securosys

Das Hardware Sicherheits-Modul für höchste Ansprüche

Primus HSM X-Series

- Konzipiert, entwickelt und hergestellt in der Schweiz
- Marktführende Verschlüsselungsleistung
- Höchste Verfügbarkeit
- Manipulationsschutz während Transport, Aufbewahrung und Betrieb
- Einfachste Inbetriebnahme, Konfiguration und Wartung
- Integrierte Zwei-Faktor-Authentisierung
- Skalierbar und flexibel partitionierbar gemäss Ihren Bedürfnissen

Die X-Series unserer Primus HSM liefert marktführende Leistung für höchste Ansprüche an Sicherheit, Verfügbarkeit, Flexibilität und Manipulationsschutz.

Unterschiedliche Leistungsklassen

Die X-Series ist in unterschiedlichen Leistungsklassen erhältlich: X200, X400, X700, X1000 und X2000. In ihrer leistungsfähigsten Ausführung, Primus X2000, kann sie 2000 RSA-4096-Operationen pro Sekunde verarbeiten. Gruppiert können sie Georedundanz und Belastungsverteilung sicherstellen.

Anwendungen

Die Geräte der X-Series sind vielfältig einsetzbar. Sie eignen sich optimal zur Absicherung von Finanztransaktionen wie EBICS und PCI, vom Zugriff auf die Cloud (CASB), vom Schlüsselmanagement im PKI-Umfeld, Blockchain-Systemen, Datenbankverschlüsselungen (TDE), Code- sowie Dokumentensignierung und Archivierung zur Einhaltung der behördlichen Bestimmungen. Jede Anwendung kann sich über die API-Provider JCE/JCA, CNG (MS), PKCS#11 (p11-kit, OpenSSL, Apache,Nginx), oder REST.

Funktionen

Die Geräte generieren Schlüssel, speichern diese und verwalten deren Verteilung. Abgesehen davon führen sie Authentisierungs- und Verschlüsselungsaufgaben durch. Ein einzelnes Gerät kann auch partitioniert und für mehrere Benutzer zugänglich gemacht werden. Primus HSM unterstützen sowohl symmetrische (AES, Camellia) als auch asymmetrische Verschlüsselungsalgorithmen (RSA, ECC, Diffie-Hellman) und modernste Hash-Verfahren (SHA-2, SHA-3). Sie können nahtlos und einfach in beliebige Netzwerkumgebungen integriert werden. Die Primus X-Series HSM können mittels Decanus Remote Control Terminal von fern konfiguriert und überwacht werden.

securosys

Sicherheitsmerkmale

Sicherheitsarchitektur

- Mehrschichtige Sicherheitsarchitektur, die auch militärischen Sicherheitsanforderungen genügt
- Interne Überwachungsmechanismen für fehlerfreien Betrieb

Verschlüsselung / Authentisierung (Auszug)

- 128/192/256 Bit AES mit GCM-, CTR-, ECB-, CBC-, MAC-Modus
- Camellia, 3DES (Rückwärtskompatibilität), ChaCha20-Poly1305
- RSA 1024-8192, DSA 1024-8192
- ECDSA 224-521, GF(P) beliebige Kurven (NIST, Brainpool,...)
- ED25519, Curve25519
- Diffie-Hellman 1024, 2048, 4096, ECDH
- SHA-2/SHA-3 (224 - 512), SHA-1, RIPEMED-160, Keccak, HMAC, CMAC, GMAC, Poly1305
- Aufrüstbar auf quantencomputerresistente Algorithmen

Schlüsselerzeugung

- Zwei Hardwaregeneratoren zur Erzeugung von echten Zufallszahlen (TRNG)
- NIST SP800-90-kompatibler Zufallszahlengenerator

Schlüsselmanagement

- Schlüsselkapazität bis zu 30 GB
- Ultrasicherer Tresor für Langzeitschlüssel und -zertifikate
- Bis zu 120 Partitionen mit je 240 MB Kapazität

Betrieb

- Anzahl Clientverbindungen nicht beschränkt
- Unbegrenzte Anzahl Backups

Antimanipulations-Mechanismen

- Sensoren für die Detektion unberechtigter Eingriffe
- Sofortige Löschung aller Schlüssel und sensibler Daten
- Schutz vor Manipulation bei Transport und Lagerung mittels digitalem Siegel

Firmware

- Lokaler Firmware-Update auf dem Gerät oder optional mit dem Remote Control Terminal Decanus

Identitätsbezogene Authentisierung

- Mehrere Sicherheitsbeauftragte (2 aus *n*)
- Identifikation basierend auf Smartcard und PIN

Netzwerkmerkmale

Softwareintegration

- JCE/JCA Provider
- PKCS#11, P11-Kit, OpenSSL, Apache, Nginx
- Microsoft CNG
- REST (TSB Modul)

Netzwerkmanagement

- IPv4 / IPv6
- Monitoring und Logging (SNMPv2, syslog)

Gerätemanagement

- Lokale Konfiguration, Fernkonfiguration (Decanus)
- Integriertes Logging
- Firmware Update
- Ausführliche Diagnosemöglichkeiten

Technische Daten

Performance (pro Sekunde, simultan)

	RSA 4096	ECC 256	ECC 521	AES256
X2000	2000	8000	3000	10000
X1000	1000	3000	550	5000
X700	700	3000	550	3000
X400	400	3000	550	2000
X200	200	2000	350	1000

Stromversorgung

- Zwei redundante Stromanschlüsse, unterbruchsfrei anschliessbar. Zur Wahl stehen:
- 100–240 V AC, 50–60 Hz
- 36 bis 75 V DC
- Leistung: 60 W (typ.), 80 W (max.)
- Supercap zur Datenspeicherung
- Backup-Lithiumbatterie: Lithium Thionyl Chloride 0.65g Li, IEC 60086-4, UL 1642, 3.6V

Interfaces

- 4 Ethernet RJ-45-Ports mit 1 Gbit/s (Rückseite)
- 1 RS-232 Management Port (Vorderseite)
- 1 USB Management Port (Vorderseite)
- 3 Slots für Smart cards

Bedienung

- 3 Ports für Securosys Sicherheits-Smartcards
- 4 LED für System- und Interfacestatus
- Flüssigkristallanzeige mit Pad für Konfiguration
- Konsoleninterface
- Optional mit Terminal Decanus zur Fernbedienung

Elektromagnetische Kompatibilität (EMC) (Soll)

- EMV/EMC: EN 55022, EN 55024, FCC Part 15 Class B
- Sicherheit: IEC 62386-1

Spezifikationen

- Temperaturbereich (IEC 60068-2-1 Ad, IEC 60068-2-2 Bd): Aufbewahrung -25 ... +70 °C; Betrieb 0 ... +40 °C, empfohlen 1 ... 30 °C
- Feuchtigkeit (IEC 60068-2-78 Cab): 40 °C, 93% RH, nicht-kondensierend
- MTBF (RIAC-HDBU-217Plus) bei 25 °C: 100 000 h
- Abmessungen (B×H×L) 440 x 88 x 441 mm (2HE 19" EIA Standardrack)
- Gewicht 13.5 kg

Zertifizierung

- FIPS140-2 Level 3
- CC EN 419221-5 eIDAS Schutzprofil
- CE, FCC, UL

HAUPTSITZ
Securosys SA
Max-Högger-Strasse 2
8048 Zürich
SCHWEIZ
+41 44 552 31 00
info@securosys.com
www.securosys.com

DEUTSCHLAND & EU
Securosys
Deutschland GmbH
Darrestrasse 9
87600 Kaufbeuren
DEUTSCHLAND
+49 8341 438620
info@securosys.de
www.securosys.de

APAC
Securosys
Hong Kong Ltd.
Unit 704B Sunbeam Centre
27 Shing Yip Street
Kwun Tong
Hong Kong
+852 8193 1646
info-apac@securosys.com
www.securosys.com

Vorderansicht


Rückansicht

Entwickelt und hergestellt in der Schweiz. Wir sind bestrebt, unsere Angebote stets zu verbessern und behalten uns vor, Spezifikationen ohne Ankündigung zu ändern.