

Badgeo FIDO2 + QSCD

FIDO2 + PKI contact smart card Passwordless



The universal strong authentication and qualified digital signature solution 100% Made in Europe

- ✓ JCOP4 smart card certified Common Criteria EAL6+
- ✓ eIDAS QSCD-certified PKI applet
- ✓ Middleware SafeSign Identity Client
- ✓ FIDO2 (CTAP 2.1) + FIDO U2F applet
- ✓ Interfaces MIFARE, DESFire EV2/EV3
- ✓ Contactless / NFC options: ISO 15693 and 125 KHz

FIDO2 + QSCD products are compatible with the majority of of deployed business applications.



Robust middleware

SafeSign Identity Client
(CSP/KSP/PKCS#11)



Integrated smart card (Mini SIM)

- Java Card™ JCOP4
 - CC EAL6+
- DES/3DES, AES, ECC, RSA



Wide compatibility

- Strong authentication, directories, PKI, SSO, VPN, encryption, digital signature
- Windows 10/11 with Microsoft Entra ID, Google, GitHub... and identity federations such as Evidian, Ilex, Okta, Ping Identity...



Badgeo FIDO2 + QSCD is a contact smart card made in Europe. It integrates an eIDAS QSCD-certified PKI applet and a FIDO2 (CTAP 2.1) and FIDO U2F applet. Badgeo FIDO2 + QSCD thus allows users to benefit from high-quality logical security solutions as well as an extremely reliable qualified digital signature solution, while remaining easy to use.

- ✔ Meets European security requirements (eIDAS, QSCD, NIS, PSD2...)
- ✔ Options: physical access with MIFARE, DESFire EV2/EV3 and ISO 1569
- ✔ Protection against phishing and preservation of the integrity of electronic documents
- ✔ No “key wrapping” / No shared key preinstalled

Interface(s)

- Contact: ISO 7816
- Contactless / NFC: MIFARE, DESFire EV2/EV3
- Contactless / NFC options: 15693 and 125 KHz

Smart card

- Java Card™ JCOP4 certified Criteria Common EAL6+

Supported Operating Systems

- QSCD: Windows, Mac OS, Linux
- FIDO: Windows

Browsers

- Edge, Firefox, Chrome, Safari

QSCD features

- Supported crypto-algorithms:
 - RSA 2K (bits)
 - RSA 3K (3072 bits)
 - RSA 4K (4096 bits)
 - ECC NIST P-256 / SECG secp256r1 (256 bits)
 - ECC NIST P-384 / SECG secp384r1 (384 bits)
 - ECC NIST P-521 / SECG secp521r1 (521 bits)
- Options:
 - PIN
 - PIN length between 5 and 15 bytes
 - PIN try limit set to 3
 - PUK
 - PUK length between 5 and 15 bytes
 - PUK try limit set to 3

FIDO2.0 / FIDO2.1 features

- Supported signature-algorithm:
 - ECC NIST P-256 / SECG secp256r1 (256 bits)
- Extensions:
 - credProtect
 - hmac-secret
 - credBlob (personalization option)
 - largeBlobKey (personalization option)
 - minPinLength (personalization option)
- Options :
 - rk (resident keys) - Discoverable credentials
 - Maximum number limited by available persistent memory (256 to 512 bytes per credential)
 - clientPIN, PIN protocol 1 and PIN protocol 2
 - PIN length between 4 and 63 bytes
 - PIN try limit set to 8. After 8 unsuccessful tries, the authenticator must be reset
 - No default value
 - ep - Enterprise Attestation (personalization option)
 - All options and extensions supported (pinUvAuthToken, authnrCfg, largeBlobs...)

Dimensions and weight

- Size: length 85.6 mm / width 54 mm / height 0.76 mm
- Weight: 5 g



About NEOWAVE and AET Europe

NEOWAVE and AET Europe solutions address the cybersecurity, digital trust and Identity Access Management markets. NEOWAVE is a French company, specializing in strong authentication and secure transactions. NEOWAVE products combine the high level of security provided by smart cards with the advantages of connectivity and storage technologies: USB, RFID / NFC and Bluetooth Low Energy (BLE).

AET Europe is a Dutch company, developing software solutions for user identification, authentication and digital signatures. AET Europe products are SafeSign IC, BlueX Certificate Management and ConsentID.

NEOWAVE

Pôle d'activités Y. Morandat, 1480 avenue
d'Arménie, 13120 Gardanne - France

+33 (0)4 42 50 70 05

contact@neowave.fr

www.neowave.fr



aet europe

IJsselburcht 3, NL-6825 BS Arnhem,
Pays-Bas

+31 26 365 33 50

sales@aeteurope.com

www.aeteurope.com