White Paper – The “Winkeo FIDO2” Security Key Use-Case

Seal SQ
STRONG AUTHENTICATION

Winkeo FIDO2

FIDO SECURITY KEY

The following pages explain the need for strong authentication solutions in today's connected world, and the advantages of FIDO keys. It highlights the advanced performance and security features of the WINKEO FIDO security key. These features are the result of an extensive collaboration with SEAL SQ and are powered by its MS 6003 series secure element, Common Criteria CCEAL5+ Certified.

Contents

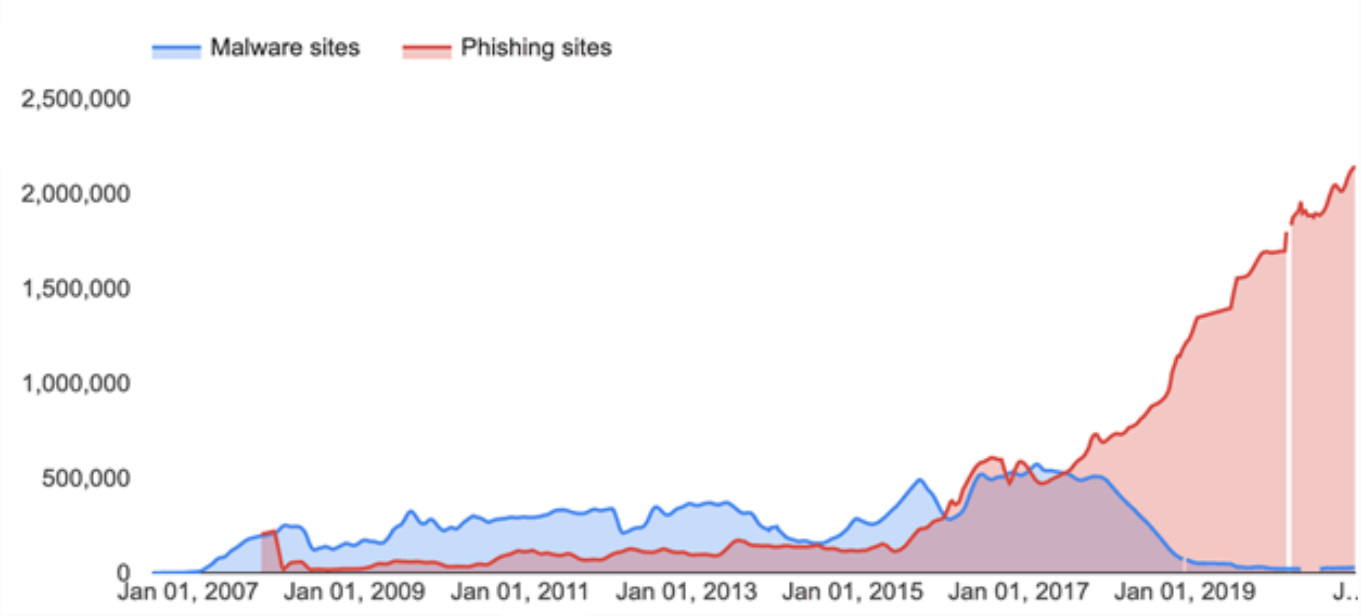
CYBERSECURITY CONTEXT

Strong authentication is now part of our daily life. The sophistication of data theft techniques is such that a simple authentication is no longer enough to guarantee optimal protection. Additional security is essential.

Increased use of connected devices and online services raise huge cybersecurity challenges whether for states, businesses or individuals. These new uses store more personal and confidentiels data every day. They break the traditional user security boundaries.

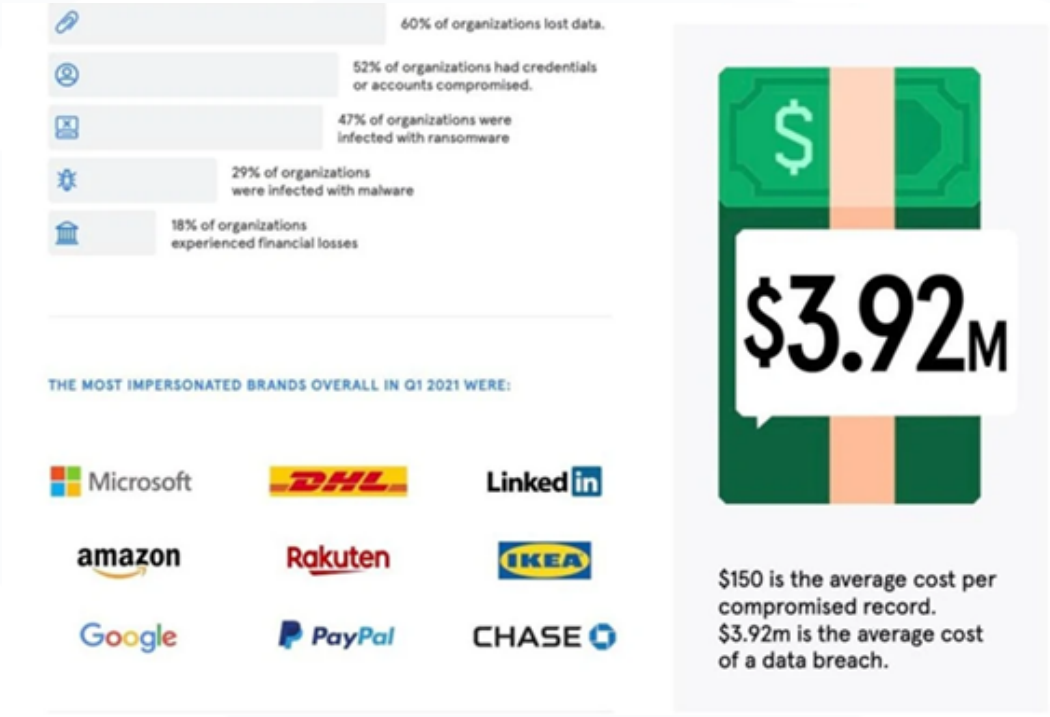
Increasingly sophisticated hacking techniques are emerging: MITM (Man-In-The-Middle), phishing attacks, malware and other cyber attacks that have become more complex. Strengthening access and data security becomes a necessity.

In practice, attackers may have gained access to your account in several ways: a too simple password, the use of the same password on several sites one of which has been hacked…
2021 Tessian* research found that employees receive an average of 14 malicious emails per year. Some industries were hit particularly hard, with retail workers receiving an average of 49. CISCO's 2021 Cybersecurity threat trends report suggests that at least one person clicked a phishing link in around 86% of organizations. The company's data suggests that phishing accounts for around 90% of data breaches.



In 2021, RiskIQ estimated that businesses worldwide lose $1,797,945 per minute due to cybercrime—and that the average breach costs a company $7.2 per minute. IBM's 2021 research into the cost of a data breach ranks the causes of data breaches according to the level of costs they impose on businesses.

Phishing ranks as the second most expensive cause of data breaches—a breach caused by phishing costs businesses an average of $3.92 million, according to IBM. And Business Email Compromise (BEC)—a type of phishing whereby the attackers hijack or spoof a legitimate corporate email account—ranks at number one, costing businesses an average of $5.01 million per breach.

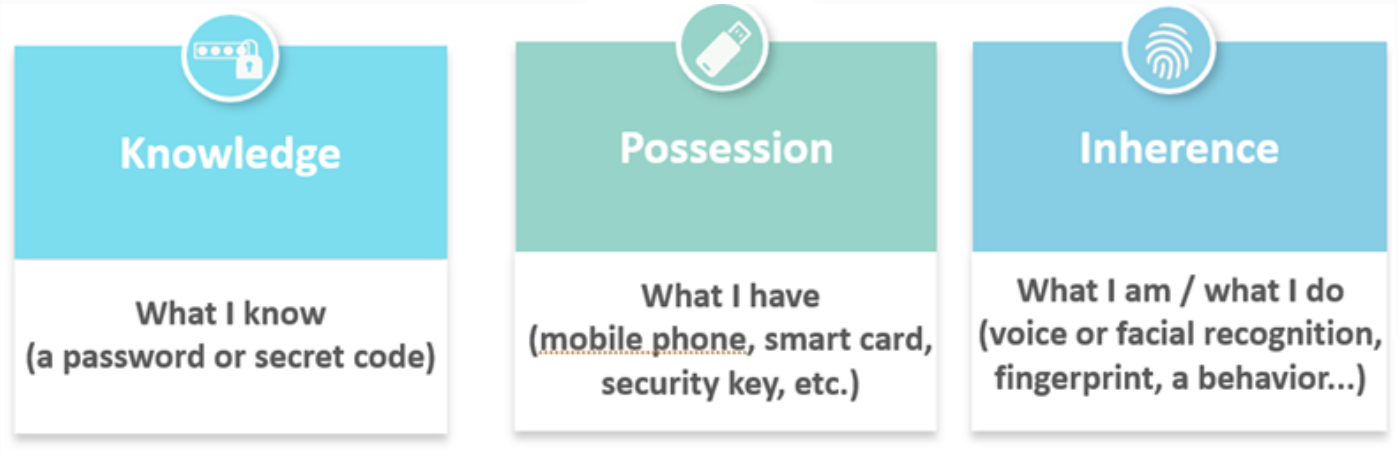


Source: IBM security Data breach report

The rise of hybrid work environments, expanding threats and a growing demand for flexibility and adaptability are leading organizations to invest on new Identity and Access Management (IAM) capabilities. According to a survey ran by Statista* in 2020 on over 300 organizations of 2000+ workers, 67% of CIOs were planning to increase investment on Password-less Authentication technologies in the coming years.

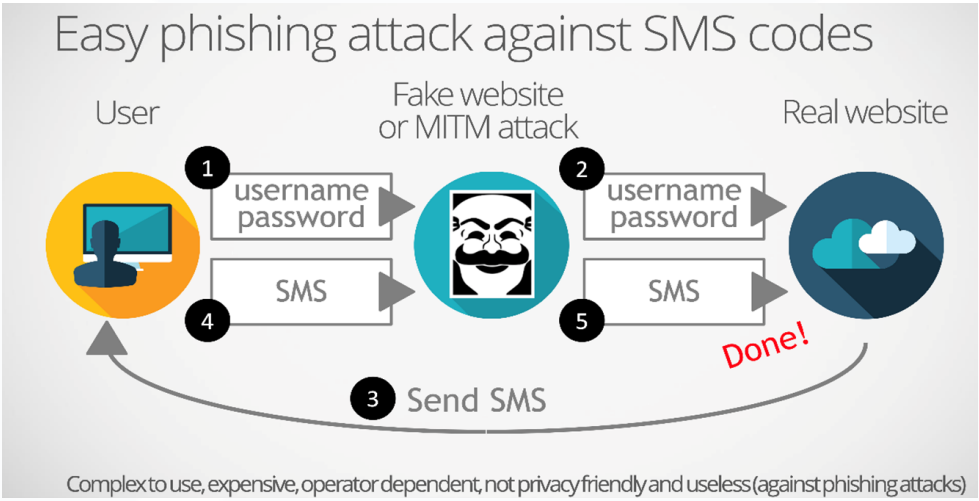
LEVELS OF SECURITY

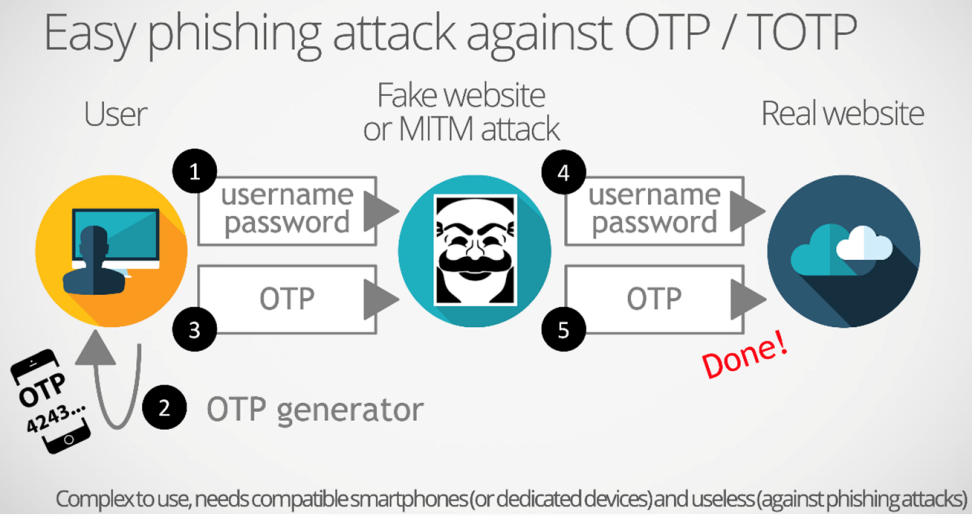
Simple authentication using a single factor such as a password is no longer sufficient. It shouldn't be relied on as the only method to keep accounts safe as they are an easy target for hackers. Multifactor authentication, MFA, adds an additional layer of security to online services and accounts. This procedure consists of verifying the identity of the originator by the combination of at least 2 of the following 3 criteria:



The use of MFA tends to become widespread. More and more IT services are pushing or even imposing MFA (recently Salesforce, Whatsapp…).
This method provides a step up in security but is not 100% effective against common threats like phishing and other advanced attacks. MFA does not constitute strong authentication.

Attempts to strengthen sign in security with SMS transmitted codes and locally generated OTP codes have been shown to have vulnerabilities (text messages can be intercepted on the phone network and OTP codes relayed during 'time-of-use » phishing attacks).



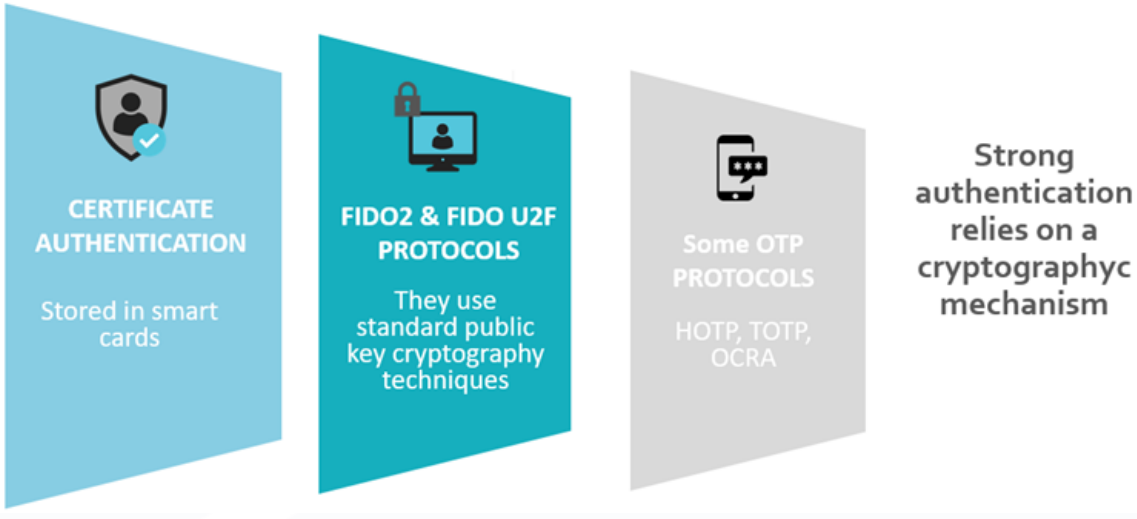


STRONG AUTHENTICATION

Strong authentication becomes essential when data or services are highly sensitive. It constitutes a phishing-resistant authentication.

According to the the CNIL, Commission Nationale Informatique & Libertés, the French Data Protection Agency, in order to be considered strong, authentication must use a possession factor incorporating a qualified or certified safety component and be based on cryptographic mechanisms. The CNIL recommends favoring the use of strong authentication methods based on cryptographic mechanisms in accordance with the RGS (The French General Security Reference).

Among the examples of strong authentication listed by the CNIL:



Strong authentication based on a possession factor which is an item of equipment assigned to a single user guarantees a high level of security. It must be equipped with a security component allowing cryptographic keys to be stored and handled securely.
Parameters and security are deemed to be robust with a strong authentication relying on a cryptographic mechanism. The secret element is generally a cryptographic key.

FIDO strong authentication: NEOWAVE's Winkeo FIDO2 (+U2F) security key

What is FIDO?

The FIDO (Fast IDentity Online) consortium is an international alliance that collaborates to strengthen the security of Web access. The FIDO Alliance's function is to propose and promote security architectures:

- stronger – that go beyond password and One-Time-Password (OTP) solutions
- interoperable
- simpler for consumers to use

The FIDO Alliance has been working to define a secure and universally supported standard, the FIDO standard. It is already adopted by most world Internet leaders such as Google, Microsoft, Facebook, Bank of America, Wordpress, etc…
Based on free and open standards from the FIDO Alliance, FIDO Authentication enables password-only logins to be replaced with secure and fast login experiences across websites and apps.

How FIDO works?

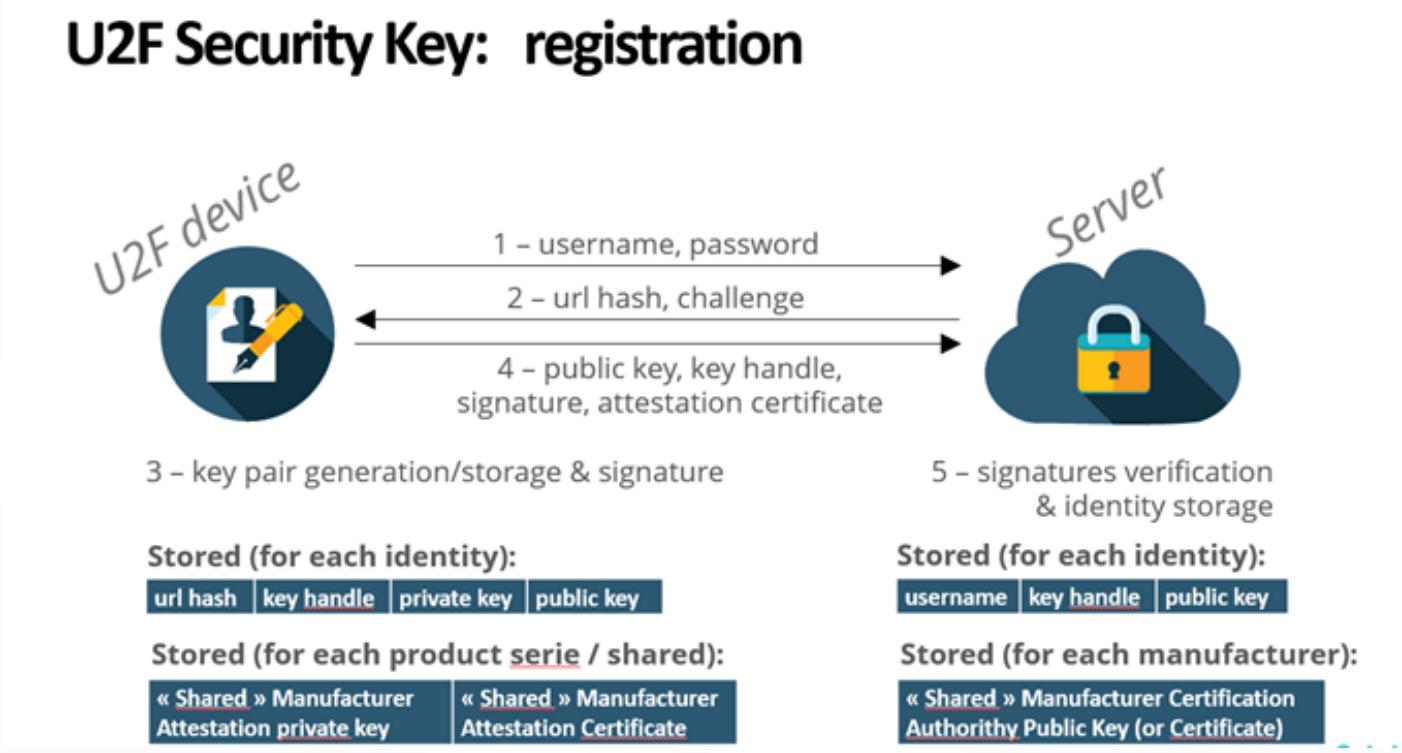
The different FIDO protocols use asymmetric public key cryptography. They make it possible to stop phishing attacks with secure second factor (FIDO U2F standard) and achieve password-less or PIN protected authentication (FIDO2 standard).
Before authentication process, the user must first register the security device (a key or a smart card). He has to do it only once. Upon registration, a private and public key pair is generated. The private key is stored on the local device and never leaves it, which prevents from server-side secrets to be stolen. The FIDO public key is stored in the web service key database.
Authentication will now only be possible by justifying the private key that the user must unlock by an action (entering a PIN code, inserting a two-factor device, pressing a button, etc.). Even if the login data is hacked, attacks are impossible because the private key associated with dedicated hardware is needed to access the web service or application.

NEOWAVE, a specialist in strong authentication, offering FIDO products

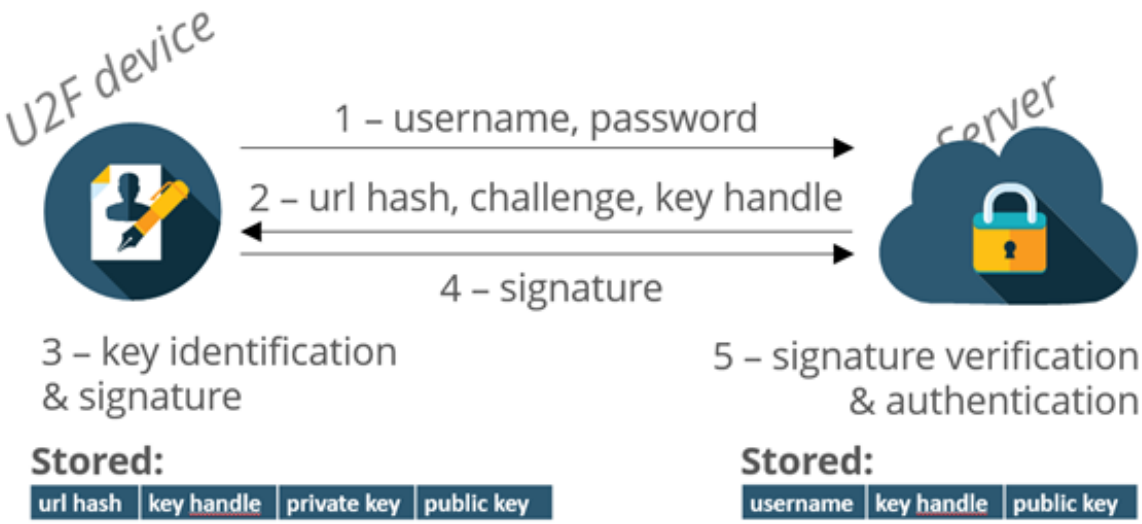
NEOWAVE is an innovative company specializing in strong authentication and secure transactions. NEOWAVE's main mission is to protect companies' and individuals' digital assets through strong authentication technologies based on secure components and digital certificates. NEOWAVE has adopted the FIDO standard and developed its FIDO solutions. The products in this range are based on the U2F (Universal Second Factor) and FIDO2 protocols.

FIDO U2F protocol:

It supports a second factor experience. It allows online services to augment the security of their existing password infrastructure by adding a strong second factor to user login.



U2F Security Key: authentication



U2F Security Key: Browser as a client

Use-case: Second-factor authentication with a WINKEO FIDO2 (+U2F) key:

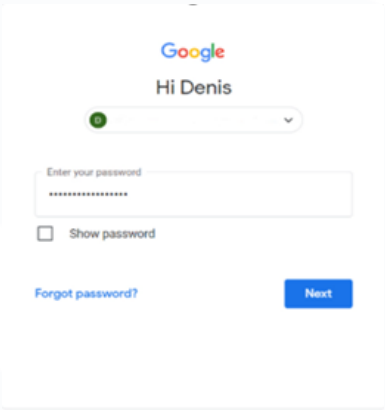
1. I activate the “Two-step validation” section

Before using your Winkeo FIDO2 (+U2F) key, you have to set up two-factor authentication on your online account if it is not yet done. Once activated, you will have to associate your Winkeo FIDO2 (+U2F) key to your account. Most web services follow a similar process consisting in selecting the “Security” tab in the “Settings” to activate the “Two-step validation” section and then to “Add a Security Key”.

2. I authenticate myself

For any future connection to your online account, you will now need to enter your login and password then insert the Winkeo FIDO2 (+U2F) security key and press the button on the security key to authenticate yourself.

You will find the procedure on Google here after as an example:



Enter your login and password

Insert your security key into the computer

Press the button on the security key to authenticate yourself

For a step by step tutorial: https://authentification-web.fr/set-up/
To know the FIDO U2F compatible services: https://authentification-web.fr/services-compatibles-fido-u2f /
It is possible to use the same Winkeo key for two-factor authentication on hundreds of different web accounts and services. However, it is necessary to register the key with each service prior to use.

FIDO U2F is dedicated to:

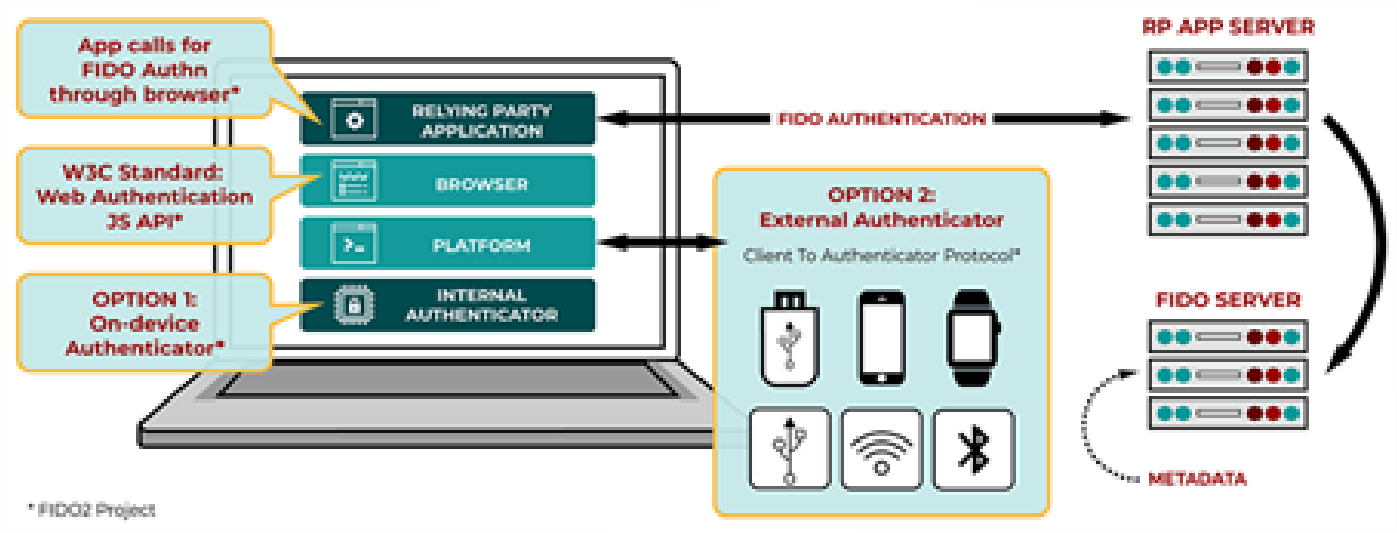
- Enterprises which have moved to Google Cloud Platform, Salesforce, etc
- Corporate: Online services with high security requirements:
  - Dematerialization and trusted services
    - Digital signature
    - Registered letter
    - Online consent
  - Cloud / Content Manager / Health Data (Hosting / CMS)
  - Financial Services (banks, crypto-currencies / Bitcoin).
- Users: FIDO compatible web service providers

FIDO U2F is classified “substantial eIDAS level” and can be the perfect authentication tool to activate/use HSM and other “High eIDAS level” certified secure elements.

FIDO2 protocol:

Thanks to the integration of the W3C Web Authentication with Client-to-Authenticator, Protocols (CTAP), the FIDO protocol allows not only encrypted and anonymous connections, but also connections without passwords.

It supports password less, second-factor and multi-factor user experiences with authenticators (such as FIDO Security Keys, mobile devices, wearables, etc.).



Use-case: Passwordless authentication with a WINKEO FIDO2 (+U2F) key:

To associate the Winkeo FIDO2 (+U2F) key with online services and applications, we invite you to contact NEOWAVE team or your system / network administrator in order to follow the recommendations and the appropriate procedure.

If you want to register and then select the Winkeo FIDO2 (+U2F) key at the sign-in interface as a means of passwordless authentication using Microsoft:
You will find the official documentation on the integration of FIDO2 to sign in to your Azure AD joined Windows 10 device here after: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

We suggest you a summary guide for setting up a Winkeo key as a means of authenticating a user of the Azure Active Directory company directory and opening Windows 10 sessions: https://authentification-web.fr/set-up/

To know the FIDO2 compatible services: https://authentification-web.fr/services-compatibles-fido2/

Once your FIDO2 (+U2F) key is associated with your user account, the procedure for any future connection to your account will be to insert your security key into your computer, then enter the PIN code of the security key and finally press the key's button to authenticate yourself and open your session.

You will find the procedure on signing in to your Azure AD joined Windows 10 device as an example:

Insert your security key into the computer

Enter the PIN code of your security key

Press the button on the security key to authenticate yourself

It is possible to use the same Winkeo key for passwordless logins on hundreds of different web accounts and services. However, it is necessary to register the key with each service prior to use.

To test a FIDO2 key https://webauthn.io

FIDO2 is dedicated to:

- All users of Azure Active Directory and Windows 10 Systems
  - Ideal authentication method in case of shared computers
  - Field technicians, Families, small and medium offices
  - Integrated and promoted by Microsoft

- All Trusted Service Provider companies
  - eIDAS Electronic IDentification Authentication and trust Services regulation
  - IDECYS+: by CertEurope – trusted third party of Oodrive group
    - Provides a simple, convenient and secure digital identity to 15 000 companies
    -

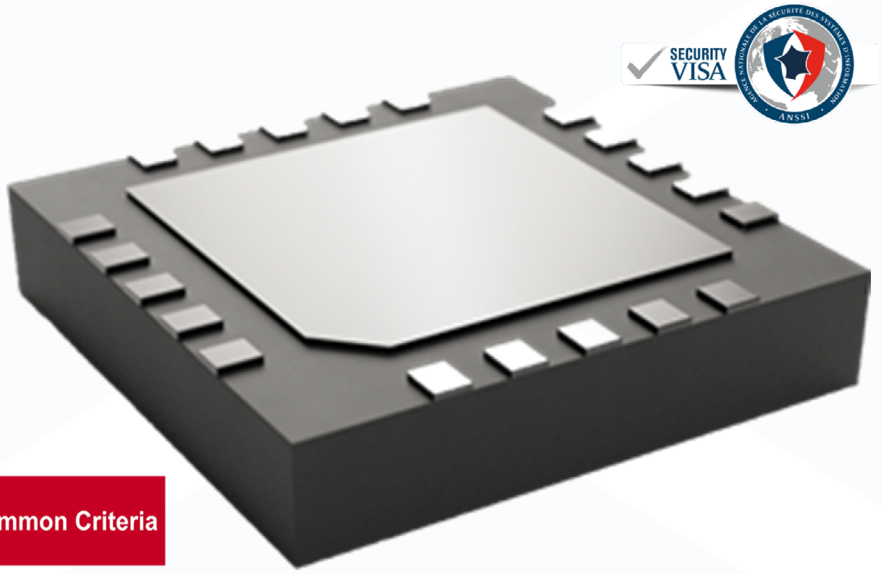
FIDO2/WebAuthn:

- Integrated by Microsoft on OS level
- If your company is using AzureAD you can use FIDO2 Devices to open Windows

FIDO is a solution of the future that meets the current challenge of securing web access.

NEOWAVE has chosen to design and to make trusted hardware devices, security keys and smart cards, that integrate components secured by SEAL SQ and that implement the FIDO protocol. The combination of FIDO authentication with such hardware device ensures a very high level of security while simplifying the user experience.

SECURE COMPONENT MAIN FEATURES



NEOWAVE's FIDO products embed a SEAL SQ's secure micro controller, part of the MicroXsafe SEAL SQ chip family. A CC EAL 5+ Certified Secure Controller family delivered with SDK for OS development. Targeted applications are Secure storage (crypto wallets, encrypted hard drives & dongles), Access control (FIDO dongles, access cards), and generally any custom applications.

The Chip used by NEOWAVE is the MS-6003 and has been exclusively designed to offer a tamper resistant platform for the development of sensitive applications in embedded systems. It is based on the 32-bit ARM Secure core SC300, has 1Mbyte flash and 24kByte of RAM.

The chip has fully integrated USB interface, including 48MHz clock generation, 8kV ESD protection and a nano-powered Real Time clock, which makes it an excellent choice for the production of secure USB dongles like FIDO keys.

The embedded security features of the chip include protections against a range of physical attacks, voltage, frequency and temperature monitors, scrambled memory and the like, allowing it to pass the Common Criteria EAL5+ certification, one of the highest levels of certified tamper resistance.

Using the provided library and extended guidelines on secure firmware development, NEOWAVE has been able to create the FIDO USB keys responding to the highest security standards.

About SEAL SQ

SEAL SQ (NASDAQ: WKEY; SIX Swiss Exchange: WIHN) is a leading global semiconductors and cybersecurity company.

SEAL SQ Semi-conductor's division is based in the French Silicon Valley in the south of France. It is one of the only 6 semiconductors companies in the world that can develop certified secure micro controllers to protect the exponentially growing number of digital interactions between people, applications and objects.

For more than two decades SEAL SQ Semiconductors has been developing secure chips, secure embedded firmware, and trusted hardware provisioning services, leading to more than 51 families of patents related to secure micro controllers.

SEAL SQ chips are designed, tested and produced using the highest standards of security, reliability and quality. Operations are run under certified environment (ISO 27001)

SEAL SQ is working with leading Security Certification labs. As a member of International Security Working Groups SEAL SQ participates in defining certification standards and anticipating new generations of attacks.

SEAL SQ products are compliant with the most demanding certification bodies in the world: Common Criteria EAL5+ and FIPS 140-2 level 3.

NEOWAVE WINKEO FIDO2 USB KEY FEATURES AND ADVANTAGES

Winkeo FIDO2 key, a high level of quality for an optimal security

- **Effective against phishing**
  - **Based on the FIDO protocol (FIDO2 and FIDO U2F).** The private key never leaves the Winkeo FIDO2 device. Logging in to your account is impossible without the security key
  - A security key based on **digital certificates**
- **Authentication (MFA and strong) easy to deploy**
  - Improved user experience as no software installation is required
  - For all types of terminals with USB-A interface
  - A competitive price and a lower cost deployment (no support required such as a smartphone for example)

CYBERSECURITY™
MADE IN EUROPE

- **100% designed and manufactured in France**
  (manufacturing, assembly and customization)
  - No back door / no compromise on security
  - Optimal architectures (single-chip…)
  - Product designed for French / European manufacturing
  - Customizable, unique numbers, logos…
  - Reduction of the carbon footprint
  - Quality and proximity of technical support
  - Agility of an SME with the skills of a large group
- **Very high level of certification and qualification**
  - Components certified common criteria EAL5+ by the ANSSI
  - « Cybersecurity Made in Europe » Label
  - ANSSI certifications / qualifications