

Cryptographic Module Validation Program

Certificate #3205

Details

Module Name

SafeNet Luna K7 Cryptographic Module

Standard

FIPS 140-2

Status

Active

Sunset Date

6/24/2023

Validation Dates

6/25/2018

11/20/2018

Overall Level

3

Caveat

When operated in FIPS mode and initialized to Overall Level 3 per Security Policy

Module Type

Hardware

Embodiment

Multi-Chip Embedded

Description

The SafeNet Luna K7 Cryptographic Module is a high-assurance, tamper-resistant Hardware Security Module which secures sensitive data and critical applications by storing, protecting and managing cryptographic keys. It provides end users with industry-leading security and performance, and can quickly be embedded directly into servers and security appliances for FIPS 140-2 validated key security. The module meets compliance and audit needs for FIPS 140, HIPAA, PCI-DSS, eIDAS, GDPR.

FIPS Algorithms

| | |
|----------------|--|
| AES | Certs. #4753 and #4754 |
| CVL | Certs. #1392 and #1431 |
| DRBG | Cert. #1634 |
| DSA | Certs. #1274 and #1275 |
| ECDSA | Certs. #1188 and #1189 |
| HMAC | Cert. #3166 |
| KAS | Certs. #133 and #134 |
| KBKDF | Cert. #152 |
| KTS | AES Cert. #4753 ; key establishment methodology provides between 128 and 256 bits of encryption strength |
| RSA | Certs. #2597 , #2598 , #2631 and #2632 |
| SHS | Certs. #3896 , #3897 , #3951 and #3952 |
| Triple-DES | Cert. #2525 |
| Triple-DES MAC | Triple-DES Cert #2525 , vendor affirmed |

Allowed Algorithms

AES (Cert. [#4753](#), key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength); Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength); NDRNG; RSA (key wrapping; key establishment methodology provides between 112 and 152 bits of encryption strength); Triple-DES (Cert. [#2525](#), key unwrapping; key establishment methodology provides 112 bits of encryption strength)

Hardware Versions

808-000048-002, 808-000066-001, 808-000073-001

Firmware Versions

7.0.1, 7.0.2, 7.0.3

Vendor

[Gemalto](#)

20 Colonnade Road, Suite 200
Ottawa, ON K2E 7M6
Canada

Security & Certifications Team
SecurityCertifications@gemalto.com

Related Files

[Security Policy](#)
[Consolidated Certificate](#)

Lab

EWA CANADA
NVLAP Code: 200556-0