Nokia 1830 Security Management Server

Secure transport over optical and microwave networks

The Nokia 1830 Security Management Server (SMS) is a secure, scalable module that supports centralized key management for the entire cryptographic life cycle of each encrypted wavelength service. Using a powerful processor and security enhanced Linux operating system, it generates the quantum safe keys to perform the encryption. It provides highly scalable and unified key management in support of secure business-critical data communications.

Overview

The 1830 SMS enables enterprise IT organizations, network operators and managed service providers to offer secure infrastructure services to their customers while allowing them to keep 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. It supports scenarios where unique encryption keys must be used between each sender and receiver pair, and these keys are 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. Its hardware and software design, implementation and manufacturing have been independently certified to meet the security standards set by major certification bodies.
Key features

- Centralized key management: Key creation, expiration, rotation and destruction
- Clear separation of network and security tasks
- Unified policies for key management and encryption
- Common key management across optical (Nokia 1830 Photonic Service Switch [PSS]) and microwave (Nokia 9500 Microwave Packet Radio [MPR]) transport portfolios
- Automated and scheduled key rotations
  - Configurable rotation interval, e.g., minutes or hours
  - Rotation based on predefined schedule or on demand
- Graphical view of security alarms
- SDN control via REST APIs

Key benefits

- Centralized 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
- 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
  - TLS certification validation at startup

- Strong security features
  - Offload computationally intensive cryptographic processing, enabling more sophisticated security algorithms
  - Enable strong hardware-generated keys (to match AES-256 bit encryption) to guard against classical and quantum computer attacks
- Fully certified by independent parties
  - Hardware and HSM software implementation certified to meet Common Criteria Evaluation Assurance, Federal Information Processing Standards (FIPS) and Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) certifications

Technical specifications

Security features

- NIST-certified AES-256 encryption solution for data encryption
- Random generator: Physical salt 256 bits
- RADIUS support
- Security-Enhanced Linux (SELinux CentOS)
- Tamper-protected hardware

Platform security certifications

- FIPS 140-2, Level 3
- Common Criteria EAL4+/ANSSI QR
- European restricted and NATO restricted certifications (ANSSI)
- Digital signature PP CWA 14167-2 compliant

Standards compliance

EMC compliance
North American Region
- FCC Part 15 (Class A)
### European market
- EN 55024
- EN 55032 (Class A)
- EN 300 386 (Telecom centres)
- ES 201 468 (Telecom centres)
- ITU-T K.20
- TCOM 1TR9
- BT GS7

### Asia-Pacific market
- CISPR32 (Class A)

### Environmental/safety compliance

#### North America Region
- Telcordia GR-63-CORE
- Telcordia GR-1089-CORE
- IEC/EN 60950-1 (ed 2.2)

#### European market
- 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 (ed 2.2)
- Compliant to RoHS requirements

* Ongoing testing for temperature and humidity limits

---

### Product specifications

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height</td>
<td>88 mm (3.46 in)</td>
</tr>
<tr>
<td>Width</td>
<td>482.6 mm (19.0 in)</td>
</tr>
<tr>
<td>Depth</td>
<td>394.4 mm (15.53 in)</td>
</tr>
</tbody>
</table>

| Weight          | 10 kg (22 lb) |

| Interfaces      | 2 x 10/100/1000 Base T Ethernet ports |
|                 | 4 x USB2 ports |
|                 | 1 x VGA |
|                 | Embedded Smart card reader and keyboard |
|                 | LCD screen 2 x 16 digits |
|                 | Reset button on front panel |

| Power           | 100-240 VAC with typical draw of 88W (150W max rate of PSU) |

| Operating temperature | 0° to 45°C (32° to 113°F) |

| Redundancy       | Hot swap, battery backup and high availability via replicated backup instance of the 1830 SMS on warm-standby |

| Installation options | Rack mounting (2RU 19 in) |

| Cooling          | Front-to-back airflow |
Figure 1. Certified and unified Layer 1 encryption across optical and microwave transport

- L1 encryption over transport networks
- Traffic hitless key distribution and rotation

Optics (WDM) encrypted

1830 PSS

Microwave encrypted

9500 MPR

Trusted

1830 SMS

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: SR1801021189EN [January]