Cryptographic Module Validation Program

Certificate #2714

Details

Module Name
IDPrime MD 830-revB

Standard
FIPS 140-2

Status
Active

Sunset Date
8/18/2021

Validation Dates
8/19/2016
1/24/2018
8/2/2018

Overall Level
3

Caveat
When operated in FIPS mode

Module Type
Hardware

Embodiment
Single Chip

Description

IDPrime MD 830-revB is a Minidriver enabled PKI smartcards, working seamlessly with any Microsoft® environment (without any additional middleware), and offering all the necessary services (with either RSA or Elliptic curves algorithms) to secure an IT Security and ID access infrastructure.

Tested Configuration(s)

- N/A

FIPS Algorithms

AES	Cert. #3779
CVL	Cert. #719
DRBG	Cert. #1045
ECDSA	Cert. #814
KBKDF	Cert. #81
KTS	AES Cert. #3779; key establishment methodology provides between 128 and 256 bits of encryption strength
RSA	Certs. #1946 and #1947
SHS	Cert. #3146
Triple-DES	Cert. #2100

Other Algorithms

EC Diffie-Hellman (CVL Cert. #719, key agreement; key establishment methodology provides between 112 and 192 bits of encryption strength); NDRNG; RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

Hardware Versions

SLE78CFX3000PH and SLE78CFX3000PH PICO

Firmware Versions

IDCore30-revB - Build 06, IDPrime MD Applet V4.3.5.D and MSPNP Applet V1.2

Vendor

Gemalto
20 Colonade Road, Suite 200
Ottawa, ON K2E 7M6
Canada

Frederic GARNIER
Frederic.Garnier@gemalto.com
Phone: +33 442364368
Fax: +33 442366953
Arnaud Lotigier
Arnaud.LOTIGIER@gemalto.com
Phone: +33 4.42.36.60.74
Fax: +33 4.42.36.55.45

Related Files

Security Policy
Consolidated Certificate

Lab

InfoGard Laboratories, Inc.
NVLAP Code: 100432-0