securosys

Das schlanke Hardware Sicherheits-Modul

Primus HSM E-Series

- Marktführend bezüglich Preis-Leistungs-Verhältnis
- HSM Network Appliance als Ersatz für PCIe-Karten
- Einfachste Inbetriebnahme, Konfiguration und Wartung
- Manipulationsschutz während Transport, Aufbewahrung und Betrieb
- Skalierbar und flexibel partitionierbar
- Konzipiert, entwickelt und hergestellt in der Schweiz

Die E-Series unserer Primus HSM bietet hohe Leistung zu einem unschlagbaren Preis. Die Anbindung der Geräte an bestehende Systeme ist genauso einfach wie die Inbetriebnahme.

Unterschiedliche Leistungsklassen

Die E-Series ist in unterschiedlichen Leistungsklassen erhältlich: E20, E60 und E150. Geräte dieser Series können entweder über die serielle Schnittstelle konfiguriert werden oder auf Wunsch auch komfortabel übers Netzwerk mit unserem Decanus, dem Terminal zur Fernbedienung.

Anwendungen

Die Geräte der E-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, Updateszenario, 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-Geräte 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
- 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 - 4096, ECDH
- SHA-2/SHA-3 (224 - 512), SHA-1, RIPEMD-160, Keccak, HMAC, CMAC, GMAC, Poly1305
- Aufrüstbar auf quantencomputerresistente Algorithmen

Schlüsselerzeugung

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

Schlüsselmanagement

- Schlüsselkapazität bis zu 6 GB
- Ultrasicherer Tresor für Langzeitschlüssel und -zertifikate
- Bis zu 50 Partitionen mit je 120 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 mit Fernbedienung Decanus oder virtueller Smartcard

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 (Konsole)
- Fernkonfiguration (Decanus)
- Integriertes Logging
- Firmware Update
- Ausführliche Diagnosemöglichkeiten

Technische Daten

Performance (pro Sekunde, simultan)

	RSA 4096	ECC 256	ECC 521	AES 256
E150	150	1100	180	1500
E60	60	700	120	600
E20	20	350	60	200

Stromversorgung

- Stromanschluss:
  - 100–240 V AC, 50–60 Hz
- Leistung: 30 W (typ.), 50 W (max.)
- Backup-Lithiumbatterie: Lithium Thionyl Chlorid 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 (Rückseite)
- 1 USB Management Port (Rückseite)

Bedienung

- Konsoleninterface
- 4 LED für System- und Interfacestatus
- Optional mit Decanus Remote Terminal zur Fernbedienung

Elektromagnetische Kompatibilität (EMC) (Soll)

- EMV/EMC: EN 55022, EN 55024, FCC Part 15 Class B
- Sicherheit: IEC 60950

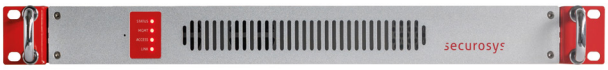
Spezifikationen

- Temperaturbereich (IEC 60068-2-1 Ad, IEC 60068-2-2 Bd): Aufbewahrung -25 bis +70 °C; Betrieb 0 bis+40 °C, empfohlen 1 .. 30˚C
- Feuchtigkeit (IEC 60068-2-78 Cab): 40 °C, 93% RH, nicht-kondensierend
- Ausfallsicherheit MTBF (RIAC-HDBU-217Plus) bei 25 °C: 80 000 h
- Abmessungen (b×h×l) 417 x 44 x 365 mm (1U 19" EIA Standardrack)
- Gewicht 5,8 kg

Zertifizierung

- FIPS140-2 Level 3
- CC EN 419221-5 eIDAS Schutz-Profil
- CC EAL 5+ 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



Vorderansicht

Rückansicht

HEADQUARTER
Securosys SA
Förrlibuckstrasse 70
8005 Zürich
SCHWEIZ
+41 44 552 31 00
info@securosys.com
www.securosys.com

GERMANY & 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