



Winkeo-A FIDO2 + QSCD

USB-A security key with middleware

The universal solution
for strong authentication and electronic signature

100% Made in Europe



- 1 For strong authentication and qualified electronic signature
- 2 eIDAS QSCD-certified PKI applet
- 3 Compliant with FIDO2 (CTAP 2.1) and FIDO U2F standards
- 4 Contact smart card (ISO 7816) JCOP4 certified Common Criteria EAL6+
- 5 Meets European security requirements (eIDAS, QSCD, NIS, PSD2...)

Winkeo-A FIDO2 + QSCD is compatible with systems that support PC/SC and HID protocols.



Winkeo-A FIDO2 + QSCD features:

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

- USB 2.0 Type-A interface
- Contact smart card (ISO 7816) JCOP4 certified Common Criteria EAL6+
- Compatible with systems supporting PC/SC and HID protocols
- Compatible with Windows, Mac OS and Linux operating systems
- User presence by button
- No “key wrapping” / No shared key preinstalled
- Dimensions and weight: Length 43.8 mm / Width 18 mm / Thickness 9.76 mm / Weight 5g

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.

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 supported options and extensions (pinUvAuthToken, authnrCfg, largeBlobs...)



NEOWAVE

Pôle d'activités Y. Morandat,
1480 avenue d'Arménie,
13120 Gardanne - France
T : +33 (0)4 42 50 70 05
• www.neowave.fr
• contact@neowave.fr

 **aet europe**

IJsselburcht 3,
NL-6825 BS Arnhem,
The Netherlands
T : +31 26 365 33 50
• www.aeteurope.com
• sales@aeteurope.com

Member of:

 **POLESCS**

 **HEXATRUST**
CYBERSECURITY & DIGITAL TRUST

 **fido**
alliance
member



 **ACN**
Alliance pour la confiance numérique