securosys

Das Hardware Security 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. Die Anbindung der Geräte an bestehende Systeme ist genauso einfach wie die Inbetriebnahme.

Unterschiedliche Leistungsklassen

Die X-Series ist in unterschiedlichen Leistungsklassen erhältlich: X200, X400, X700 und X1000. In ihrer leistungsfähigsten Ausführung, Primus X1000, kann sie 1200 RSA-4096-Operationen pro Sekunde verarbeiten. Auf Wunsch können Geräte dieser Series auch komfortabel mit unserem Decanus übers Netzwerk angesteuert werden, dem Terminal zur Fernbedienung.

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. Als Netzwerk-Appliance entfallen die Nachteile von auf PCIe-Karten basierenden Lösungen (Betriebssystemabhängigkeit, Update Szenario, Redundanz).

Funktionen

Die Geräte generieren Schlüssel, speichern diese und verwalten deren Verteilung. Abgesehen davon führen sie Authentisierungs- und Verschlüsselungsaufgaben durch. Gruppiert können sie Georedundanz und Belastungsverteilung sicherstellen. Ein einzelnes Gerät kann auch partitioniert und für mehrere Benutzer zugänglich gemacht werden. Primus HSM unterstützen sowohl symmetrische (AES, 3DES) 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.

securosys

Securosys SA
Förrlibuckstrasse 70
8005 Zürich
Schweiz
+41 44 552 31 00
info@securosys.ch
www.securosys.ch

Sicherheitsmerkmale

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

Verschlüsselung / Authentisierung
- 128/192/256 Bit AES mit GCM-, CTR-, GCTR-, ECB-, CBC-, MAC-Modus
- Camellia, 3DES
- RSA 1024, 2048, 3072, 4096, 8192
- ECDSA 256-521, GF(P) beliebige Kurven
- DSA 256-8192
- Diffie-Hellman 1024, 2048, 4096
- SHA-2 (256 - 512), SHA-3, SHA-1
- Aufrüstbar auf quantencomputerresistente Algorithmen

Schlüsselerzeugung
- Zwei Hardwaregeneratoren zur Erzeugung von echten Zufallszahlen (TNRG)
- 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
- Möglichkeit zur sofortigen Löschung aller Schlüssel und sensibler Daten
- Schutz vor Manipulation bei Transport und Langzeitspeicherung mittels digitalem Siegel

Firmware
- Lokaler Firmware-Update auf dem Gerät oder optional mit der Fernbedienung Decanus

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

Netzwerkmerkmale

Softwareintegration
- JCE/JCA Provider
- PKCS#11, OpenSSL
- Microsoft CNG

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

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

Technische Daten

Verschlüsselungsperformance (pro Sekunde)

	RSA 4096	ECC 521	ECC 256	AES (Mbit)
X1000	1200	1200	1200	>800
X700	700	320	1100	>700
X400	400	640	1100	>600
X200	200	160	550	>500

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

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 60950

Spezifikationen
- Temperaturbereich (IEC 60068-2-1 Ad, IEC 60068-2-2 Bd): Aufbewahrung -25 bis +70 °C; Betrieb 0 bis+40 °C
- Feuchtigkeit (IEC 60068-2-78 Cab): 40 °C, 93% RH, nicht-kondensierend
- Ausfallsicherheit 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 (in Vorbereitung)
- CC EAL 4+ zertifizierter Stammschlüsselspeicher
- CE, FCC, UL

Wir sind bestrebt, unsere Angebote stets zu verbessern und behalten uns vor, Spezifikationen ohne Ankündigung zu ändern.

Entwickelt und hergestellt in der Schweiz

DV2.11

Vorderansicht

Rückansicht