tokenMe EVO

Safety doesn't happen by chance

tokenME is a practical small device able to carry users digital identities and to be easily integrated into preexisting PKI infrastructures

eIDAS compliant

AUTHENTICATION AND DIGITAL SIGNATURE WITH A TINY TOKEN

The fast growth of electronic frauds and data theft is making security a major issue in the ICT sector. The safest solution is currently represented by the adoption of PKI infrastructures and therefore the digital certificates are used as credentials.
Thanks to the capability of computing asymmetric algorithms tokenME EVO generates the certificates within its secure element, that can be used as credentials over PKI infrastructures for the users Strong Authentication (2 factors) process and for Digital Signature

tokenME EVO is compliant with the most common operating systems and its adherence to CCID and PC/SC standards allows an easy and full integration in preexisting infrastructures without additional driver installation. Its compact size makes it an easy portable device and can be inserted into standard USB ports simultaneously with other devices as it does not obstruct any other adjacent slot.

tokenME EVO is excellent for:
qualified digital signature as defined in the eIDAS European regulations for the digital signature or Personal Identification validation tool (PIV) for US applications.

The tokenME EVO therefore becomes the secure container of your digital identity whatever standard you need to comply with.

MAIN FEATURES

- Strong Authentication SSL/TLS with most common browsers
- Smart Card Logon
- Memory : 80 Kb (up to 128Kb as optional)
- Speed up to 412,903 bps
- Token SW for the management of PIN, PUK and digital certificates
- Shortcut protection
- Compatibility and certifications : EN 60950/IEC 60950, ISO-7816, PC / SC, CE, FCC, RoHS, VCCI, CCID, Microsoft WHQL, EMV

COMMON CRITERIA VERSION

- Qualified Digital Signature eIDAS compliant
- EAL5+ without application
- EAL4+ PP SSCD with the IAS ECC applet
- EAL4+ PP-BAC, EAC, BAP, EAP with the LDS applet

FIPS FEATURES VERSION

- Certification: FIPS 140-2 Level 3
- Global platform 2.1.1
    - DAP RSA : to secure applet loading with PKI
    - Secure channel protocol SCP 01/SCP 02 and SCP03 (based on AES algorithm)
    - GP 2.1.1 commands : Store Data / Process Data / Extradite
    - Delegated Management

TECHNICAL FEATURES

Communication interface
USB full speed

Dimensions
50mm(H)X20mm(W)X8mm(L)

Weight
8 g

Connector
USB type A or type B

Supply Voltage/Recharge
5V DC (from USB port)/50mA max

Operating Temperature
0-50° C

Data retention
10 years minimum

Insertion cycles
100.000 cycles minimum

API & supported standards
PKCS#11, Microsoft CSP/CSP-NG, TokenD, PC/SC, X.509 v3, SSL v3, IPSec

Secure Element
NXP JCOP 3 P60 series

Algorithms
DES | 3DES: algorithm with 2 and 3 keys
AES: 128, 192, 256bits
RSA: Cipher/Decipher, (SFM&CRT) from 512 up to 2048 bits (steps of 32b)
RSA Key Generation: up to 4096
EC: DSA GF(p) from 160 up to 521 bits
EC-DH from 160 up to 521 bits
EC Key Generation: up to 512 bits
SHA: SHA1, SHA-224, SHA-256, SHA384, SHA512 EC-DSA SHA-1, SHA-256, SHA-224, SHA-384 and SHA-512

RNG
Pseudo/Secure Random

System Requirements
Windows Vista | Win 7 | 8 | 8.1, 10 | Windows Server 2003 | 2008 (R2) | 2013 | 2016
Mac 10.9 and above,
Linux, Android 5.0 and above