securosys

Vergleich und Entscheidungshilfe

Primus HSM X- oder E-Series?

Die Securosys Primus HSM der X- und der E-Series sind optisch unterschiedlich, verfügen aber über folgende gemeinsame Qualitätsmerkmale:

- Einfachste Inbetriebnahme, Konfiguration und Wartung
- Manipulationsschutz während Transport, Aufbewahrung und Betrieb
- Skalierbar und flexibel partitionierbar
- Konzipiert, entwickelt und hergestellt in der Schweiz
- Unterschiedliche Leistungsklassen

Beide Gerätetypen sind vielfältig einsetzbar und verfügen über dieselbe Firmware und Connectivity. Sie eignen sich optimal zur Absicherung von Finanztransaktionen wie EBICS und PCI, vom Zugriff auf die Cloud (CASB) oder vom Schlüsselmanagement im PKI-Umfeld.

Die Geräte generieren, speichern und verwalten Schlüssel. Ausserdem führen sie Authentisierungs- und Verschlüsselungsaufgaben durch. Sie können nahtlos und einfach in beliebige Netzwerkumgebungen integriert werden. Ein Gerät kann auch partitioniert und für mehrere Benutzer oder Applikationen zugänglich gemacht werden.

Diese Übersicht hat zum Ziel, die Unterschiede darzustellen und Ihnen bei der Entscheidung zu helfen. Hier die wichtigsten Kriterien:

Sie benötigen ...	... dann eignet sich für Sie ...
▪ zwingend zwei Stromanschlüsse für Redundanz bzw. Wechseln während des Betriebes	⇨ Primus X-Series
▪ höchste Verfügbarkeit	⇨ Primus X-Series
▪ höchste Verschlüsselungsleistung	⇨ Primus X-Series
▪ nicht zwingend höchste Performance	⇨ Primus E-Series

Vorderseite

X-Series

E-Series

Rückseite

X-Series

E-Series

Auf der Rückseite dieses Blattes sind die Spezifikationen dargestellt, wobei die Unterschiede speziell hervorgehoben werden. Bitte beachten Sie auch die separaten Factsheets zur X- und zur E-Series.

securosys

Sicherheitsmerkmale

Sicherheitsarchitektur

- Mehrschichtige Sicherheitsarchitektur
- Interne Überwachungsmechanismen für fehlerfreien Betrieb

Verschlüsselung / Authentisierung

- 128/192/256-Bit AES with GCM-, CTR-, ECB-, CBC-, MAC Mode
- Camellia, 3DES (Rückwärtskompatibilität), ChaCha20-Poly1305
- RSA 1024-8192, DSA 1024-8192
- ECDSA 224-521, GF(P) arbitrary curves (NIST, Brainpool,...)
- ED25519, Curve25519
- Diffie-Hellman 1024, 2048, 4096, ECDH
- SHA-2/SHA-3 (224 - 512), SHA-1, RIPEMED-160, Keccak, HMAC, CMAC, GMAC, Poly 1305
- Upgradeable to quantum computer-resistant algorithms

Schlüsselerzeugung

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

Schlüsselmanagement

- Ultrasicherer Tresor für Langzeitschlüssel und -zertifikate

	X-Series	E-Series
Schlüsselkapazität	30 GB	6 GB
Partitionen/Kapazität	bis 120 à 240 MB	bis 50 à 120 MB

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

Netzwerkmerkmale

Softwareintegration

- JCE/JCA Provider,
- PKCS#11, P11-kit, OpenSSL, Apache, Nginx
- MS CNG,

Netzwerkmanagement

- IPv4/IPv6
- Monitoring und Logging (SNMPv2, syslog)
- Ausführliche Diagnosemöglichkeiten
- Agent für Ereignisse

Gerätemanagement

- Lokale Konfiguration (Konsole)
- Fernkonfiguration (Decanus)
- Integriertes Logging
- Firmware-Update
- Ausführlich Diagnosemöglichkeiten

Technische Daten

Verschlüsselungsperformance (pro Sekunde)

	RSA 4096	ECC 256	ECC 521
X2000	2000	8000	3000
X1000	1000	3000	550
X700	700	3000	550
X400	400	3000	550
X200	200	2000	350
E150	150	1100	180
E60	60	700	120
E20	20	350	60

Stromversorgung

- Backup-Lithiumbatterie
- Stromanschlüsse:
  - **X-Series:** Zwei redundante Stromanschlüsse, unterbruchsfrei anschliessbar. Wählbar zwischen 100-240 V Wechselstrom, 50-60 Hz und 36-75 V Gleichstrom
  - **E-Series:** 100 bis 240 V Wechselstrom, 50 bis 60 Hz
- Leistung:
  - **X-Series:** 60 W (typ.), 80 W (max.)
  - **E-Series:** 35 W (typ.), 50 W (max.)
- Spezielles
  - **X-Series:** Supercap zur Datenspeicherung

Bedienung

- Konsoleninterface
- **X-Series:** Bedienungseinheit mit Display
- 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

- Temperaturbereiche (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:
  - **X-Serie:** 100 000h
  - **E-Series**: 80 000h
- Abmessungen (b×h×l)
  - **X-Series:** 440 x 88 x 441 mm; passt in ein 2HE 19" EIA Standardrack
  - **E-Series:** 417 x 44 x 365 mm; passt in ein 1 HE 19" EIA Standardrack
- Gewicht: **X-Series** 13,5 kg, **E-Series** 5,8 kg

Zertifizierung

- FIPS140-2 Level 3 Betriebsmodus
- CC EAL 4+ zertifizierter Stammschlüsselspeicher
- CC EN 419221-5 eIDAS protection profile (in progress)
- CE, FCC, UL

Interfaces

- 4 Ethernet RJ-45-Ports mit 1 Gbit/s (Rückseite)
- 1 RS-232 Management Port
- 1 USB Management Port
- **X-Series:** 3 smartcard slots

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

HAUPTSITZ
Securosys SA
Förrlibuckstrasse 70
8005 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