Cryptographic Module Validation Program CMVP

Certificate #3925

Details

Module Name	CryptoServer Se-Series Gen2
Standard	FIPS 140-2
Status	Active
Sunset Date	5/9/2026
Overall Level	3
Caveat	When operated in FIPS mode
Module Type	Hardware
Embodiment	Multi-Chip Embedded
Description	The CryptoServer Se-Series Gen2 is an encapsulated, protected security module realized as a multi-chip embedded cryptographic module as defined in FIPS 140-2. Its realization meets the overall FIPS 140-2 Level 3 requirements. The module's primary purpose is to provide secure cryptographic services such as encryption or decryption (for various cryptographic algorithms like AES and Triple-DES), hashing, signing and verification of data (RSA, ECDSA, DSA), random number generation, on-board secure key generation, key storage and further key management functions in a tamper-protected environment.
Tested Configuration(s)	- N/A

Approved Algorithms

AES	Certs. #C1114, #C1130, #C1132, #C1134 and #C1245
CKG	vendor affirmed
CVL	Certs. #A1019, #C1115, #C1116, #C1135 and #C1163
DRBG	Cert. #A1066
DSA	Cert. #C1189
ECDSA	Certs. #C1190 and #C1191
ENT	P
HMAC	Cert. #C1136
KAS-SSC	vendor affirmed
KBKDF	Cert. #C1162
KDA	vendor affirmed
KTS	vendor affirmed
KTS	AES Certs. #C1130, #C1132 and #C1245; key establishment methodology provides between 128 and 256 bits of encryption strength
KTS	AES Cert. #C1114 and AES Cert. #C1134
RSA	Certs. #C1192 and #C1193
SHA-3	Cert. #C1118
SHS	Certs. #A1065, #C1117 and #C1119
Triple-DES	Cert. #C1121

Allowed Algorithms	Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength); Diffie-Hellman (shared secret computation provides between 112 and 256 bits of encryption strength); EC Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength); EC Diffie-Hellman (shared secret computation provides between 112 and 256 bits of encryption strength); RSA (CVL Certs. #C1115 and #C1116, key wrapping; key establishment methodology provides between 112 and 256 bits of encryption strength)
Hardware Versions	[CryptoServer Se-Series Gen2 5.01.2.0, CryptoServer Se-Series Gen2 5.01.4.0, and CryptoServer Se-Series Gen2 5.01.4.2] and optional component: crypto accelerator Exar DX8204
Firmware Versions	SecurityServer-Se2-Series-4.32.0.3-FIPS
Product URL	http://hsm.utimaco.com/cryptoserver/securityserver-se-gen2/

Vendor

Utimaco IS GmbH
Germanusstraße 4
Aachen 52080
Germany

Erling Wesselhoff
erling.wesselhoff@utimaco.com
Phone: +49 241-1696-200
Fax: +49 241-1696-199

Digitally signed by BACIU VICTOR
Date: 2022.11.07 10:04:06 EET
Reason: MoldSign Signature
Location: Moldova

Related Files

Security Policy
Consolidated Certificate

Validation History

Date	Type	Lab
5/10/2021	Initial	PENUMBRA SECURITY