features such as NGE, stateful zoned-based service aware firewalls, network and port translation, access control lists and other tools.

Network group encryption (NGE)

Nokia Network Group Encryption (NGE) protects all grid applications traffic end-to-end without needing to convert all traffic to IP-routed packets. In addition, IP/MPLS network control plane traffic is also protected by NGE.

Transport security with 1830 Photonic Service Switch (PSS)

The 1830 PSS offers high-capacity optical DWDM connectivity with low latency encryption and optical intrusion detection thereby ensuring the confidentiality, integrity, and availability of in-flight data.

NetGuard Security Management Center

Centralized configuration, monitoring and analysis for security functions in multivendor networks.

NetGuard Identity Access Manager

Network-wide attribute- and role-based identity management, access management, and single sign-on capabilities.

NetGuard Audit Compliance Manager

Auditing and analysis of all parameters in physical and virtual networks to preserve data integrity.

NetGuard Endpoint Security

Network-based anti-malware solution for fixed, mobile and IoT devices.

M2M security

Nokia's scalable Intelligent Management Platform for All Connected Things (IMPACT) solution enables lifecycle device management (handles data collection, event processing, device management, data contextualization, data analytics, end-to-end security and applications enablement) for any device, any protocol and across any application.

Nokia security services

Nokia worked as a security system integrator for many years. Today, we are involved in more than 500 security projects worldwide, offering capabilities that range from design to support. We also lead the industry in securing commercial LTE networks.

Nokia Bell Labs Consulting

Works as a trusted partner for connecting deep technology insights to critical financial decisions. Security is a key dimension of our network and operations transformation consultative engagements globally.

Acronyms

4G:	Fourth generation
DoS:	Denial of service
IKE:	Internet key exchange
IoT:	Internet of things
IP:	Internet protocol
IPSec:	Internet protocol security
ISO:	International Standards Organization
ITU:	International Telecommunication Union
ITU-T:	ITU telecommunication standardization sector
L1:	Network layer 1
L2:	Network layer 2
L3:	Network layer 3
LTE:	Long term evolution mobile communications standard
M2M:	Machine to machine
MPLS:	Multi-protocol label switching
NERC:	North American Electric Reliability Corporation
NERC-CIP:	The Critical Infrastructure Protection standards body of NERC
NGE:	Network Group Encryption
NIST:	National Institute of Standards and Technology
NSP:	Network Services Platform
OID:	Optical intrusion detection
P2P:	Point to point
SAR:	Service Aggregation Router
SSH:	Secure shell cryptographic network protocol
TDM:	Time division multiplexing
TTL:	Time to live security protocol
VPN:	Virtual private network

Resources

Application note:	Network Group Encryption Group Nokia 7705 Service Aggregation Router security overview for utilities
Article:	Protecting the smart grid amidst a cyber security evolution
Data sheet	Nokia NetGuard Identify Access Manager Nokia NetGuard Audit Compliance Manager Nokia NetGuard Security Management Center
Report	Validating secure and reliable IP/MPLS communications for current differential protection Nokia 2017 threat intelligence report
Solution sheet	Nokia NetGuard Endpoint Security Nokia IMPACT
Strategic white paper:	M2M security: Ensuring device security for the Internet of Things devices Using light device management to secure endpoints in the Internet of Things
Videos:	Network Group Encryption secures IP/MPLS networks Reliable teleprotection over IP/MPLS with Nokia Secure optical transport with Nokia

Let us help with your cyber-security transformation.

The world's smart grid communications specialist, Nokia brings its leadership and expertise in communications technology and network security to meet the most demanding requirements of power utilities. Its solutions help them create an intelligent, responsive and adaptive communications network.

Talk to Nokia about how we can help build and secure your power utility communications network at all levels. For more information, visit networks.nokia.com/power-utilities.

NOKIA