Cryptographic Module Validation Program

Certificate #2098

Details

Module Name
IDPrime MD 830

Standard
FIPS 140-2

Status
Active

Sunset Date
8/3/2021

Validation Dates
3/5/2014
8/4/2016
4/3/2018

Overall Level
3

Caveat
When operated in FIPS mode

Module Type
Hardware

Embodiment
Single-chip

Description

IDPrime MD 830 is a Minidriver enabled PKI smartcard, offering all the necessary services (with either RSA or Elliptic curves algorithms) to secure an IT Security and ID access infrastructure.

FIPS Algorithms

AES	Cert. #2261
CVL	Cert. #41
ECDSA	Cert. #363
KTS	AES Cert. #2261; key establishment methodology provides between 128 and 256 bits of encryption strength
RSA	Certs. #1158 and #1163
SHS	Cert. #1946
Triple-DES	Cert. #1413
Triple-DES MAC	Triple-DES Cert. #1413, vendor affirmed

Other Algorithms

EC Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength); RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

Hardware Versions

SLE78CFX3009P

Firmware Versions

IDCore30 Build 1.17, IDPrime MD Applet version V4.1.2.F and MSPNP Applet V1.0

Vendor

Gemalto
Avenue du Jujubier, Z.I Athelia IV
La Ciotat 13705

France

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
NVLAP Code: 100432-0