securosys

El asequible módulo de seguridad de hardware Primus HSM E-Series

- Relación calidad-precio líder en el mercado
- Dispositivo de red HSM como reemplazo de las tarjetas PCIe
- Instalación, configuración y mantenimiento sencillos
- Protección contra manipulaciones durante el transporte, el almacenamiento y el funcionamiento
- Escalable y flexible , particionable según sus necesidades
- Diseñado, desarrollado y fabricado en Suiza

La serie E de nuestro HSM Primus ofrece un alto rendimiento a un precio excepcional. La conexión de los dispositivos a los sistemas existentes es tan fácil como la puesta en marcha.

Diferentes Clases de Rendimiento

La serie E está disponible en varias clases de rendimiento: E20, E60 y E150. Se puede configurar a través del puerto serie o a través de la red con nuestro terminal remoto Decanus.

Aplicaciones

Los dispositivos de la serie E son muy versátiles. Construidos como dispositivos de red , carecen de las desventajas de las soluciones basadas en PCIe, como la dependencia del software de los sistemas host PCIe y el propio sistema host. La serie E es ideal para proteger transacciones financieras como EBICS y PCI, acceso a la nube (CASB), gestión de claves en el entorno PKI o para proteger sistemas blockchain, gestión de criptoactivos .

Funciones

Los dispositivos generan claves de cifrado, almacenan y gestionan la distribución de estas claves. Además de la gestión de claves, también realizan tareas de autenticación y cifrado. Se pueden agrupar varios HSM Primus para admitir la redundancia y el equilibrio de carga.Cada HSM Primus también se puede particionar para varios usuarios (multiusuario). Primus admite algoritmos criptográficos simétricos (AES, Camellia), asimétricos (RSA, ECC, Diffie-Hellman) y hashing (SHA-2, SHA-3). Se pueden integrar sin problemas y fácilmente en cualquier entorno de red. El HSM Primus E-Ries se puede controlar a distancia con nuestro terminal de control remoto Decanus.

securosys

Características de seguridad

Arquitectura de seguridad
Arquitectura de seguridad multinivel
Supervisión interna de hardware para operaciones sin errores

Cifrado/Autenticación (extracto)
AES de 128/192/256 bits con modo GCM, CTR, ECB, CBC y MAC
Camelia, 3DES (legado), ChaCha20-Poly1305
RSA 1024-8192, DSA 1024-8192
ECDSA 224-521, Curvas arbitrarias GF(P) (NIST, Brainpool,...) ED25519, Curva25519Diffie-Hellman 1024-4096, ECDH
SHA-2/SHA-3 (224-512), SHA-1, RIPEMD-160, Keccak, HMAC, CMAC, GMAC, Poly1305
Actualizable a algoritmos resistentes a ordenadores cuánticos

Generación de claves
Dos generadores de números aleatorios verdaderos (TNRG) de hardware Generador de números aleatorios compatible con NIST SP800-90

Gestión de claves
Capacidad de claves: hasta 6 GB
Bóveda ultrasegura para claves y certificados a largo plazo
Hasta 50 particiones @ 120 MB de capacidad

Operación
Número ilimitado de copias de seguridad
Número de conexiones de cliente no restringidas

Mecanismos antimanipulación
Varios sensores para detectar accesos no autorizados
Destrucción activa de material clave y datos confidenciales en caso de manipulación
Protección contra manipulaciones durante el transporte y el almacenamiento durante varios años mediante precinto di- gital

Firmware
Actualización local del firmware en el dispositivo o, opcionalmente, en el mando a distancia Deca- nus

Autenticación basada en identidad
Múltiples oficiales de seguridad (2 de *n*)
Identificación basada en tarjeta inteligente y PIN usando Decanus Remote o a través de las funciones de red de tarjetas inteligentes virtuales

Funciones de red

Integración de software
Proveedor de JCE/JCA
PKCS#11, P11-Kit, OpenSSL, Apache, Nginx
GNC de Microsoft
REST (Módulo TSB)

Gestión de redes
IPv4/IPv6
Supervisión y registro (SNMPv2, syslog)

Gestión de dispositivos
Configuración local (consola)
configuración remota (Decanus)
Registro integrado
Actualización de firmware
Funciones de diagnóstico mejoradas

Datos técnicos

Rendimiento (por segundo, simultáneo)
RSA 4096 ECC 256 ECC 521 AES 256 E150 150 1100
180 1500
E60 60 700 120 600
E20 20 350 60 200

Poder
Fuente de alimentación:
100 ... 240 V CA, 50 ... 60 Hz
Disipación de potencia: 30 W (típico) ... 50 W (máx.)
Batería de litio de respaldo: cloruro de tionilo de litio 0,65 g de litio, IEC 60086-4, UL 1642, 3,6 V

Interfaces
4 puertos Ethernet RJ-45 con 1 Gbit/s (trasero)
1 puerto de gestión RS-232 (trasero)
1 puerto de gestión USB (trasero)

Mandos
Interfaz de consola
4 LEDs para el estado del sistema y de la interfaz (multicolor) Terminal de control remoto Decanus opcional

Especificaciones de la prueba ambiental (objetivo)
EMV/EMC: EN 55022, EN 55024, FCC Parte 15
Clase B Seguridad: IEC 60950

Especificaciones
rangos de emperatura (IEC 60068-2-1 Ad, IEC 60068-2-2 Bd): almacenamiento -25...+70 °C; funcionamiento 0...+40 °C, recomendado +1 .. 30°C
Humedad (IEC 60068-2-78 Cabina): 40 °C, 93% HR, sin concentración
MTBF (RIAC-HDBU-217Plus) a tamb = 25 °C: 80 000 h
Dimensiones (an×h×d) 417 x 44 x 365 mm (se adapta a un bastidor estándar EIA de 1U de 19" - ver foto a continuación)
Peso 5,8 kg

Certificación
FIPS140-2 Nivel 3
Perfil de protección CC EN 419221-5 eIDAS
Almacenamiento de claves raíz con certificación CC EAL 5+
CE, FCC, UL

Nos esforzamos por mejorar continuamente nuestras ofertas y, por lo tanto, nos reservamos el derecho de cambiar las especificaciones sin previo aviso.
Diseñado y fabricado en Suiza