entersekt
and you're in.

The ultimate guide to **FIDO**.

Your ultimate guide to improving digital security with FIDO. FIDO harnesses technology to improve security and eliminate ineffective passwords through strong authentication.

Powered by Entersekt

Table of **contents**

The problem with passwords.

$2,9 million

What cybercrime cost the global economy in 2020, every minute.

80%

The number of these cyberattacks that were password releated.

01 The problem with passwords

Large businesses are allocating close to **50% of IT help desk expenditure** towards password resets, with the average annual staffing expenditure for this assistance totaling over $1 million. Evidently, passwords are not only ineffective; they also actively cost businesses a lot of money—and individuals plenty of headaches.

> In 2020, cybercrime cost the global economy **$2.9 million every minute.** Of these, **80% were password related.**

Although password security has always been a problem, recent changes in work models have seen IT teams reshuffling their priorities at short notice. Systems have to keep running and employees need to stay connected, wherever they are. Considering the expansion of remote work, the playing field for hackers has only widened.

FBI statistics **reveal a fourfold increase** in cybersecurity-related complaints since the beginning of the COVID-19 pandemic.

Passwords prove to be less effective and more costly

Besides passwords proving less effective, more costly, and time-consuming, they are also a personal frustration for many individuals. Remembering countless codes, forgetting them, and resetting them eats up valuable time that one could direct to more useful activities. Good security habits are often neglected for the benefit of convenience. To secure sensitive data and avoid violations, awareness and resilience are imperative.

With the increase in cyberattacks during the COVID-19 pandemic, passwordless authentication needs to take center stage. While a concern before, the entirely online nature of modern work necessitates more stringent (and simpler) digital security measures. The aim of the passwordless future is to make security cost-efficient, less time-consuming, and convenient for users. Offering clients and employees the assurance of better information security boosts trust while minimizing loss.

In comes FIDO. **Fast Identity Online (FIDO)** measures harness technology to improve security and eliminate ineffective passwords through strong authentication. Streamlining access while boosting security, FIDO is the future of digital safety technology.

What is **FIDO?**

Fast Identity Online, commonly referred to as FIDO, is a technical specification for digital identity authentication.

02 What is FIDO?

Logins that require users and software to know correct codes and passwords necessarily encourage an exchange of sensitive information. Even if you can keep your password a secret, a hacker can coax the software into giving up your information.

Meanwhile, FIDO implements cryptographic credentials as multi-factor measures to improve security.

> FIDO simplifies verification while improving security.

FIDO simplifies verification while improving security. This is why many major device manufacturers (including Apple, Huawei, and Windows) have integrated this verification solution into their platforms.

How does FIDO work?

As opposed to passwords that entail symmetric cryptography, FIDO applies an asymmetric method. Symmetric encryption uses a single shared secret to communicate encrypted data between parties. Asymmetric cryptography instead allows the user to create a public and a private key. Once the user confirms they have the first key (swiping a finger or entering a PIN), a challenge or puzzle based on the key is generated for the login attempt. Only the holder of the private key will be able to solve the puzzle—yet solving it won't give away the key.

Since the challenge only serves that login attempt specifically, the same solution can't work repeatedly, or across different services. The user, therefore, is the only one that can solve the puzzle or challenge.

Asymmetric cryptography minimizes the use of passwords and reduces the risk of weak password security. The same username can be used across multiple logins without posing a security threat since challenge questions are uniquely generated for every sign-in. Unlike a password, the private key is never actually transferred over the internet, which makes digital theft much more difficult.

What is FIDO2?

FIDO2 is a continuation of the work done by the FIDO Alliance's initial efforts to facilitate a passwordless authentication system.

03 What is FIDO2?

Where FIDO mainly focused on integrating second-factor authentication, FIDO2 aims to eliminate password use entirely over the internet, allowing users to use common devices to authenticate to online services on mobile or desktop.

FIDO2 was designed to present license-free standards for secure, global internet authentication.

FIDO2 aims to eliminate password use entirely over the internet, allowing users to use common devices to authenticate to online services on mobile or desktop.

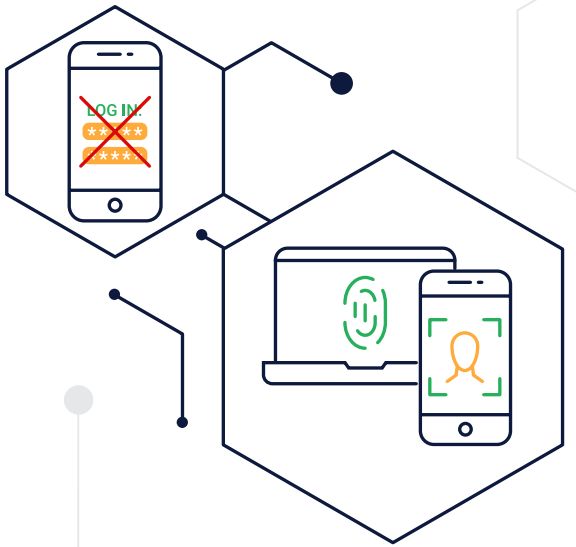
Since it eliminates the use of passwords as a security model, it also eliminates the traditional threats associated with the username and password logins such as phishing and man-in-the-middle cyberattacks.

How does FIDO2 work?

With FIDO2 authentication, biometric readers and cryptographic hardware elements are embedded in a laptop, smartphone, or tablet device. This includes touch, voice, or face ID recognition. Cross-platform authenticators may also require the insertion or pairing of a physical USB or Bluetooth security key.

FIDO2 authentication minimizes the attack window for cybercriminals, naturally eliminating the possibility of phishing schemes and password theft. This process renders OTP codes obsolete—therefore, attackers cannot persuade victims to share this sensitive information. A fraudster cannot install malware through fraudulent links, since **FIDO-enabled tools** only work with URLs that the user personally registers.

In addition, it creates a streamlined experience, since one does not have to remember different passwords and login details for every site, balancing security, convenience, and privacy.



Who is the **FIDO Alliance?**

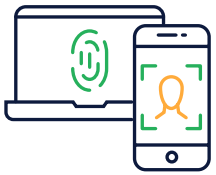
The **FIDO Alliance** is an open industry body aiming to reduce global reliance on passwords by developing verification standards, compliance, and smarter device authentication.

04 Who is the FIDO Alliance?

The alliance aims to develop and promote authentication models that offer stronger security than passwords and one-time PINS, are simple to use, and are easier to manage.

Despite the consensus that password use needs curtailing, online service providers are hesitant to outlay the cost and deal with the complexities of transitioning to a new model. Additionally, consumers have not had a great user experience with past systems, making them hesitant to adopt new methods.

The FIDO Alliance operates industry certification programs and provides technical specifications and formal standardization for biometric components. The alliance also works to define scalable mechanisms for stronger authentication, eliminating password reliance.



1. FIDO authentication

2. Identity verification and binding

3. The Internet of Things (IoT)

Learn more about the **FIDO Alliance's** three focus areas on **page 15**.

05 FIDO's[1] development over the years

July 2012
The FIDO Alliance is founded.

February 2013
The Alliance launches publicly.

April 2013
Google, Yubico and NXP join the Alliance and bring with them the idea of an open, second factor authentication protocol.

February 2014
PayPal and Samsung collaborate for the first deployment of FIDO authentication.

December 2014
The completed v1.0 passwordless protocol and the second-factor protocol are completed and published.

February 2015
Microsoft announces it would support FIDO authentication in Windows 10.

May 2015
NTT DOCOMO becomes the first mobile network operator to deploy FIDO Authentication.

June 2015
The Alliance announces support in FIDO 1.0 specifications for contactless transport over Bluetooth and Near Field Communication (NFC).

November 2015
The first FIDO Certified iOS products are announced.

February 2016
The W3C launches a new standards effort in Web Authentication based on the FIDO2 2.0 Web APIs submitted by the FIDO Alliance.

September 2016
Intel, Lenovo, PayPal and Synaptics announce a collaboration to use FIDO standards to web-enable biometric authentication on the desktop.

December 2016
Over the course of 2016, Aetna, BcCard and Feitian join the lineup of FIDO services on the FIDO Board.

January 2017
Facebook announces support for FIDO Authentication.

December 2017
The FIDO Alliance announces updates to the specifications including FIDO UAF 1.1.

January 2018
Amazon joins the FIDO Board.

April 2018
FIDO2 is officially launched.

September 2018
FIDO2 browser support and first certified products are made available to reduce password use on the web.

December 2018
FIDO UAF 1.1 and CTAP are recognized as international standards by the ITU-T.

February 2019
The Samsung Galaxy S10 and S10+ smartphones are the first to achieve certification from the FIDO Alliance's new Biometric Component Certification Program.

February 2019
Android earns FIDO2 Certification.

March 2019
WebAuthn recommendation become an official web standard.

May 2019
Windows Hello earns FIDO2 Certification.

April 2020
Android phones can be used as a 2FA security key.

January 2020
Apple joins the FIDO Board.

May 2020
LoginWithFIDO is launched to educate consumers and service providers on the benefits of FIDO.

June 2020
Apple expands its support for FIDO Authentication in Safari on iOS 14, MacOS Big Sur, and iPadOS 14.

July 2020
Platform and browser support for FIDO Authentication grows to new heights.

April 2021
The German Federal Office for Information Security achieves the Certified Authenticator Level 3+ certification.

May 2022
Apple, Google, and Microsoft commit to expanded support for the FIDO standard.
Read more.

[1] https://fidoalliance.org/overview/history/

What are the FIDO standards, protocols, and specifications?

FIDO authentication technologies are designed to standardize digital access verification by means of mobile phones, computers, or USB devices. FIDO standards and specifications provide high-quality cryptographic assurance that access is verified and secure.

06 What are the FIDO standards, protocols, and specifications?

There are two established FIDO authentication protocols: **Universal Authentication Framework (UAF)** and **Universal Second Factor (U2F)**. UAF enables verification from trusted devices, using a secure password-free and multi-factor experience. The U2F protocol uses second-factor verification in addition to a password.

FIDO2 merges UAF and U2F to offer a truly passwordless experience and provides the option of both built-in and roaming authenticators. FIDO2 protocols involve the World Wide Web Consortium's (W3C) Web Authentication specification and Client-to-Authenticator Protocols (CTAP) working in tandem to eliminate the sharing of login information over the internet.

FIDO2 merges UAF and U2F to offer a truly passwordless experience and provides the option of both built-in and roaming authenticators.

WebAuthn

The Web Authentication (WebAuthn) Application Programming Interface (API) is a specification written by the W3C and FIDO allowing servers to register and verify users with public-key cryptography. This allows servers to integrate with the strong authenticators now built into devices, like Windows Hello or Apple's Touch ID.

A credential, or private-public key pair, is created for a website. The private key is stored on the FIDO authenticator, where it remains secure on the user device or the roaming authenticator. Meanwhile, the public key is stored on the server with a randomly generated credential ID. The server uses the public key to verify the user's identity—this key is not a secret. It does not have to be, since it poses no security threat unless paired with the corresponding private key, which only the user holds. The public key is therefore irrelevant to hackers, and databases storing this information are no longer attractive.

As part of the FIDO2 framework enabling passwordless authentication between servers, browsers, and authenticators, WebAuthn is supported by over 80% of browsers worldwide, including Edge, Chrome, Firefox, and Safari.

Client-to-Authenticator Protocol

The Client-to-Authenticator Protocol (CTAP) facilitates communication between an external authenticator, such as a mobile phone or laptop, and a browser (client) or operating system platform.

The flow of communication involves the browser establishing a connection with the authenticator. The browser or application then obtains information regarding the authenticator and its capabilities. It sends a command for an operation that the authenticator supports; the authenticator then responds with relevant data.

FIDO Client-to-Authenticator Protocol 1 is essentially the new name for U2F, as it enables external and portable authenticators to interoperate with a computer or client platform. Client-to-Authenticator Protocol 2, on the other hand, facilitates external security key communication with a website or account. An authenticator that facilitates CTAP2 is called a FIDO2 authenticator or WebAuthn authenticator.

What are the three focus areas of the **FIDO Alliance?**

To achieve better digital and web security, the FIDO Alliance focuses on three key areas: user authentication, identity verification and binding, and the Internet of Things (IoT). Each target addresses aspects of digital identity lifecycle management, from initial account onboarding and recovery to device authentication.

07 What are the three focus areas of the FIDO Alliance?

1. FIDO authentication

For simpler, safer, and easy user authentication, the FIDO Alliance has published clear U2F, UAF, WebAuthn, and CTAP specifications. These technical specifications detail authentication methods that are scalable with various industry and business needs.

They allow systems to safely exchange information with reliable passwordless authentication.

These specifications are continually updated as well, to maintain the most current best practices.

2. Identity verification and binding

Since FIDO Authentication and secure information exchange are largely based on the physical device, account recovery when a device is lost or stolen is critical to safeguarding the user's information. Although fraudsters cannot immediately access the device due to biometric unlocking mechanisms, validating user identity during account onboarding and meeting Know Your Customer (KYC) requirements is essential for account recovery.

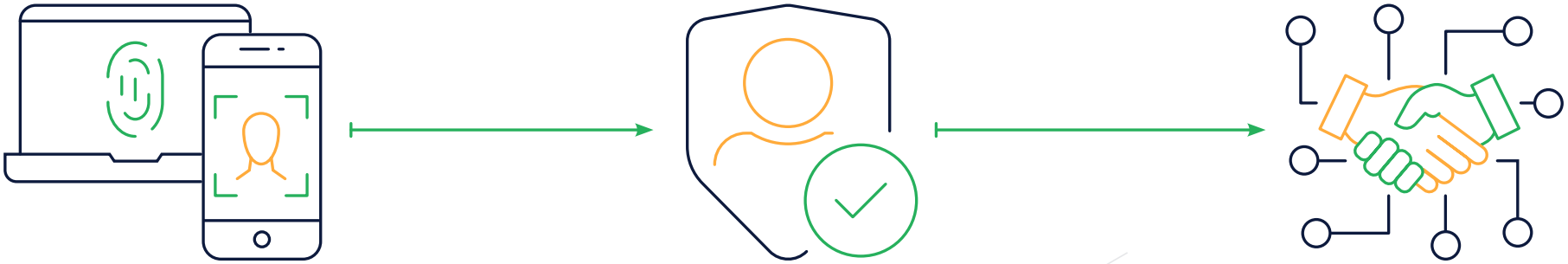
FIDO's Identity Verification and Binding Working Group (IDWG) aims to strengthen identity verification for secure account recovery. Methods of identity assurance for account onboarding and recovery include biometric matching and government-issued IDs.

The alliance has expressed the importance of certification, authoritative guidance, and performance evaluation. The IDWG determines the criteria for remote identity verification and is designing a certification program and educational resources to support criteria adoption.

3. The Internet of Things (IoT)

A lack of IoT security standards, default password settings, outdated processes, and manual onboarding all leave networks and devices open to large-scale cyber threats. The FIDO Alliance has founded the IoT Technical Working Group (IoT TWG) to provide target architectures and specifications for a comprehensive authentication framework to boost passwordless verification.

These specifications include IoT device authentication profiles to allow operations between providers and IoT devices, automated onboarding, binding of applications, as well as IoT device verification via smart routers.



1. FIDO authentication

2. Identity verification and binding

3. The Internet of Things (IoT)

What are the benefits of using **FIDO?**

FIDO replaces outdated, weak methods of authentication with a modern, passwordless option. Balancing security and user experience is a key component of any modern authentication offering.

08 What are the benefits of using FIDO?

> FIDO aims to improve digital security while also enhancing safe and user-friendly recovery options.

FIDO authentication achieves this by providing a high level of security based on public-key cryptography, eliminating the need for passwords and OTPs. This translates to a better user experience, with less friction.

Great security

Universal 2nd Factor (U2F) authentication and multi-factor authentication measures are impervious to interception or redirection. In addition, USB or NFC (near-field communication) devices cannot be duplicated, counterfeited, or reverse-engineered. These factors alone are a significant security boost for your operations.

For secure recovery, a number of safe options exist including backup codes and fallback or alternative numbers which can be used as verification if the primary device has been lost.

Ease of use

Besides increased security, ease of use makes for another significant benefit. FIDO enables customers to use their own common devices, by way of biometrics, to authenticate to online services. FIDO cryptographic credentials are unique to every website, never leave the user's device, and never sit stored on a server. As a platform-agnostic solution—it does not require outside apps—FIDO's relative accessibility has led to widespread adoption across platforms, operating systems, browsers, and markets.

PSD2 compliance

FIDO's multi-factor authentication also helps it meet even the most stringent international security regulations. This helps institutions meet PSD2 compliance in the European market (one of the most exacting when it comes to digital security) which requires multi-factor authentication for all transactions underpinned by customer authentication practices.

> FIDO's multi-factor authentication also helps it meet even the most stringent international security regulations.

FIDO applications in different industries.

08 FIDO applications in different industries

Payments and financial services

Besides considering all the logins a single user creates for online shopping, subscriptions, and once-off purchases. Every purchase one makes online seems to require a new account. As such, users wind up overwhelmed, and default to password-recycling. And not only are these accounts not secure; they also hold credit card details and personal data, left floating through cyberspace despite only being used once… five years ago.

With millions of accounts hacked and hijacked, more internet services—especially financial institutions—realize the need to move away from passwords. New user-friendly, scalable, and future-proof ways to verify clients are in demand.

> With millions of accounts hacked and hijacked, more internet services—especially financial institutions—realize the need to move away from passwords.

Financial institutions and banks have seen a large shift away from physical banking and branch services toward online and mobile transactions. Fast access and convenience have, however, come at a trade-off for security and robust authentication.
For exactly this reason FIDO specifications focus on boosting security in a way that also improves user experience.

Considering the astronomical costs associated with online fraud and cyberattacks, there is little question as to increased banking security's priority. Providing stronger user security will inevitably reduce enterprise losses.

FIDO's passwordless authentication model can integrate into online banking, payments, transfers, trading, and mobile banking. Entersekt is a sponsor member of the FIDO Alliance that developed and offers one of the first global FIDO-certified servers for e-commerce payment transaction authentication.

Universal Second Factor allows online banking services to verify safer logins with a strong second factor by means of the user's mobile phone. Integrating a secure second factor allows a 4-digit PIN to take the place of a complex password, without risking security breaches.

Further FIDO security models integrate a single gesture to log on to a device or account, reducing the necessity of remembering and re-creating complex passwords. Users can perform the same authentication method across various services, making access fast, convenient, and secure. The security key stays on the device with no tracking ability between services or accounts. With no online passwords to steal, replay attacks, phishing, and man-in-the-middle cyberthreats are minimized.

Biometric authentication

Biometric authentication also means that no third parties find themselves involved in protocols.

> With no online passwords to steal, replay attacks, phishing, and man-in-the-middle cyberthreats are minimized.

As biometric authentication is device-specific and user-specific, banks and financial institutions see significantly reduced development and maintenance costs. There is also a reduction in the time and labor dedicated to password resets and accidental account blocks due to incorrect login details. Enhanced futureproofing also reduces expenditure on future system transitions and upgrades.

FIDO decreases the risk of breaches, reduces losses and service costs, and increases client security and satisfaction. Considering all of this, financial institutions can seriously benefit from implementing FIDO applications, securing their position as industry leaders.

Healthcare and insurance

When it comes to industries needing to secure personal data, healthcare and insurance are at the top of the list. Advanced digital and data security are the backbones of any competent medical administration system and healthcare unit. This gives medical staff and patients peace of mind knowing that their information is secure with authorities who adhere to accountability standards. FIDO can assist in ensuring that only patients and trusted advisors can access patient details, including payment, medical aid, and personal information and records.

As medical services progress to online and mobile applications, FIDO authentication and identity verification allow public access with a single login. The British National Health Service is a prime example of this integration. The NHS has launched an app for the public to digitally access their health and social care information, as well as a range of services including scheduling medical appointments and requesting repeat prescriptions.

Dealing with highly sensitive information

The nature of this information is not only large-scale but also highly sensitive. Users were initially required to use a two-factor authentication method, together with an OTP. However, the login method proved too cumbersome and resulted in poor adoption of the medical services digital rollout. With password-free FIDO login protocols streamlining access, the NHS launched biometric logins to simplify app use, enhance security, and improve user experience.

Medical staff access, authorization, signatures, claims, and financial data are also a high-security priority. Reduced password reliance makes these services faster, more efficient, and more secure. After all, you can't hack a password to access medical institution data if the password does not exist! Medical institutions comprise a vast range of departments and require significant IT attention. By simplifying secure, passwordless logins, IT departments can gain hours weekly focusing on value-add tasks, rather than troubleshooting password resets. This not only saves time but can also prove a huge financial saving to the institution.

> With password-free FIDO login protocols streamlining access, the NHS launched biometric logins to simplify app use, enhance security, and improve user experience.

Government services

Enabling users to access government services with both government and user security at the forefront is no simple task. The U.S. General Services Administration (GSA) offers public and federal employees an online interface to access services including the federal government's job board and traveler programs. In addition, the platform handles security operations and customer support. Their adoption of FIDO security protocols in the e-service rollout has streamlined secure service access to millions of citizens.

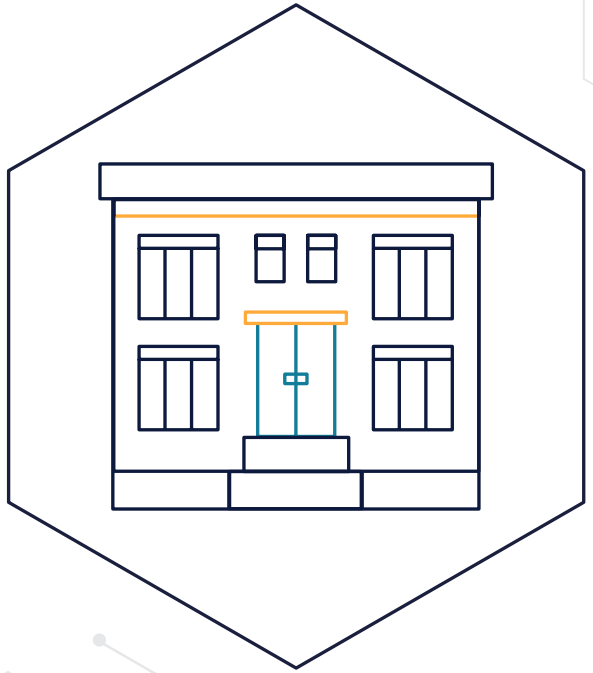
As e-government services develop and become more accessible to the public and federal employees, securing digital access is of paramount priority. Access not only needs to be secure, but also cost-effective, user-friendly, and efficient. Accordingly, USGSA implemented a single platform (login.gov), focusing on providing one protected service for increased security, optimizing account management, and reducing costs.

> As e-government services develop and become more accessible to the public and federal employees, securing digital access is of paramount priority.

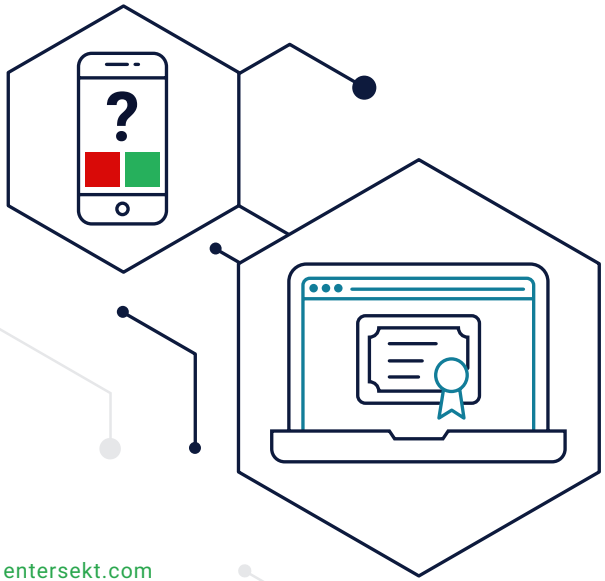
Cyberattacks still happen with SMS one-time passwords

With the rise of phishing and cyberattacks, a strategic and future-proof digital security approach was imperative. Although multi-factor authentication with the integration of SMS one-time passwords seemed a popular option and already familiar to users, it did not eliminate security risks. Involuntarily downloaded malware can easily proliferate on a mobile device, monitoring text messages. Phishing threats within government e-services target accounts controlling identity data, such as birth dates and Social Security numbers.

Login.gov evaluated the FIDO Alliance's FIDO2 standards, concluding that its anti-phishing properties made it most suitable for the government platform's security needs. FIDO2's strong authentication standards enable public and federal users to leverage on-device biometrics and security keys with anti-phishing cryptographic security.



Instead of shared login information and passwords, FIDO2 uses key cryptography techniques to provide increased protection against channel attacks. As much as government information needs securing, FIDO2 protocols provide the same protections for user privacy. These protocols do not provide information that online services can then access to track a user. Biometric security login measures remain device-bound and never transferred over the internet. These factors offer both the user and provider peace of mind with an easy login experience.



Biometric security login measures remain device-bound and never transferred over the internet. These factors offer both the user and provider peace of mind with an easy login experience.

In addition to the heightened security protocols that FIDO2 provides, it also proved a major cost-saver. SMS OTPs can become costly to manage, especially as the number of users continues to increase.

FIDO2 authentication involves a setup phase where users verify their email addresses. After this, they select the multi-factor authentication method that best suits them. This could include SMS OTP, backup codes, FIDO2 security keys, or biometric access. Users can create a security key nickname and must insert the key during setup or respond to the prompt by touching a biometric sensor or looking into a camera. Once complete, the user can then securely use their login.gov account. Multi-factor authentication is saved for up to 30 days on any specific device, meaning that once the user logs in, MFA won't be required again on that device (if the option is selected) until the window expires.

USGSA rolled out these services just over three years ago, to great success. The program quickly picked up momentum, and within less than one year of launch, login.gov was onboarding one million new users monthly. Educating users has also played a large part in government e-services rollout and enhancing user trust.

Telecommunications and mobile services

Although Entersekt does not serve the telecom industry specifically, mobile services such as phone, voice, video, internet, and other communication modes can also benefit from FIDO. Considering the amount of sensitive information transferred, it is important that telecom and mobile services provide high-profile security. Security measures in this sector are not only essential to protect customer information, but also to protect employee and company data. FIDO protocols offer authentication models that are more effective than password logins, based on scalable and open standards.

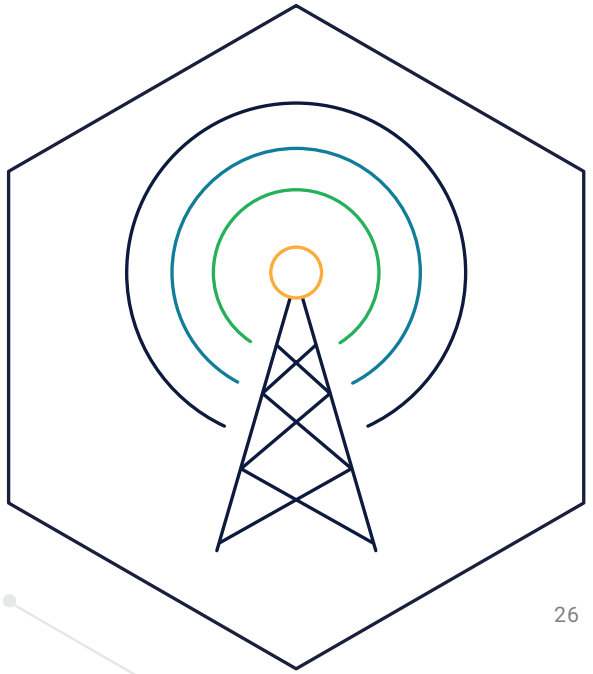
> Security measures in this sector are not only essential to protect customer information, but also to protect employee and company data.

As telecom companies evolve to online and mobile processes, fast and easy access often compromise security. Customers and employees alike can fall into an urgency trap and are consequently less vigilant with security measures. FIDO security and verification features make online and mobile security simple and fast enough not to impose on user experience, while still enhancing data protection and reducing cyber threats.

Most people use the same password for various applications and devices simply because it is less of a hassle. FIDO does away with even having to remember a password. With a single biometric gesture to log on to a device, mobile phone, or company network, safety and speed actually increase in tandem. Consumers and suppliers are more likely to trust said provider or service with their sensitive data. Thus, strong security can boost a brand's reputation in the market and position them as an industry leader, especially in an area highly susceptible to security breaches.

> Strong security can boost a brand's reputation in the market and position them as an industry leader.

Upscaling telecom security with FIDO requires little provisioning costs, and offers a comprehensive choice of authentication for users. It reduces company setbacks, breaches, losses, maintenance costs, and future-proofs telecom offerings.



Enterprise applications

Enterprise data security is often required at different levels and in different scenarios. Access to privileged accounts with high-security needs requires different security characteristics than regular employee user accounts, which may only need medium security authenticators. Enterprises must check that employees have authenticators that meet security verification standards to access highly sensitive resources. Although Entersekt does not involve itself in this market, data security and authentication should be a key concern for any enterprise.

The two main classes of authenticators are bound and roaming authenticators. When evaluating enterprise needs in designing a FIDO verification solution, you should consider both classes to ensure that the enterprise and its employees reap the benefits of enhanced security and exceptional user experience.

Bound authenticators

Bound authenticators, also referred to as platform authenticators, are integrated directly into laptops, smartphones, and other access devices. They include facial and voice recognition, iris scanners, and more commonly fingerprint scanners. These authenticators generally replace password-based verification solutions, offering a simplified user experience.

When adopting these enterprise security measures, a user generates a credential bound to that device. To access the application from a different device, the user must register and generate new authorization. With an increased remote working landscape, this option is ideal to ensure that employees can only access company data in their remote work environment. FIDO UAF and FIDO2 authenticators can serve as bound authenticators.

Roaming authenticators

Unlike bound authenticators, roaming or hardware authenticators exist separately from devices. This includes verification connectors such as USB, NFC, Bluetooth. Roaming authenticators also support 2FA and passwordless models.

One can use a roaming authenticator in addition to a bound authenticator on a device; it need not be either/or. FIDO authenticator applications will generally include some combination of cryptographic functions, biometric matching, key storage, and device verification. In cases where employees bring in their own devices, it is important to vet authenticators before registering them to access company information and data resources.

When integrating authentication solutions, enterprises also must fully comprehend FIDO credential lifecycle management. FIDO authentication protocols are different from traditional OTP and password-based systems. In a FIDO-based system, users may have various authenticators at once (for example, one for a laptop and one for mobile). The lifecycle involves a registration phase, authentication, renewal, and revocation.

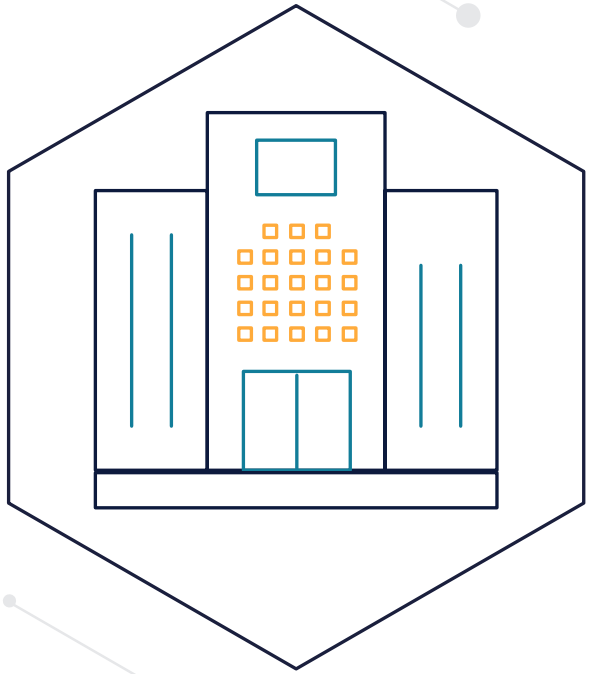
In enterprise security integration, it is also essential to understand the processes for revocation and deletion should there be a security breach, as well as account recovery procedures for lost items.

Companies can make safer payments, risk fewer cyber threats, and implement various levels of security as required by each department.

FIDO perks

Enterprises that employ FIDO security protocols keep company information safe, but the technology offers a range of other perks as well. FIDO can allow customers easier access personal profiles with 2FA. It also offers suppliers a secure way to access the required information. FIDO protects employee and HR information, and substantially reduces IT costs and time spent on password-related help desk tasks.

Companies can make safer payments, risk fewer cyber threats, and implement various levels of security as required by each department.



Entersekt, the future of secure banking and financial services.

Entersekt specializes in secure customer authentication. As an ambassador for streamlined, omnichannel experiences, Entersekt is certified to support FIDO and FIDO2 protocols.

10 Entersekt, the future of secure banking and financial services

With global losses from cybercrime surpassing $1 trillion in 2020, it's evident that passwords are not efficient at keeping data and money safe. It's also no surprise that inefficient management of weak and predictable passwords is the root of 80% of data breaches. OTPs attempt to combat this problem; however, they too run the threat of interception.

> Global losses from cybercrime surpassed $1 trillion in 2020.

Thus, FIDO has come to the forefront as the solution to global over-reliance on password authentication. The FIDO Alliance launched in 2013 and has continually sought to develop better security measures that are both cost-effective and user-friendly. The latest standard, FIDO2, meets the highest levels of security, with both single-factor and multi-factor passwordless authentication as well as biometrics, delegated authentication, and digital identity recovery. FIDO specifications support verification using roaming or platform authenticators, or even a combination of the two.

Entersekt specializes in secure customer authentication. As an ambassador for streamlined, omnichannel experiences, Entersekt is certified to support FIDO and FIDO2 protocols. Entersekt marries patented customer authentication technology with bound and roaming authenticators to deliver features at the forefront of fintech security.

Customers traditionally find step-up verification a hindrance, especially when it takes extra time during their login or payment process. Inconsistency between channels also historically frustrates users as they hop from passwords to cryptic puzzles to biometric access. Poor functionality and the lack of an integrated solution not only detract from the customer experience but slows down the digital team's efforts to streamline cross-channel customer journeys.

Entersekt allows you to offer customers smooth, cross-channel digital experiences while providing a cyber-safe solution with FIDO authentication.

Transform your banking app into a one-touch verification tool, used every day for digital banking, help center communications, online shopping, and more. With Entersekt's patented technology, you can identify your customers' mobile devices and communicate directly via a mutually endorsed, end-to-end encrypted channel.

Who needs more passwords when there are already billions in circulation?

> FIDO has come to the forefront as the solution to global over-reliance on password authentication.

FIDO authentication provides passwordless verification that is effortless to integrate. It eliminates the threat of compromised access and the frustration of remembering and changing passwords. With Entersekt's FIDO2-certified server, your customers can safely and easily verify their identity online without a password. In addition, Entersekt allows you to cater to customers who do not use your app with SMS OTPs, network-initiated USSD, and out-of-band voice calls.

Look after your web security

When it comes to web security, Entersekt's browser authentication solution combines certified digital technology, biometric recognition, and web-based cryptographic technology to create a unique identity. This highly secure browser identifier enables password-free login and a security layer to detect threats.

Entersekt's customer solutions don't only benefit your customers—they can benefit your business as well. Customers who feel confident in the security you provide and empowered by the streamlined technology will opt-in for increased digital services and transactions. Besides this increased revenue, losses will also decline as security improves and successful cyberattacks decrease.

Passwordless logins across browsers and devices minimize the risk of phishing and malware attacks, safeguarding sensitive information. Since Entersekt solutions meet all relevant global regulations, your cybersecurity system also remains compliant when implementing them.

> Transform your banking app into a one-touch verification tool, used every day for digital banking, help center communications, online shopping, and more.

Contact Entersekt today to book a demo and leverage omnichannel customer authentication that enables cross-channel innovation, increases consumer engagement, and reduces costs associated with fraud.

Visit www.entersekt.com

About **Entersekt.**

Entersekt ensures that digital financial transactions are frictionless and secure. The company provides a single cross-channel platform for financial services institutions to meet authentication requirements and optimize user experiences. With a range of options available for deployment and configuration, Entersekt's solutions are fully customizable across all channels and devices. A strong track record of over ten years' working with leading financial services institutions across the US, Europe and Africa, combined with multiple patented security innovations, has established Entersekt as global industry leader in authentication. Backed by companies like Silicon Valley-based Accel-KKR, one of the world's top private equity firms, Entersekt continues to expand its footprint across key regions. For more information, visit entersekt.com.

entersekt

For more information about Entersekt, or to speak to a FIDO expert, please visit www.entersekt.com or email info@entersekt.com.

/Entersekt

@Entersekt

/Entersekt