NEOWAVE

Winkeo-C FIDO2 + QSCD

Passwordless FIDO2 + PKI USB-C token

CYBERSECURITY™
MADE IN EUROPE

eIDAS   fido ALLIANCE

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

- ✓ USB-C PC/SC smart card and HID
- ✓ JCOP4 smart card certified Common Criteria EAL6+
- ✓ eIDAS QSCD-certified PKI applet
- ✓ Middleware SafeSign Identity Client
- ✓ FIDO2 (CTAP 2.1) + FIDO U2F applet

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...

ACN
Alliance pour la confiance numérique

AKTANTIS

UGAP

fido ALLIANCE

Winkeo-C FIDO2 + QSCD is a USB-A token made in Europe. It integrates an eIDAS QSCD-certified PKI applet and a FIDO2 (CTAP 2.1) and FIDO U2F applet. Winkeo-C 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...)
- ✅ User presence by button
- ✅ Protection against phishing and preservation of the integrity of electronic documents
- ✅ No "key wrapping" / No shared key preinstalled

Interface(s)
• USB-C 2.0 PC/SC + HID

Smart card
• Micro SIM : ISO 7816 Java Card™ JCOP4 certified Criteria Common EAL6+

Supported Operating Systems
• Windows, Mac OS, Linux, Android, iOS

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 43.8 mm / width 18 mm / height 9.76 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.