Evidian

FIDO Authentication in DirX Access

Enables enterprises to face contemporary cybersecurity threats and enhance their security

The recent, rapid rise of data breaches and sophisticated cyberattacks has exposed the current state of security information technology systems, forcing system providers to search for an innovative and more secure authentication mechanism.

Standards issued by the Fast Identity Online (FIDO) Alliance represent the next generation in authentication technologies by addressing the general need for stronger authentication.

These technologies mitigate the issues connected with legacy authentication methods and stand up to contemporary cyberthreats by shifting the authentication model from traditional password-based authentication to easy-to-use multi-factor authentication.

DirX Access, part of Atos' DirX product suite, is a comprehensive solution for authentication and authorization for identity federation. Beginning with version 8.7, DirX Access has been extended with FIDO-based authentication mechanisms.

Motivation

There is a good reason for this authentication model shift in modern enterprise applications: passwords have been one of the weakest links in IT security for a long time. Generally, stolen credentials and phishing take up the first slots of the top 20 actions in breaches. Passwords are clumsy, hard to remember and need to be changed all the time. As recognition technologies are introduced, the use of passwords and tokens in medium-risk use cases will drop, encouraging companies to look for products that focus on developing an environment of continuous trust with a good user experience.

FIDO standards concentrate on improving the major aspects of mature security-related solutions: strong security, better user experience, and reduced costs. The security aspect is achieved (among other things) by employing public key cryptography, while the user experience and cost-effectiveness of the solution stem from using FIDO authenticators, which typically use different factors of user authentication such as hardware tokens (something you have) or biometrics (something you are). Issued by the FIDO Alliance, the overall solution has strong support from major market players, including Google, Intel, Lenovo, MasterCard, Microsoft, and PayPal.

DirX Access incorporates a FIDO server implementation that supports all of the FIDO-based standards: Universal Authentication Framework (UAF), Universal Second Factor (U2F), and W3C Web Authentication. As a result, it can address any customer's infrastructure parameters and provides for easy integration with other enterprise systems. DirX Access integrates the FIDO-based authentication internally with its other product features, such as single sign-on, identity federation, and risk-based authentication. Support for a wide range of other authentication methods and high configurability makes DirX Access a mature solution that can be successfully deployed in a variety of demanding scenarios.

This paper provides a brief introduction to the FIDO-based standards (in the section "What is FIDO?") and their benefits (in the section "Benefits"). The section "FIDO-based Authentication with DirX Access" describes how DirX Access integrates the FIDO standards into its rich and extensive feature set.

What is FIDO?

The FIDO Alliance was formed in 2012 as a response to the need for better and stronger authentication methods. Its mission is to change the nature of online authentication by developing technical specifications that define an open, scalable and interoperable set of mechanisms that reduce the reliance on passwords. FIDO standards define both the authentication protocols and the (security) requirements for the infrastructure in which these protocols operate.

Benefits

The main ideas behind FIDO are ease of use, privacy, security and standardization. Thanks to its design, FIDO brings a number of benefits into the world of authentication mechanisms:

- End users benefit from improved user experience.
- Enterprises and organizations benefit from stronger security and reduced costs.

Improved User Experience

No need to remember passwords

This primary security vulnerability can finally be removed from the authentication process.

Simple action to sign in

To perform local authentication on a device, a user can simply swipe a finger, look into the camera, plug in a USB stick, or similar.

Transferable user experience

The same authenticator device can be securely used for multiple services, providing a consistent user experience across multiple services.

Fast and convenient

The nature of FIDO enables authentication methods that are faster and more convenient than contemporary strong authentication methods to be brought to market. For example, compare a PIN-based FIDO authenticator to the OTP method: in the former case, the challenge is hidden from the user; in the latter case, the user needs to process it manually.

Biometrics, if used, never leave the device

Biometrics used during the authentication process are stored on the user's device, typically in a secure storage. The user's biometric data are only compared in the FIDO authenticator; the proof of identity is then communicated to the requesting third party using public key cryptography. This approach has two beneficial consequences: the user does not need to worry about identity theft, and the FIDO server provider does not need to worry about the credentials theft in the sense that they do not contain any personal data.

Stronger Security

Identity cannot be stolen

Identity cannot be stolen when server-side credentials are stolen.

The relying party stores only the public key part of each related FIDO credential. This part does not provide the attacker with any means of impersonating the user.

Client-side credentials cannot be stolen

FIDO's intention is to leverage authenticators capable of storing user credentials (private key) in a hardware-backed trusted environment such as Trusted Platform Module, Trusted Execution Environments or Secure Elements. These environments ensure that even if the attacker steals the device, the stored credentials are prevented from abuse. Specific authentication methods (such as biometrics) keep credentials from being stolen and also prevent the attacker from using the authenticator.

Protection against phishing, man-in-the-middle and replay attacks

The challenge-response aspect of the protocol in connection with the public key cryptography protects against phishing and replay attacks. Each protocol run is bound to a (server) origin and a (communication) channel which allows the server to detect MITM attacks.

Services and accounts cannot be linked

The authenticator produces a unique key pair for each server; as a result, even if an entity possesses all the public keys from multiple servers, it cannot link these public keys to a single user.

Reduced Costs

Little or no provisioning costs

Provisioning system users with a new kind of authentication selection typically involves completing two tasks: procuring a (hardware) authenticator for each user and registering related credentials at the server side. FIDO decreases costs in both of these cases: the former with the possibility to reuse a user's personal authenticator (BYOD) and the latter with the enablement of auto-registration – users can typically use self-service credential management portals.

Lower breach risks and potential damages

The protocol design itself mitigates the costs connected with attack damages by solely preventing the possibility of an attack or by allowing an inexpensive remedy process.

Broad choice of authenticators for users

FIDO standardization allows vendors to offer a wide variety of authenticators, both embedded and pluggable.

FIDO Infrastructure

To enable FIDO-based authentication, two components are necessary: a FIDO authenticator connected to or built into a client device possessed by the user to be authenticated, and a FIDO server that provides the authenticated state to the application it protects.

Although it is solely under the user's control, the FIDO authenticator that provides proof of the user's identity is trusted by the server side. This relationship stems from employment of the authenticator attestation, one of the main principles on which FIDO is built.

The FIDO infrastructure can consist of components manufactured by different vendors whose cooperation is ensured by the interoperability aspects of the issued standards.

FIDO Protocols

Topologically, FIDO-based protocols belong to a group of protocols based on the challenge-response model. This model ensures that each protocol run differs sufficiently from all the other runs. Asymmetric (public key) cryptography serves as the identity proof-providing mechanism.

Typically, the protocols from the FIDO suite enable the following actions:

Registration

The registration process enrolls a new FIDO credential (public and private key) binding an authenticator held by the user with the user's account at the server side. It enables easy and cost-free user credentials provisioning.

Authentication

Authentication via the FIDO protocol is, from the user's perspective, a simple and transparent task leading to a state in which the server side obtains the user's identity.

Transaction Confirmation

An extension to the authentication action provided by the FIDO UAF is represented by a transaction confirmation use case. When dealing with sensitive transactions (like banking), the transaction data can be bound to a FIDO authentication request and subsequently credibly displayed to the user. This process makes both sides indisputably aware of the entire action.

Deregistration

To provide the user with complete credential management possibilities, FIDO covers the deregistration protocol flow.

Authentication Flow

Figure 1 depicts the authentication process using the FIDO protocol.

- The user accesses a protected resource (web page, mobile application) and wants to sign in.
- The protected resource informs the FIDO server component of the server-side application, which in turn sends a challenge to the user's device with the built-in/connected FIDO authenticator.
- The authenticator locally verifies the user's identity based on something the user has (a device), something the user is (biometrics, such as fingerprint, iris scan or voice pattern), or something the user knows (a PIN). Any data that originates in the verification process (such as the digitalized fingerprint) do not leave the device. Instead, if successful, the authenticator signs the server-issued challenge with a private key relevant to that given server and user account.
- The signed response is sent back to the FIDO server, which verifies it using the corresponding public key.

Different standards from the FIDO suite focus on different authentication use cases. FIDO UAF, Windows Hello and Web Authentication standards provide a password-free user experience represented predominantly by biometric-based authentication methods (but not limited to them). A second-factor user experience is then provided by FIDO U2F, which enables the addition of the second-factor authentication aspect to the existing infrastructure.

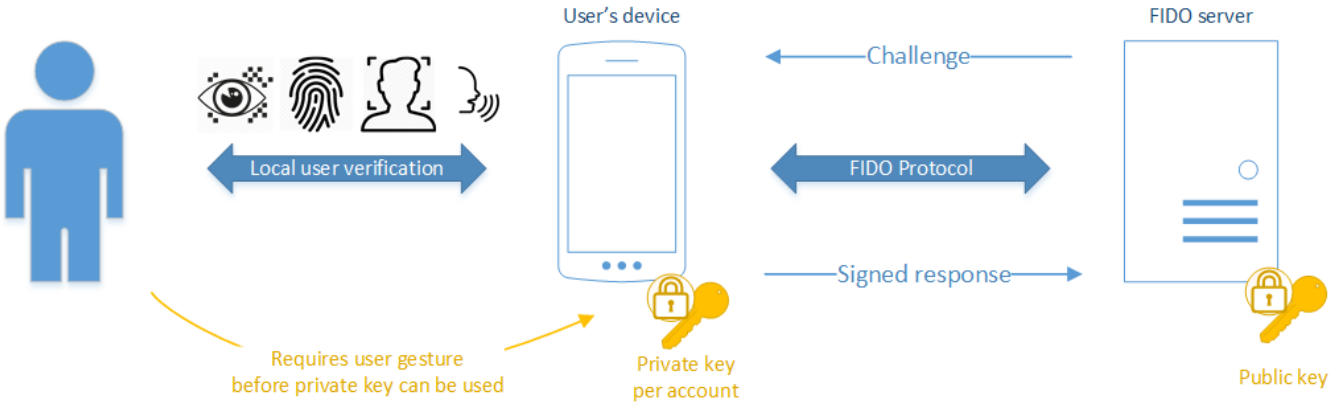

Figure 1: Authentication Flow

FIDO-based Authentication with DirX Access

DirX Access acts as an identity provider to third-party applications, making it the perfect system component to contain a FIDO server implementation. Therefore, its rich suite of supported authentication methods has been extended with all of the currently issued FIDO standards.

Authentication Application

In DirX Access, the authentication methods are typically made accessible through the Authentication Application web application. This deployment-ready application is highly customizable via the standard web technologies to combine the possibility of out-of-box deployment with the ability for adaptation to any customer's requirements. It now provides a front end to FIDO operations and workflows that both enables the authentication process and acts as a self-service credential-management portal providing self-registration/deregistration of FIDO credentials.

Configurability

One of the main principles that DirX Access follows is high configurability. Applying this principle to the FIDO server implementation means that the administrator is able to set up the entire system according to the company's security policies. The configuration allows the administrator to choose which FIDO standards will be supported and in addition allows for the assignment of fine-grained policies to each supported standard.

FIDO UAF defines a vocabulary of FIDO policies that determines the supported authenticators (for example, by exact denomination or according to some authenticator properties). DirX Access extends the employment of this standardized mechanism to all the other FIDO standards. The policies are evaluated against the corresponding authenticator's properties – a metadata statement – that are distributed via the FIDO Alliance metadata service (Figure 2).

This design helps to establish a trust between an authenticator model and DirX Access as the authenticators listed in the metadata service have been certified by the FIDO Alliance. To fulfill the requirements calling for employment of custom authenticators or authenticators which for some reason haven't been certified, DirX Access provides a way to supply custom certificates that enable the use of these authenticators.

The configuration of each respective authentication method is completed by setting up the assurance level parameter. This parameter reflects the administrator's trust in the configured method and helps in defining step-up and risk-based authentication mechanisms.

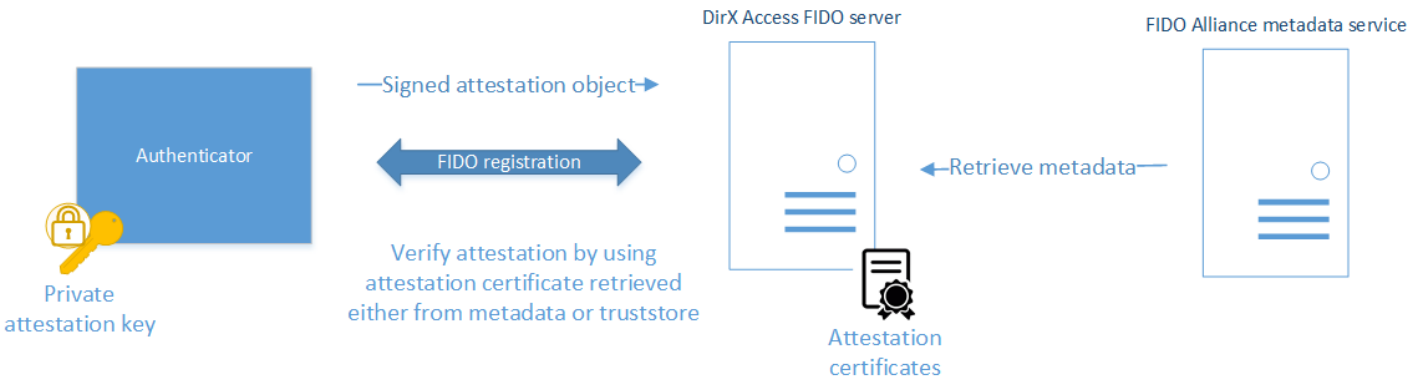

Figure 2: Authenticator Attestation

Integration with Single Sign-on

Single sign-on (SSO) is a property of an access control mechanism ensuring that the sign-on process is performed only once per single session and enabling access to multiple applications typically within the same domain. This property creates a convenient user experience as switching from one application to the next appears to be seamless to the user. DirX Access supports SSO in the web environment, where the FIDO authentication methods can be used during the initial authentication process to harden the security and simplify the process.

Integration with Identity Federation

Identity federation in DirX Access is a process which extends SSO to the multi-domain environment. Identity federation technologies enable authentication and authorization across applications from different domains that share trust with DirX Access. Nowadays, this is the easiest approach to protect online applications and services, as these packages do not need to be altered and need only to communicate via standardized means to an identity provider which informs them about the user's authenticated session. The more secure the authentication process is on the side of the identity provider, the more guarantees can be given to the relying services, which again pinpoints the importance of supporting FIDO standards. As DirX Access supports SAML, OAuth 2.0-based (OpenID Connect, UMA 2.0), and WS-Federation standards, it is a complete tool implementing a strong and reliable identity provider.

Integration with Risk-based and Step-up Authentication

DirX Access was one of the first products to employ the machine learning and pattern recognition techniques in its process of user authentication. Internally called risk-based authentication (sometimes referred to as adaptive authentication), this mechanism assesses risks connected with a real-time context of a user session and compares them with the assurances given by the user, typically the authentication methods already performed. If the risks are too high, the mechanism requires the user to provide stronger proof of its identity to balance the risks. The FIDO server implementation widely extends the range of possible proofs as the FIDO authentication methods provide a high degree of security.

Highlights and Conclusion

By implementing DirX Access, new authentication options based on FIDO2 and W3C standards enable businesses and users to move beyond passwords for stronger, simpler authentication leveraging devices they use every day. Integrated with its other product features, such as single sign-on, identity federation, and risk-based authentication, DirX Access provides a mature solution that can be successfully deployed in demanding access management scenarios in all industries. Security based on FIDO specifications makes online security a simpler and better user experience while providing stronger security and reducing risks for the enterprise.

White Paper

About Atos

Atos is a global leader in digital transformation with over 110,000 employees in 73 countries and annual revenue of over € 11 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education as well as multicultural and pluralistic approaches to research that contribute to scientific and technological excellence. Across the world, the group enables its customers, employees and collaborators, and members of societies at large to live, work and develop sustainably and confidently in the information technology space.

Find out more about us
atos.net
atos.net/careers

Let's start a discussion together

For more information: www.evidian.com/dirx