GlobalDots

Technical Whitepaper

~~Login~~ Unlock: Biometric Passwordless Authentication

with FIDO2 certified WebAuthN

March 2022

Passwords are Obsolete; So is the Concept of Login

In response to recognizable gaps and challenges in modern-day Identity and Access Management (IAM), powerful new capabilities are developed to usher in a new era of increased security and simplified authentication experiences.

Today's latest identity solutions offer seamless passwordless authentication across multiple contexts and channels, all without usernames, passwords, One Time Passwords (OTPs) or any form of shared secret.

This paper explores the technology behind biometric passwordless authentication (FIDO2 webAuthN) and its manifestations in applications and web services at global scale.

> We believe that organizations who seek to level up security, simplicity & speed can greatly benefit from this upcoming passwordless revolution.

A Full-Fledged Identity Crisis

Existing modalities of authentication and expression of digital identity are mired in a complex mix of legacy security platforms, point vendor products, and in-house builds. Many organizations suffer from this outcome as *digital security has evolved through additive countermeasures increasing over time*, with new solutions building on top of one another. This has resulted in three key side effects:

Security stacks have grown more complex and involve more and more moving parts

End users run a gauntlet of security processes that are painful to navigate

Fraudsters enjoy broader success as the efficacy of existing countermeasures devolves

So even with all this investment and development of security systems over many decades, identity and authentication systems are simply harder to run.
They cost more, customers are less happy, and hackers are still succeeding.
Adding new processes on top of old stacks is doing more of the same and expecting a different outcome. A new approach is needed. That new approach is passwordless.

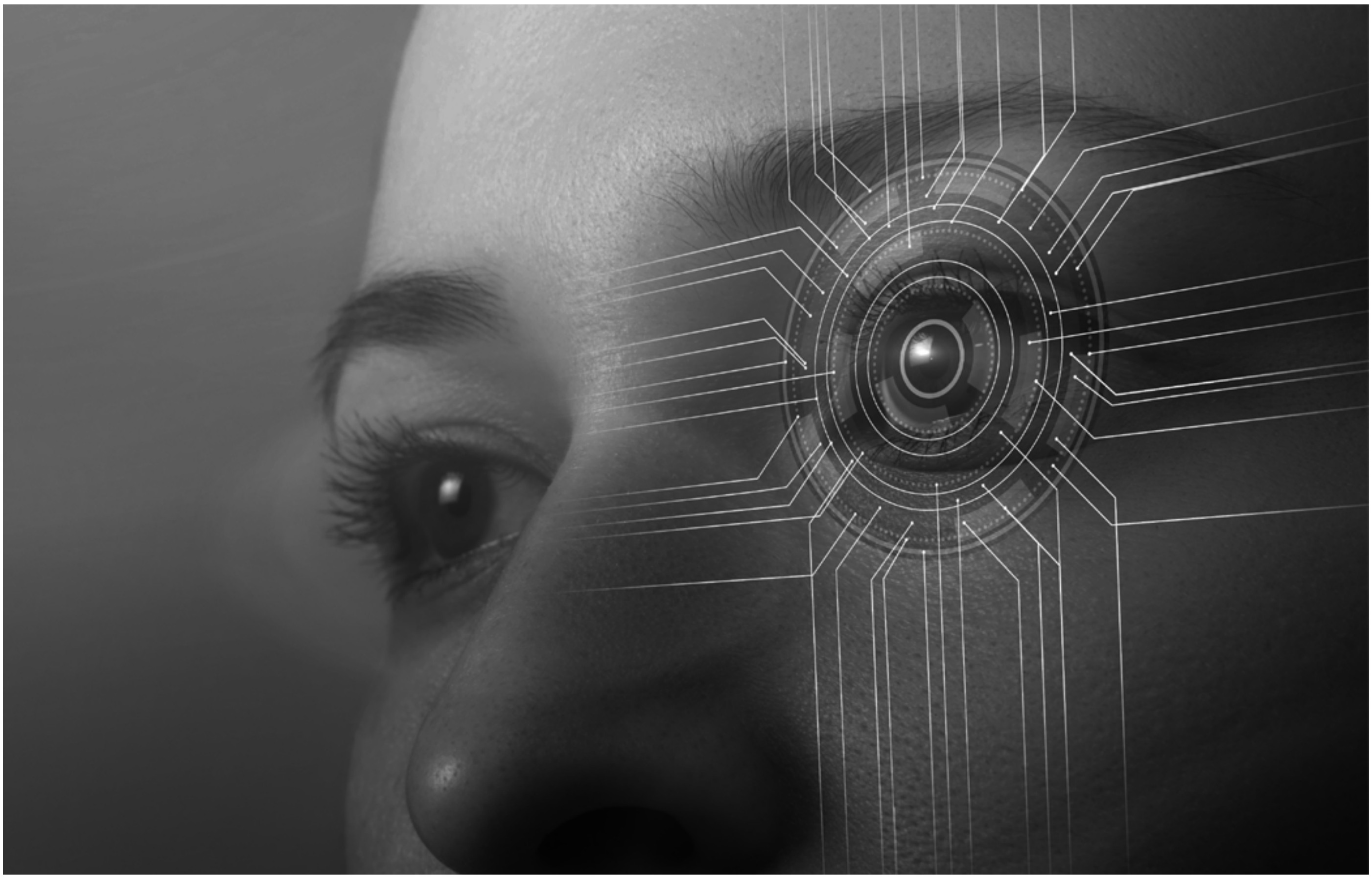
Passwordless: A New Epoch in Digital Security

Passwordless is more than just a new countermeasure. It's a complete side-step from the currently complex trajectory of passwords, PINs and OTPs. It's an entirely new paradigm that turns the usability and security conundrum (where good security comes at the expense of good usability) on its head.

Passwordless is a delight to use, as end users invoke the same biometric processes they normally do whenever they pick their phone or log in to their PC. Strong Multi-Factor Authentication (MFA) is achieved instantly and effortlessly, and with no shared secrets.

With no passwords, there are no passwords that can be leaked or stolen.
Credential stuffing, rainbow tables, keylogging, and replay attacks - all eliminated.
With no OTPs, there are no secrets to intercept. Stolen keyfobs, SIM swap, man-in-the-middlevia SS7 - all eliminated. As a result, hacking and the propensity for account takeover is significantly reduced.The most common and effective hacks are removed from the playing field, giving rise to a superior security posture, and more delightful experience for end users.

Passwordless is simple. Passwordless is secure. Passwordless changes the game.



About Device Biometrics

Device biometrics refer to the biometric readers embedded in endpoint devices. Today's most widespread readers enable face or fingerprint recognition. Both include special hardware and sensors embedded in the device itself.

Face recognition in modern devices works by projecting and analyzing over 30,000 invisible dots to create a depth map of your face and also captures an infrared image of your face. It then transforms the depth map and infrared image into a mathematical representation and compares that representation to the enrolled facial data.

Fingerprint scanning in modern devices uses advanced capacitive touch to capture high resolution images of your fingerprint. The sensor reads fingerprints in 360-degrees of orientation, analyzes the subepidermal layers of the skin and categorizes each fingerprint into arch, loop or whorl categories. It then maps individual details of fingerprint ridges, including variations like pores, and compiles all of the data together. The reader then uses this data to match and recognize fingerprints.

The technologies behind fingerprint scanning and face recognition make them the most accurate authentication technologies on the market today, with extremely low False Acceptance Rates (FAR) and False Rejection Rates (FRR). These low rates are important for both customer experience and security. A low FRR means that the probability of a legitimate user being rejected while trying to authenticate is significantly minimised. A low FAR means that the probability of attackers spoofing the biometric process is also significantly minimised. Due to this unique balance, device biometrics are considered the ultimate authentication solution on the market.

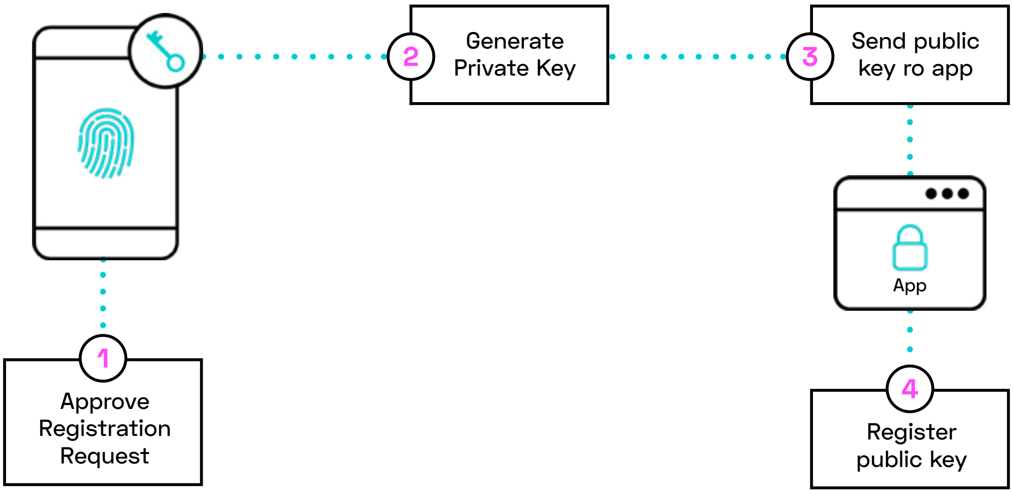
A common misconception about device biometrics is that either the application or the operating system manufacturer (i.e. Apple, Google) keep the user's biometric data, which opens up liability and security risks.

> The way device biometrics work is by keeping a mathematical representation of the user's face or finger on the device itself. This information never leaves the user's device and is never shared with the application or any other service.

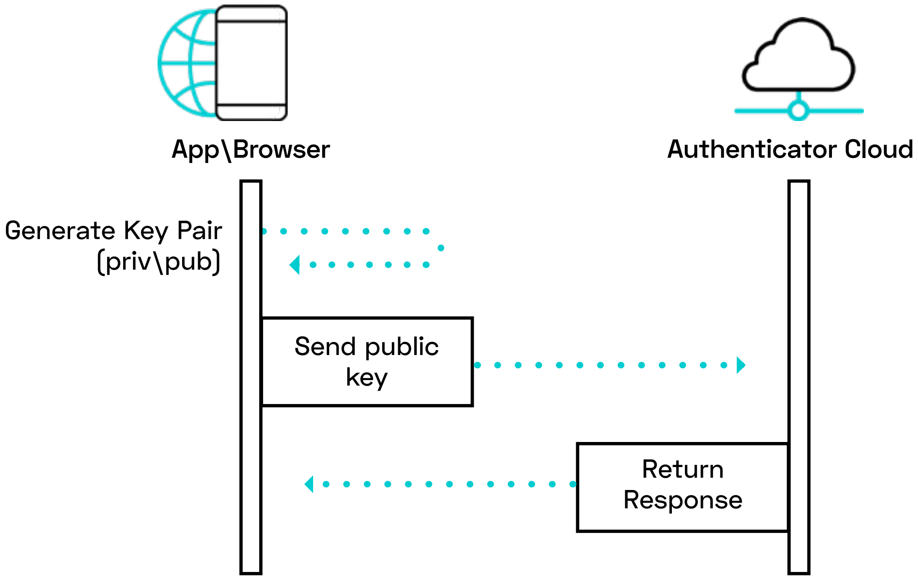
In fact, the device includes a special hardware, usually referred to as a Trusted Environment (or Secure Enclave for Apple devices) which is responsible for storing the information as well as doing the matching between stored information and new face or finger scans. The protocol, which is described in the next section, is responsible for a secure validation of the biometric data without releasing any biometric related data from the trusted environment.

Replacing Passwords with WebAuthN/FIDO

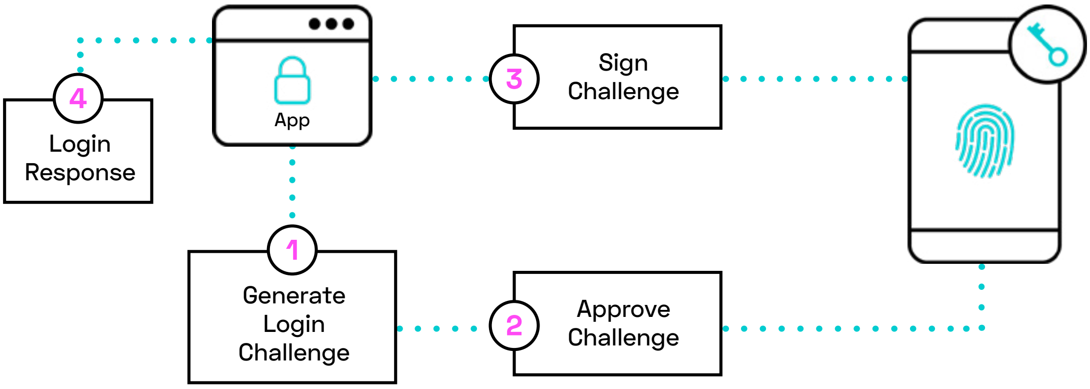
The Web Authentication API (also known as WebAuthN) is a specification written by the Word Wide Web Consortium (W3C) and the FIDO Alliance. The API allows servers to register and authenticate users using public key cryptography (PKI) instead of a password (or shared secret).
A simple explanation of this is described below:



During the registration process, the user's device generates a key pair made up of a public key and a private key. The private key has to remain secret to the user and the device and is therefore stored inside the device's trusted environment and never leaves it (2). The public key, on the other hand, is public and is not considered a secret. During the registration process, the public key is sent to the application server (3) and needs to be kept by the application (4).

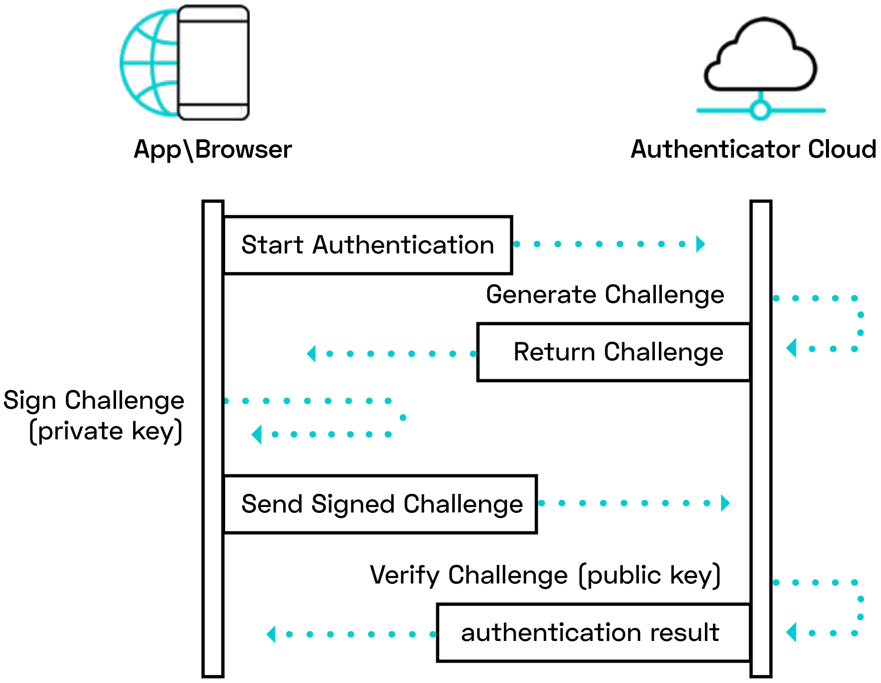


Authentication now leverages the cryptographic security established during registration. With the private key on the device, only the device knows the secret.
A simple explanation of this is described below:



During the authentication process, the application's server creates a challenge, which is a buffer of cryptographically random bytes (1). The challenge is then passed to the trusted environment on the user's device. The trusted environment now invokes the biometric authentication process on the device. The user needs to scan their face or fingerprint and the trusted environment matches the scanned biometrics to the mathematical representation it kept during the biometric enrollment process (2).

If a match is found, the private key is released, and the trusted environment uses the private key to cryptographically sign the challenge it accepted from the application (3). The signed challenge is then passed back to the application server, which now needs to verify it (4). The application server retrieves the matching public key of the user and the device, which it kept during the registration process. If the challenge was signed with the private key that matches the public key then the result of this cryptographic operation will be successful and the application server has now assurance that the user performed a biometric authentication on the registered device, using the registered authenticator.



Securing The Identity Lifecycle

The following processes are managed by the authenticator and require no effort from the application:

1

Registration

2

Authentication

3

Step-up

(or more accurately, why you don't need step-up anymore)

4

Recovery

Registration

A user registered to the authenticator is a user who previously logged into any website orapplication that uses the authenticator. The registration to the authenticator happens automatically during the very first login.
During registration, a the authenticator User ID is generated and at least one of the user's devices are also automatically registered to the authenticator.

The end user doesn't need to remember any username, nor do they need to type a username in when authenticating.

the authenticator will know who the user is by virtue of presenting their biometrics and devices during subsequent authentication phases.
The authenticator User ID is an internal ID and is not exposed to the user, as the user does not need to know or remember any User ID when using the authenticator.

Authentication

1

The authenticator makes authentication very simple to execute. And with so many potential access methods when publishing your application on both the web and mobile, this is logic that you really don't want to have to engineer yourself. By invoking the authenticator, the most appropriate method is handled automatically:

2

User Login From a Registered Device With Biometrics: When the user logs into an application from a device that is already registered to the authenticator, either a face or fingerprint scan is all that it takes to complete the process.

As part of this process, the authenticator can also identify browsers in Incognito (private) mode, browsers who block cookies or when cookies were cleared and automatically recover from these scenarios without asking the user to re-register

3

User Login From an Unregistered Device: When the user is registered to the authenticator but the specific device is not known to the authenticator, the authenticator first offers the user to transfer trust from one of the user's registered devices to this newly unreg istered device. Trust transfer is as easy as scanning a QR code. Depending on the partic ipating devices, one of the devices presents a QR code and the other device scans the QR code using the camera. The user then uses face or finger biometrics on the already registered device to complete the process.

4

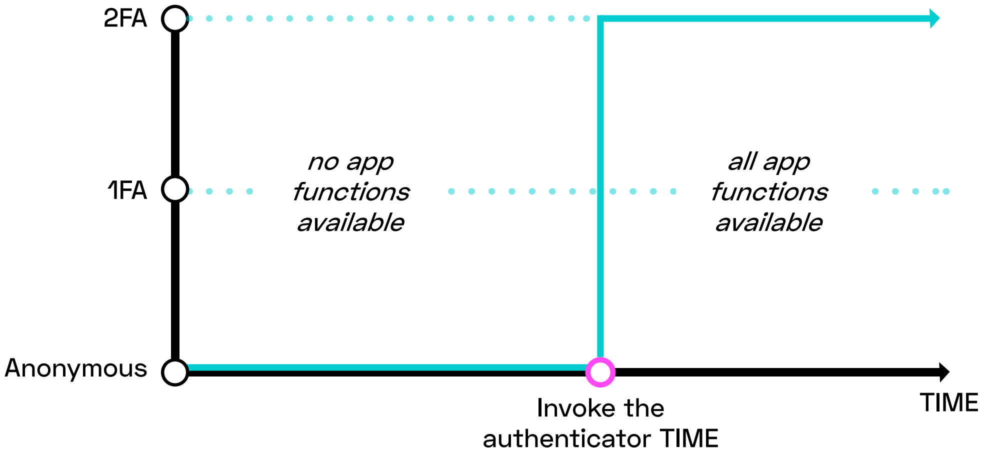
User Login From a Device That Doesn't Support Biometrics: When the user logs into a computer or a tablet that doesn't support biometrics, the user's mobile phone is used as the authenticator. The computer or tablet presents a QR code, the user scans the QR code with their mobile phone and then performs a face or finger scan on the mobile phone to complete the authentication process.

5

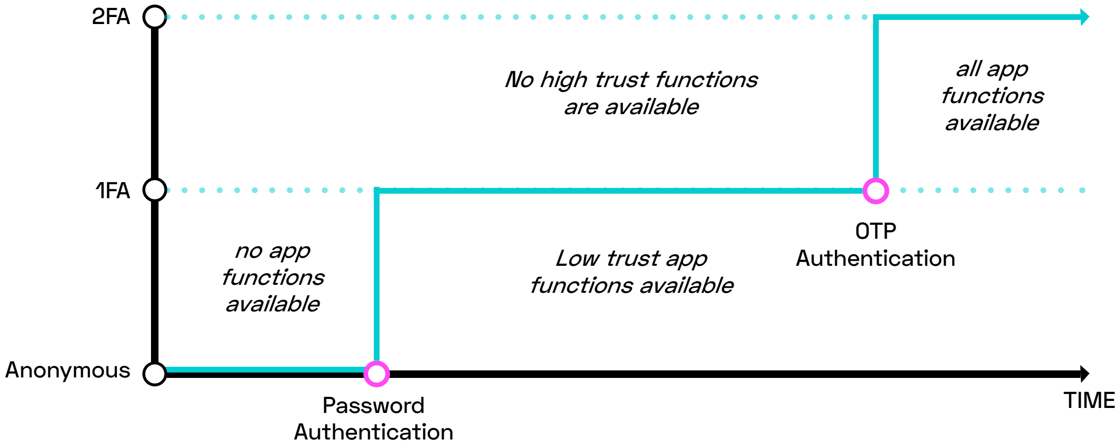
User Login From a Shared Device: When the user logs in using a shared computer, the user's mobile phone is used as the authenticator. The computer or tablet presents a QR code, the user scans the QR code with their mobile phone and then performs a face or finger scan on the mobile phone to complete the authentication process.

Step-Up (Is Dead)

The authenticator achieves “inherent MFA” from the very beginning of an authentication flow, which means that authentication is easy and inherently secure such that full 2FA is achieved with one simple action.


2FA
1FA
Anonymous
no app functions available
all app functions available
Invoke the authenticator TIME
TIME

This effectively eliminates the need to consider step-up flows in your application. Stepup is a historical design pattern that deferred higher security postures in order to avoid having to do 2FA until it was actually needed. This was necessary in order to limit the negative UX/CX that a customer had to endure because 2FA step-ups are usually more painful. For example, a customer might be forced to get an OTP code from a token or wait for an SMS OTP to come through that has to be manually typed into an application.


2FA
1FA
Anonymous
No high trust functions are available
all app functions available
no app functions available
Low trust app functions available
OTP Authentication
Password Authentication
TIME

With the authenticator providing a full 2FA/MFA outcome with one very simple action at the beginning, the need to even do a step-up is now removed.

An application may from time to time require a user to re-authenticate, but this would effectively invoke a simple biometric as and when needed, also providing a high level of security with very low friction. There is no complicated process or hoops a user needs to jump through, and there is a significantly reduced need to map your application to understand when and where you would normally invoke an older style “step-up” process.

Account Recovery

Account recovery happens when the user is coming from a new device and has no devices to transfer trust from. This is a unique and uncommon scenario and can happen, for example, when the user only had one device to begin with and has now switched to a new device and no longer has access to the previous device.

The authenticator does not rely on knowledge-based factors such as passwords or questions for the recovery. These are considered weak factors that can be stolen, and one of the main reasons organizations move to passwordless biometric technology. If recovery is done using knowledge factors, then cyber criminals could exploit this to steal credentials and register devices on behalf of users.

One of the key benefits of the authenticator is the self-service experience it provides to the end user, which reduces the TCO and specifically the cost on the IT teams. One of the key areas where this is important is Account Recovery, which, if not handled properly, translates into high IT costs. For secure account recovery, the authenticator offers the following options, which are configured per application:

Recovery using a trusted device

During registration, the authenticator would ask the user to provide a trusted person's mobile number for recovery purposes. During recovery, the trusted device would get a notification. In addition to this recovery number, the user will also be asked to validate their email address.

Recovery using email and mobile phone number

In this option, the user receives a one-time code via their email address and optionally also on their mobile phone. The user needs to enter the codes to complete the recovery process.

Recovery using email and mobile phone number + Service Provider rebinding

If the Service Provider requires higher assurance than an email OTP, they can take the user through additional steps and checks after the user completes the flow described in (2).

Recovery using an Identity Card

In this option the user is required to scan a government-issued identity card, e.g. driver's license. The authenticator validates the information from the card, while emailing the user a one-time code validation code.

Prerequisite

There are a few things an application needs to manage with FIDO2 WebAuthN:

1

Each of the user's devices needs to register separately. All public keys from all devices need to be stored & associated with the user's identity

2

With WebAuthN FIDO, key pairs are generated on a per-browser / URL domain namespace, meaning registered key pairs across numerous apps and browsers multiply quite rapidly

3

During authentication, the application needs to identify whether the device is already registered to WebAuthN, and invoke registration or authentication accordingly

The basic layer of the authenticator provides a complete, fully certified FIDO2 WebAuthN registration and authentication capability. ***The authenticator completely offloads any WebAuthN considerations from the application***, including the management of any number of registered key pairs, regardless of the device hardware, OS, browser or app.
The application simply calls the authenticator, which performs all WebAuthN-related tasks and returns the user's verified identity back to the application. Application developers are not required to be familiar with the specifics of WebAuthN and can completely rely on the authenticator to perform this for them.

Implementing Passwordless Authentication in Your Web Applications Today

Passwordless technologies are quickly evolving, with FIDO2 WebAuthN spearheading this exciting realm as of 2022. While this biometric option is a great fit for many use cases, its device prerequisites may deem it impractical in others.

In addition, an effective passwordless solution must be chosen and configured in the wider context of the organizational security architecture.

GlobalDots is a world leader in implementing holistic, innovative Security & IT ecosystems, with a portfolio of over 80 security & performance technologies and a team of seasoned solution architects. Our passwordless portfolio includes several technologies and a wide array of customization options, to harmonize with every ecosystem, use case and budget.

Contact us today for commitment-free consultation regarding the best Passwordless path for your organization

GlobalDots Your Tech Innovation Partner

GlobalDots is a world leader in discovering and implementing cloud & web innovation. Over the last 17 years, GlobalDots enabled streamlining and smart growth in over 500 business customers, providing enterprise-grade web performance & CDN; Web Security & anti-fraud solutions; DevOps & Cloud services; Cloud Security; Corporate IT; Cloud-native networking and infrastructure.

Our vendors range from world leaders to innovative, cutting-edge startups.

Our seasoned engineers test & master each solution's capabilities, pros, cons, and best practices. This allows them to quickly spot your perfect fit of technology and enable fast, smooth adoption.

What makes GlobalDots the best choice for a technology partner?

Innovation Hunters

Constantly tracking the industry to provide spot-on solutions for your ecosystem.

Vendor-Agnostic

Our ever-evolving portfolio and customizable solutions cater for each unique use case.

Streamlining Technology Adoption

Breezing you through from selection to deployment, exhausting every feature to your business benefit.

Holistic, Business-Oriented Approach

We align your IT architecture with your business profile, use case and goals focusing on what matters in terms of complexity and financial impact.

Do you want to know more?

Contact Us