Nokia 1830 Security Management Server
1830 SMS

The Nokia 1830 Security Management Server (SMS) family delivers centralized key management for encrypted services over layer 1 networks, including optical or microwave transport. Using a powerful processor and a secure microservices architecture, 1830 SMS generates quantum-safe keys for each service. It provides high-quality, strong keys and 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. 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
- 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
  - Automated and scheduled key rotations
  - Fully configurable rotation interval
  - Rotation on schedule or on demand
    - Offload computationally intensive cryptographic processing, enabling more sophisticated security algorithms
    - 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) and 1830 Photonic Service Interconnect (PSI)
  - Microwave: Nokia 9500 Microwave Packet Radio (MPR)
  - Nokia CloudBand Infrastructure System (CBIS)
  - Nokia routers: MACSec key generation
- 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

Figure 1. Certified and unified Layer 1 encryption across optical and microwave transport
## Product specifications

### Security features
- NIST-certified AES-256 encryption solution for data encryption
- Random generator: Physical salt 256 bits
- LDAP support
- Secure microservices architecture
- Tamper-protected hardware

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

### 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 reset button

### Encryption hardware interworking
- Nokia 1830 PSS encrypting transponders:
  - 11QPEN4
  - S13X100E
- Nokia 1830 PSI-2T
- Nokia 1830 PSI-M
- Nokia 9500 MPR
- Nokia 7750 and 7750 routers

### Interoperability and authentication
- NTP protocol
- Customer certificates
- Authentication against SIEM
- SSL authentication SysLog
- LDAP over SSL
- LDAP group mapping

### Redundancy
- Hot swap, battery backup

### 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
**Product specifications**

<table>
<thead>
<tr>
<th>Installation options</th>
<th>• Rack mounting (2RU 19 in)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cooling</td>
<td>• Front-to-back airflow</td>
</tr>
<tr>
<td>Dimensions</td>
<td>• Height: 88 mm (3.46 in)</td>
</tr>
<tr>
<td></td>
<td>• Width: 482.6 mm (19.0 in)</td>
</tr>
<tr>
<td></td>
<td>• Depth: 394.4 mm (15.53 in)</td>
</tr>
<tr>
<td>Weight</td>
<td>10 kg (22 lb)</td>
</tr>
<tr>
<td>Power consumption</td>
<td>88 W</td>
</tr>
</tbody>
</table>

**Nokia 1830 SMS Product Family**

The Nokia 1830 SMS product family covers a range of cryptographic requirements, from the strictest government needs to protect highly sensitive enterprise customer data. Protecting different data environments often requires different security solutions. As part of Nokia’s secure transport solution, 1830 SMS provides options for Hardware Security Modules (HSM) and network-attached HSM to meet your specific needs.

### 1830 SMS

Quantum-safe, certified secure encryption key management server, supporting efficient key rotation for very high circuit counts

### 1830 SMS netHSM

Quantum-safe, certified secure encryption key management server cryptographic module, for net-HSM applications

---

**About Nokia**

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. [networks.nokia.com](http://networks.nokia.com)

Nokia operates a policy of ongoing development and has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions. Nokia assumes no responsibility for any inaccuracies in this document and reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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.

© 2020 Nokia

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

Document code: SR2003042487EN (March) CID200458