



VOTRE PARTENAIRE TECHNOLOGIQUE POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES



EXPERTISE
Des solutions adaptées
à chaque environnement



CONFIANCE
Un partenaire fiable
à vos côtés



PERFORMANCE
Des infrastructures
sécurisées et évolutives



SUPPORT
Un accompagnement
technique de qualité



HAFS
Distributeur à valeur ajoutée

Des solutions IT innovantes pour
un monde connecté et sécurisé



**WIRELESS
RADIO**
Connectivité sans fil
haute performance



**RÉSEAUX &
SÉCURITÉ IT**
Des réseaux fiables
et sécurisés



**VIRTUALISATION
CLOUD**
Des solutions Cloud
flexibles et évolutives



CYBERSECURITY
Protéger vos données
et vos systèmes



**VIDÉO
PROTECTION**
Solutions de vidéosurveillance
intelligentes



**HCI STOCKAGE
SAUVEGARDE**
Stockage, sauvegarde
et haute disponibilité

SOLUTIONS IT

CYBERSÉCURITÉ

CLOUD

INFRASTRUCTURE RÉSEAU

STOCKAGE

PROTECTION



NEOWAVE
Authentification forte et transactions sécurisées

Qui sommes-nous ?



Société française créée en 2007 par des experts de la sécurité Informatique et des transactions sécurisées



Offre

- Solutions d'authentification forte
- Produits à base de composants sécurisés et de certificats numériques



Gammes de produits

- Produits PKI/QSCD
- Produits FIDO2
- Produits FIDO2+OTP
- Produits FIDO2+QSCD
- Lecteurs de carte à puce



Marchés

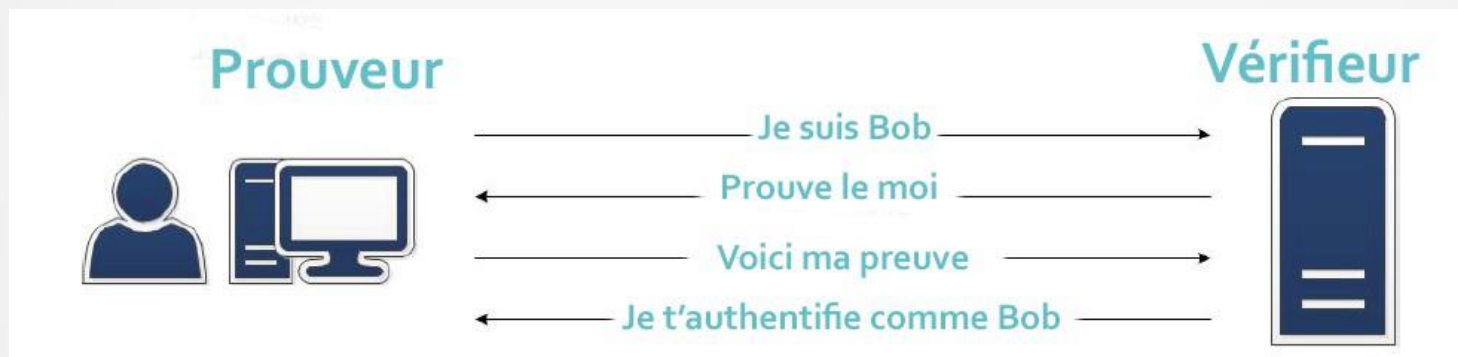
Cybersécurité, confiance numérique et gestion des identités (IAM)



Qu'est-ce que l'authentification ?

L'authentification implique un contrôleur et un vérificateur.

L'authentification est précédée d'une phase d'identification



L'identification consiste à indiquer l'identité d'une personne ou d'une chose

L'authentification est le processus de vérification de l'identité.

Qu'est-ce que le MFA ?

L'authentification multifactorielle (AMF) consiste à vérifier l'identité d'un utilisateur en combinant au moins 2 des 3 facteurs d'authentification



Connaissances

Ce que je sais
(un mot de passe ou un code secret)



Possession

Ce que j'ai
(téléphone mobile, carte à puce, clé de sécurité, etc.)



Inhérence

Ce que je suis / ce que je fais
(reconnaissance vocale ou faciale, empreinte digitale, un comportement...)

L'utilisation du MFA tend à se généraliser. De plus en plus de services informatiques poussent, voire imposent le MFA (récemment Salesforce, Whatsapp...).

Qu'est-ce que l'authentification forte ?

L'authentification forte, une authentification résistante au phishing



CERTIFICAT AUTHENTICATION

Stockés dans des
cartes à puce



PROTOCOLES FIDO2 & FIDO U2F

Basé sur les
normes libres et
ouvertes de
l'Alliance FIDO



Certains PROTOCOLES OTP

HOTP, TOTP,
OCRA

L'authentification
forte repose sur
un mécanisme de
cryptographie.

NEOWAVE

NEOWAVE

Quelle méthode d'authentification ?

Adapter l'authentification en fonction des risques et des défis

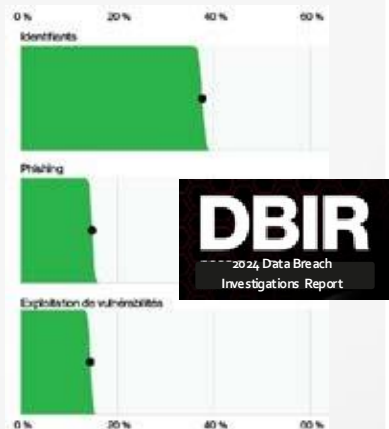
Données très sensibles	Niveau de menace élevé (système d'information de l'administration...) Aurait un impact catastrophique sur l'organisation organisation ou les individus	Authentification forte
Données sensibles	Niveau de menace moyen (courrier électronique professionnel...)	Authentification forte et/ou MFA
Données moyennement sensibles	Niveau de menace moyen (contenu de sites web publics...) n'aurait pas d'impact catastrophique sur l'organisation ou les individus	MFA Ou un mot de passe fort
Données peu sensibles	Faible niveau de menace (plateforme de réservation de courts de tennis...)	Mot de passe

Recommandations de la CNIL (Commission Nationale de l'Informatique et des Libertés)

Le Phishing : Plaie globale



Rapport d'activité 2024 de Cybermalveillance.gouv



Les trois principaux moyens par lesquels les attaquants accèdent à une organisation sont le vol d'identifiants, le phishing et l'exploitation des vulnérabilités.

Les identifiants volés sont la principale méthode employée par les cybercriminels pour accéder à une entreprise.

(Source : rapport DBIR 2024 de Verizon)

NEOWAVE

Des protections existantes inefficaces

Phishing
facile



SMS
OTP



SMS
OTP



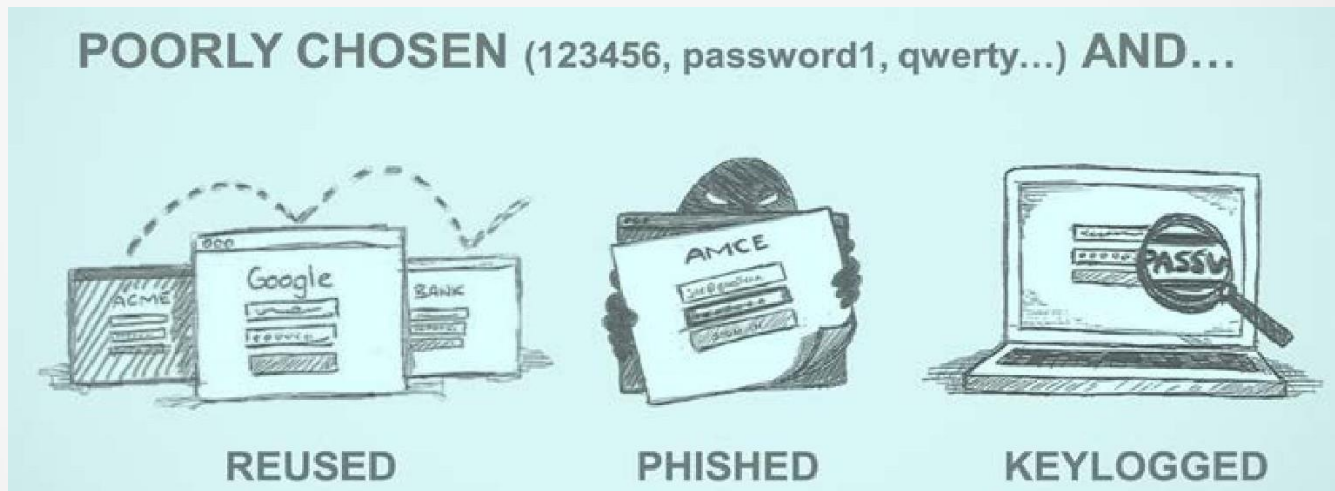
SMS et OTP ne protègent PAS contre le Phishing

Pourquoi une authentification forte ?

90% des brèches sont liées à l'authentification

Définition du phishing : Tentative d'acquisition d'informations sensibles, souvent pour des raisons malveillantes, en se faisant passer pour une entité digne de confiance dans une communication électronique.

La MFA n'est pas
considérée comme
une authentification
forte





CYBERSECURITYTM
MADE IN EUROPE

Produits PKI/QSCD



Badgeo QSCD

- Carte à puce à contact ISO 7816
- Certification QSCD/eIDAS



Badgeo HYB QSCD

- Carte à puce à contact ISO 7816
- Certification QSCD/eIDAS
- Contrôle d'accès physique
DESFire



Winkeo2J-A (C) QSCD

- Token USB-A (C)
- Certification QSCD/eIDAS



Composant carte à puce avec OS
JavaCard certifié CC EAL6+
Certification QSCD/eIDAS

+



Middleware SafeSign
Identity Client (IC)

NEOWAVE

Marchés pour les produits QSCD => contrôle d'accès logique (et physique)

Le secteur public :

- La fonction publique d'état et hospitalière
- Les collectivités territoriales (+500 postes de travail)

Le secteur privé :

- Les OIV (Opérateurs d'Importance Vitale)
- Les ETI/Groupes de +500 postes de travail

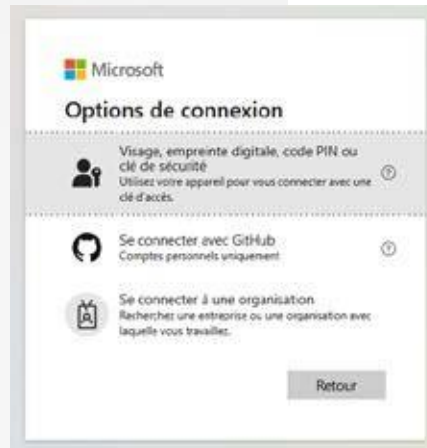
Les autorités de certification :

Toutes les ACs françaises sont nos clientes !

Badgeo QSCD

Badgeo HYB QSCD

Winkeo2J-A (C) QSCD



- Logon Windows par carte à puce
 - Branchez votre token USB ou utilisez votre carte à puce avec votre lecteur carte à puce (à contact ou NFC)
 - Entrez votre Code PIN
 - Votre session Windows s'ouvre
- Impossible de cloner votre identité stockée sur le token USB ou sur la carte à puce

L'offre produits QSCD

- Les produits QSCD :

- Le token USB ou la carte à puce
- Le middleware AET SafeSign IC
- La personnalisation graphique et électrique



- Support et formation

Large compatibilité



PKI, SSO, VPN, Chiffrement, Signature Electronique...

**Un réseau de partenaire « Premium »
complet et éprouvé**

Badgeo QSCD, Badgeo HYB QSCD, Winkeo2J-A (C) QSCD

Qualification et/ou distribution des produits QSCD par un réseau de partenaires spécialisés :

Intégrateurs en sécurité :

CS, ATOS, Thalès, SCC,
Econocom, Inmac Wstore,
Hermitage Solutions,
Horoquartz...

Autorités de certifications et
fournisseurs de PKI :

Oodrive/CertEurope, ATOS/IDnomic
Docaposte/Certinomis, Chambersign,
Almerys/Be-Ys, Tessi/Certigna,...

Des éditeurs de logiciel :

CS, The GreenBow, Ilex International, Prim'X,
AET Safesign, ATOS/Evidian, Systancia,...

Principales références produits QSCD

Entreprises



Administrations et services publics



Authentification forte pour le Web/Cloud

Clé USB



Carte à puce NFC



Carte à puce à contact



PRODUITS SIMPLES, ROBUSTES et SECURISÉS



NEOWAVE

Qu'est ce que FIDO ?



FIDO (Fast IDentity Online) est une alliance internationale pour :



- Renforcer la sécurité des accès Web (login + mot de passe) et remplacer les solutions à base d'OTP (One Time Password)
- Promouvoir des solutions interopérables
- Faciliter l'expérience utilisateur

FIDO est une solution d'avenir qui répond au défi actuel
de la sécurisation des accès Web.

Produits FIDO2 (Passkeys)



Winkeo-C FIDO2

- Clé de sécurité USB-C compatible FIDO2
- Visa de sécurité ANSSI



Winkeo2-A (C) FIDO2

- Clés de sécurité USB-A (C) compatibles FIDO2 (CTAP 2.0)



Badgeo DUAL FIDO2



- Carte à puce à contact et sans contact/NFC compatible FIDO2 (CTAP2.1)
- Certification FIDO
- Contrôle d'accès physique DESFire

Distributeurs et revendeurs des produits FIDO2

Europe

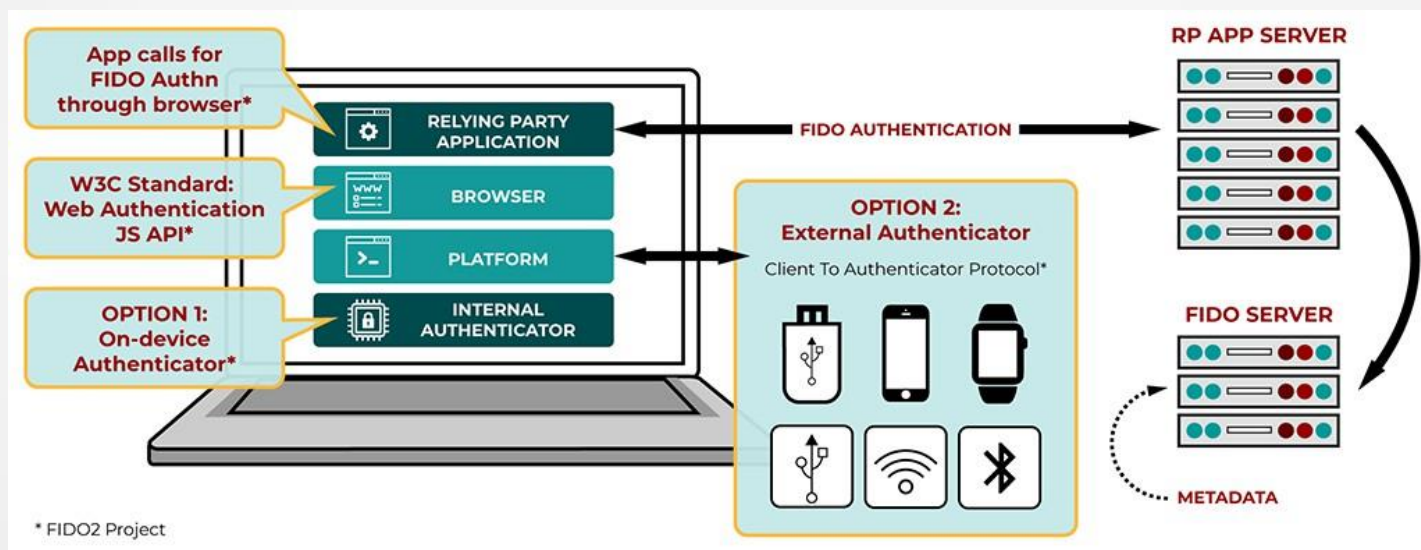
- Hermitage Solutions (France/Belgique)
- Econocom, SCC
- UGAP / OFFICE XPRESS(France)
- Open Seas (Royaume-Uni)

Afrique et Moyen Orient

- Finatech (Maroc)
- SPG (Tunisie)
- Thauranix (Afrique du Sud)

FIDO2 W3C Authentification Web avec les protocoles CTAP (Client To Authenticator Protocols)

FIDO2 prend en charge les expériences utilisateurs passwordless, second facteur et MFA avec des authentificateurs (tels que les clés de sécurité FIDO, les appareils mobiles, les wearables, etc.)



Recommandé par  Microsoft

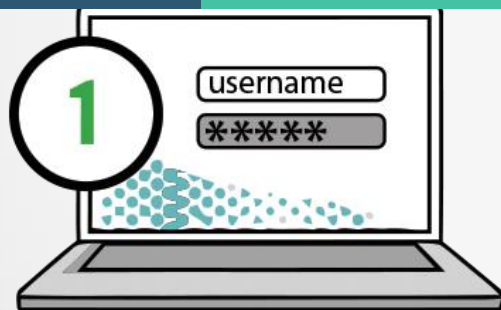
NEOWAVE

- ProSoft, MADA (Allemagne)
- Octane (Pologne et Pays d'Europe Centrale)
- Hart 4 Technology (Pays-Bas)

- www.authentication-web.com
- Amazon France, Espagne, UK, Allemagne, Italie, Belgique, Pays-Bas,....
- Cdiscount
- Rakuten
- MarkIT



NEOWAVE



Recommandé par

Google

NEOWAVE

Les services Web compatibles FIDO



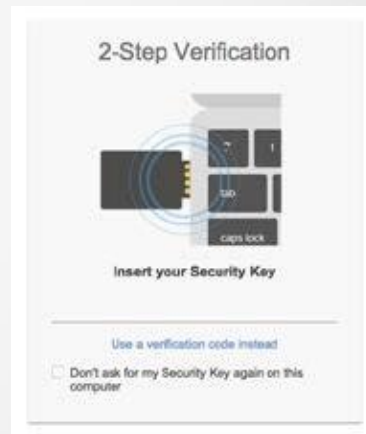
Services FIDO

FIDO2 supporté nativement par Windows 10/11
et Azure Active Directory (AAD)



Les produits FIDO2 de NEOWAVE sont qualifiés et référencés par Microsoft

Plus de 400 fournisseurs de services IT dans
le monde ont adopté les standards FIDO



NEOWAVE

Nos principales références clients

Secteur public :



Secteur privé:



Produits FIDO2+OTP



Winkeo2J-A FIDO2+OTP

- Clé de sécurité USB-A compatible FIDO2 (CTAP2.1) et OTP (TOTP, HOTP)
- Certification FIDO



Winkeo2J-C FIDO2+OTP

- Clé de sécurité USB-C compatible FIDO2 CTAP2.1) et OTP (TOTP, HOTP)
- Certification FIDO



Badgeo DUAL FIDO2+OTP

- Carte à puce à contact et sans contact/NFC compatible FIDO2 (CTAP2.1) et OTP (TOTP, HOTP)
- Certification FIDO
- Contrôle d'accès physique DESFire



Badgeo NFC FIDO2+OTP

- Carte à puce sans contact/NFC compatible FIDO2 (CTAP2.1) et OTP (TOTP, HOTP)
- Certification FIDO
- Contrôle d'accès physique DESFire



Produits FIDO2+QSCD



CYBERSECURITY™
MADE IN EUROPE



Badgeo FIDO2+QSCD

- Carte à puce à contact ISO 7816
- Compatible FIDO2 (CTAP2.1)
- Certification FIDO
- Certification QSCD/eIDAS



Badgeo HYB FIDO2+QSCD

- Carte à puce à contact ISO 7816
- Compatible FIDO2 (CTAP2.1)
- Certification FIDO
- Certification QSCD/eIDAS
- Contrôle d'accès physique DESFire



Winkeo2J-A (C) FIDO2+QSCD

- Token USB-A (C)
- Compatible FIDO2 (CTAP2.1)
- Certification FIDO
- Certification QSCD/eIDAS



Composant carte à puce avec OS
JavaCard certifié CC EAL6+
Compatible FIDO2 (CTAP2.1)
Certification FIDO
Certification QSCD/eIDAS



Middleware SafeSign
Identity Client (IC)

NEOWAVE

CLÉS DE SÉCURITÉ ET CARTES À PUCES NEOWAVE

NEOWAVE

✓ YES

✓ OPTDNL

✗ NO

	QSCDrange				FIDO2range								FIDO2+OTP range				FIDO2+QSCDrange			
USB-A	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗
USB-C	✗	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗
Contact ISO/IEC 7816	✗	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗
Contactless / NFC ISO/IEC 14443-A	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓
DisFire EV2, EV3	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓
ISO 15693 - 125KHz	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓
FIDO2 CTAP2.1	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
FIDO2 CTAP2.0	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
FIDO U2F	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PKI / QSCD	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓
HOTP / TOTP	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
Capacitive button	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗
OS																				
GlanceSecurity Made in Europe Label	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
eIDAS certified	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓
ANSSI Security Via Common Criteria EAL certified	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
FIDO L1 Certified	6+	6+	6+	6+	5+	5+	6+	6+	5+	6+	6+	6+	6+	6+	6+	6+	6+	6+	6+	6+
	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

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 / www.authentication-web.com

NEOWAVE

Lecteurs de carte à puce (1/2)



CYBERSECURITYTM
MADE IN EUROPE

LinkeoA-Y

- Lecteur USB-A PC/SC de carte à puce à contact
- Insertion horizontale



LinkeoC-Y

- Lecteur USB-C PC/SC de carte à puce à contact
- Insertion horizontale



LinkeoA-NFC

- Lecteur USB-A PC/SC de carte à puce sans contact/NFC
- ISO 14443 A,B , ISO 18092 NFC



Winkeo2-A (C) SIM

- Lecteur USB-A (C) PC/SC de carte à puce à contact au format Micro-SIM



Weneo-A SIM

- Lecteur USB-A PC/SC de carte à puce à contact au format Mini-SIM
- Logement pour Tag RFID/NFC



LinkeoA-D

- Lecteur USB-A PC/SC de carte à puce à contact
- Insertion verticale



NEOWAVE

Lecteurs de carte à puce (2/2)

Holdeo



- Lecteur de carte à puce à contact : carte professionnel de santé (CPS), carte agent (Pass'IN), future carte nationale d'identité numérique (CNIE)
- Format porte-badge
- Bluetooth Low Energy (BLE) > 5.0
- USB-C PC/SC
- SDK Android et iOS
- Mode sécurisé



LinkeoC-PRO



- Lecteur USB-C PC/SC de carte à puce à contact (ISO 7816) et sans contact (NFC / RFID) avec gestion du PIN CACHING
- Lecteur multifonction pour usage professionnel
- Écran graphique OLED et clavier
- Support des cartes à microprocesseurs et des cartes à mémoire
- Support des cartes sans contact / NFC
- Signatures multiples avec saisie unique du code PIN

Principales références Lecteurs de carte à puce

Entreprises



Autorités de certifications et organisations professionnelles



Administrations et services publics



Avantages compétitifs des produits NEOWAVE

100% conçus et fabriqués en France (assemblage et personnalisation)



CYBERSECURITYTM
MADE IN EUROPE

- ❑ Qualité, sécurité (pas de back door/ pas de compromis sur la sécurité*) * Failles identifiées chez d'autres fabricants étrangers
- ❑ Produits conçus pour une fabrication française/européenne
- ❑ Capacité de personnalisation, numéros uniques, logos,...
- ❑ Qualité et proximité du support technique
- ❑ Agilité d'une PME avec les compétences d'un grand groupe



Très haut niveau de certifications et de qualifications

- ❑ Certifications/qualifications ANSSI, FIDO et eIDAS
- ❑ Composants certifiés critères communs EAL5+ et EAL6+
- ❑ Produits FIDO2 qualifiés et référencés par Microsoft
- ❑ Label Cybersecurity Made In Europe
- ❑ Produits conformes aux exigences de sécurité européennes : NIS2, RGPD, PSD2,....



NEOWAVE



Département
Commercial



Vous accompagne



HAFS NETWORKS WCA



+225 07 89 82 56 49 / +225 07 59 05 85 82



sales-ci@hafs-networks.com



HAFS NETWORKS FRANCE



+33 (0)7 49 92 62 57 / +33(0)9 73 89 20 39



sales@hafs-networks.com

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

