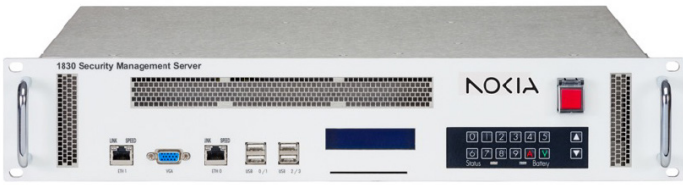
Nokia 1830 Security Management Server

Nokia Quantum-Safe Networks 1830 SMS

As part of the Nokia Quantum-Safe Networks solution, the 1830 Security Management Server (SMS) delivers centralized quantum-safe key management for encrypted services. Using a powerful processor and a secure microservices architecture, 1830 SMS generates high-quality, strong keys for each service, providing highly scalable, unified key management in support of secure, business-critical data communications.

Overview

The 1830 SMS enables network operators to offer secure infrastructure services while retaining full ownership and control of their own cryptographic keys and encryption parameters.



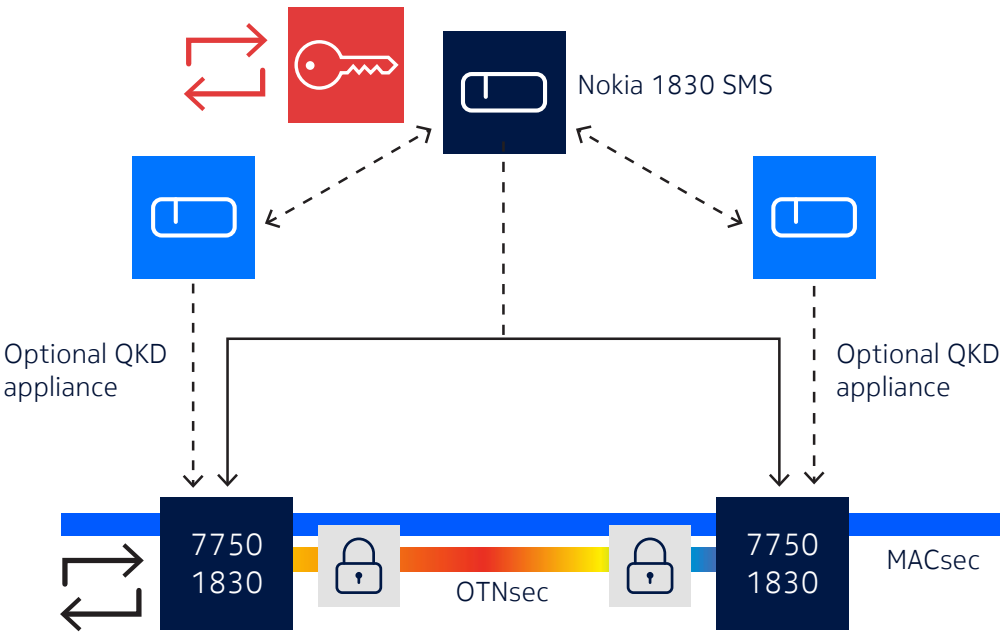
The 1830 SMS provides highly scalable and unified key management, handling encryption key creation, expiration, rotation and destruction in support of secure business-critical data communications. In Quantum Key Distribution (QKD) applications, it provides resilient mediation to the KMS layer of various QKD vendors through an ETSI GS14 extension REST-based API. It supports scenarios where unique encryption keys must be used between each sender and receiver pair, with keys frequently rotated as part of encryption security best practices.

The 1830 SMS is a scalable solution, addressing simple to complex deployments where key management is needed for secure, encrypted inter-site connections. Hardware and software design, implementation and manufacturing all were independently certified to meet the security standards set by major certification bodies.

Key benefits

- Centralized, symmetric key management, providing highly scalable and unified key management
  - Single point of trust; one point to protect from attack
  - Synchronized key rotation and distribution (traffic hitless)
  - Enhanced security and simpler operations through unified key management and encryption policies
  - Graphical view of security alarms
- Automated key management:
  - No human user is required to enter an encryption key used for data plane encryption; SMS generated keys are never seen by any humans: This eliminates the chance that a key is copied down and used inappropriately.
  - Fast and automatic recovery of encryption by providing new keys to both ends of a circuit for the cases of equipment replacement or complete shelf power failure at either end of the service. This can save precious time by not needing to manual provision new keys at both end points of the encryption service.
- Trusted key management
  - Flexible access control, enabling network partitioning into security areas for multiple enterprise customers
  - Customizable key security parameters on assigned circuits to allow enhanced end-user control
  - Holistic network-wide view of security alarm and encryption services
  - Clear separation of network and security tasks
- Strong security capabilities
- Fully configurable rotation interval
- Rotation on schedule or on demand
  - Offload computationally intensive cryptographic processing, enabling more sophisticated security algorithms

Figure 1. Nokia Multi-layer, resilient Quantum-Safe key orchestration



- Strong, high-quality hardware-generated keys guarding against classical and quantum computer attacks

- Common network key generator across several Nokia transport products:
  - Optical: Nokia 1830 Photonic Service Switch (PSS), 1830 Photonic Service Demarcation (PSD) and 1830 Photonic Service Interconnect (PSI)
  - Microwave: Nokia 9500 Microwave Packet Radio (MPR)
  - Nokia CloudBand Infrastructure System (CBIS)
  - Nokia routers: MACsec, ANYsec key generation
- Fully certified by independent parties
  - HSM hardware and software implementation certified to meet Common Criteria Evaluation Assurance and Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) certifications

- QKD/KMS connectivity
  - Highly resilient key mediation through ETSI GS14 extension REST-based API
  - Automatic reversion to classic keys in event of QKD failure
  - Coordination of key creation and rotation. The KMS is responsible to relay the key generated from QKD to NE
  - Monitoring logs and alarms from NE during key rotation and validation
  - If the key request fails, the 1830 SMS will create a key and transmit it to the NE
  - If the key teleportation is not successful after three attempts, the 1830 SMS will create a key and transmit it to the NE
  - After each failure, the 1830 SMS will resume requesting keys to the KMS by default.

Product specifications		
Security features	• NIST-certified AES-256 encryption solution for data encryption • Random generator: physical salt 256 bits • Reinforced and validated access control: ANSSI QR-validated embedded smart card reader and PIN keyboard	• Secure microservices architecture • Tamper-protected hardware • FQDN certificate management (HTTPS)
Platform security certification	• Common Criteria EAL4+/ANSSI QR • European restricted and NATO secret restricted certifications (ANSSI)	• Digital signature PP CWA 14167-2 compliant • FIPS 140-3 L2, in preparation
Interfaces	• 2 x10/100/1000 Base T Ethernet ports; supports VLAN for DCN network • 4 x USB2 ports • 1 x VGA	• Embedded Smart card reader and keyboard • LCD screen 2 x 16 digits • Front panel emergency reset button
Encryption hardware interworking	• Nokia 1830 PSS/PSS-x encrypting transponders: - 11QPEN4E - S13X100E - 2UC400E - 2UC1TE - S6AD600E - Nokia 1830 PSD-2	• Nokia 1830 PSI-M encrypting transponders: - DA2C4E, DFC12E, SFM6E • Nokia 9500 MPR (Wavence 20A secure mode) • Nokia 7750 and 7705 routers • Quantum Key Distribution (QKD)
Interoperability and authentication	• NTP protocol • HSM self-signed or CA certificate management • Authentication against SIEM • SSL authentication SysLog • Redundant LDAP, LDAP over SSL, LDAP group mapping • ANSSI certified access control (keyboard, smartcard)	• DNS name resolution for HTTPS, LDAPS, SysLog • Secure password generated from embedded, protected HSM
Redundancy and failure protection	• PSU hot swap, battery backup • Automatic configuration backup	• Automatic failover to standby; manually configurable
Product compliance	• EN 55022 (Class A), EN 55024, EN 60950 • IEC 950, UL 1950	• FCC Part 15 (Class A) • RoHS compliant
EMC compliance	• FCC Part 15 (Class A) • EN 55024 • EN 55032 (Class A) • EN 300 386 (Telecom centres) • ES 201 468 (Telecom centres)	• ITU-T K.20 • TCOM 1TR9 • BT GS7 • CISPR32 (Class A)
Environmental/safety compliance	Telcordia GR-63-CORE Telcordia GR-1089-CORE IEC/EN 60950-1 (ed 2.2) ETSI EN 300 019-2-1 (Class 1.1) ETSI EN 300 019-2-2 (Class 2.1)	ETSI EN 300 019-2-3 (Class 3.1) ETSI EN 300 132-1 ETSI EN 300 753 IEC/EN 60950-1 Compliant to RoHS
Installation options	• Rack mounting (2RU 19 in)	
Cooling	• Front-to-back airflow	
Dimensions	• Height: 88 mm (3.46 in) • Width: 482.6 mm (19.0 in) • Depth: 394.4 mm (15.53 in)	
Weight	10 kg (22.05 lbs.)	
Power consumption	88 W	

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (October) CID200458