Cryptographic Module Validation Program

Certificate #3350

Details

Module Name	Sansec HSM
Standard	FIPS 140-2
Status	Active
Sunset Date	1/2/2024
Validation Dates	1/3/2019
Overall Level	3
Caveat	When operated in FIPS mode
Security Level Exceptions	• Mitigation of Other Attacks: N/A
Module Type	Hardware
Embodiment	Multi-Chip Stand Alone
Description	The Sansec Hardware Security Module (HSM) is a hardware cryptographic module that provides data encryption, data decryption, signature generation, signature verification, message digest, message authentication code (MAC), random number generation and key management services to business systems.
Tested Configuration(s)	• N/A

FIPS Algorithms

AES	Certs. #5693 and #5694
CKG	vendor affirmed
DRBG	Cert. #2306
DSA	Cert. #1465
ECDSA	Cert. #1546
HMAC	Cert. #3792
KBKDF	Cert. #241
KTS	AES Cert. #5693 and HMAC Cert. #3792
RSA	Certs. #3064 and #3065
SHA-3	Cert. #59
SHS	Cert. #4564
Triple-DES	Cert. #2853

Allowed Algorithms	NDRNG; RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
Hardware Versions	SecHSM-V2
Firmware Versions	1.0.12
Product URL	http://www.sansec.com.cn/en/HSM.html

Vendor

Beijing Sansec Technology Development Co., Ltd
16F Huacai Building, No.16 Guangshun North Street
Chaoyang District
Beijing, Beijing 100102
China

Yongxin Xu
xuyongxin@sansec.com.cn
Phone: +86-531-88988936

Related Files

Security Policy
Consolidated Certificate

Lab

ATSEC INFORMATION SECURITY CORP
NVLAP Code: 200658-0