IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

# Akamai MFA: What's Different Here?

April 01, 2021

By: Jay Bretzmann, Joel Stradling

## IDC's Quick Take

The introduction of Akamai MFA addresses a current gap in the marketplace for advanced authentication, identity security solutions designed for workforce IAM implementations. This new software-as-a-service (SaaS) offering simplifies the adoption of multifactor authentication (MFA) while upgrading previous security key-based technology for Akamai's Enterprise Application Access cloud architecture available through partner agreements.

Akamai MFA adheres to the FIDO2 open authentication standard based upon the W3C WebAuthn JavaScript API that IDC observes to be building momentum among new vendor implementations. It also offers the wildly popular push notification technique for sending server-side challenges to smartphones (and other devices). Developments like this will further reduce the sting associated with adding another layer of protection to the user identification process and help break MFA out of what IDC repeatedly hears to be an approximate 25% adoption rate within workforce identity programs.

## Product Announcement Highlights

On March 17, 2021, Akamai announced a new identity security service aimed at helping organizations defeat one of the most prevalent forms of network security attacks, namely phishing and account takeovers. Akamai MFA is a FIDO2-based multifactor authentication solution that supports the majority of leading identity provider domains (IDPs) and hardware/software authenticator endpoint devices.

The new service introduction augments and uplifts capabilities associated with partner agreements that offered similar security key support and antiphishing identity protections. While the first-generation FIDO U2F protocol was designed to act as a second factor to strengthen existing username/password-based log-in flows, the FIDO2 protocol can also support multifactor authenticators that do not require traditional passwords — inching the market closer to a passwordless future. For all its earlier benefits, the U2F protocol is not compatible with a WebAuthn-only authenticator, and IDC believes FIDO2 requirements will steer and subsume all future authenticator development efforts.

## IDC's Point of View

The development of the JavaScript WebAuthn API was a watershed event for authentication technology when it was approved in late 2015. What this now widely adopted industry standard introduced was the ability to ensure that two parties participating in a challenge-response authentication method didn't change somewhere during the handshaking process. WebAuthn does this by embedding cryptographic client and server credentials along with a public/private PKI key pair into every exchange. Today, it may seem like a somewhat obvious thing to do, but the developers of earlier multifactor authentication technologies (FIDO U2F excepted) didn't all foresee the need, thereby exposing users to so-called man-in-the-middle (MitM) attacks.

A MitM attack is based on the ability of an attacker to fool victims into thinking that they are interacting with a legitimate website or service (relying party in WebAuthn parlance) when in fact they're not. As the user (requestor) logs into the service, they typically disclose a username/password combination. The attacker then uses those credentials to establish separate communications with the real service provider. If a second identity factor is required, the attacker then notifies the oblivious requestor and the real service sends a direct challenge to a pre-registered authenticator completing the identity circle. The attacker is now in control since the service never included user identifying credentials and the browser never included domain name information when communicating with the authenticator.

Recognizing this, a consortium of industry leaders got together to address the problem. The result was WebAuthn combined with Client to Authenticator Protocol (CTAP2) to form the FIDO2 open standard. While WebAuthn handles browser-to-server communications, CTAP2 handles client device to the private/public key producing authenticator. FIDO2 replaced earlier FIDO (Fast Identity Online) open authentication standards with a more mature approach that all major browsers and many forms of authenticators supported building on the basic ability of earlier generation security keys to recognize domain name switches. Security key protection against MitM middle attacks was practically proven by Google years ago when the corporation converted all employee access to its BeyondCorp zero trust networking model. The result? Phishing attacks disappeared.

IDC posits that every organization these days should be using FIDO2-based MFA, but as with so many other aspects of identity security, it's just not that easy to do. There are numerous IDPs holding usernames and organizational affiliations and a slew of platform and cross-platform authenticators supporting a variety of endpoint devices. Some environments prohibit the use of smartphone devices, and others mandate the use of more sophisticated forms of authentication (iris scans, vein patterns, etc.).

Besides, replacing a working identity solution is a perilous task even if it dramatically improves overall security and significantly reduces user friction. FIDO Alliance standards and FIDO2 specifications have been a long time coming. Akamai's adherence to these principles is another step toward a passwordless future, and therefore, Akamai is planting a stake in the ground as an early mover and SaaS innovator leading the charge away from the much unloved username/password access paradigm. IDC believes others will soon follow.

Akamai's MFA stands to differentiate its newly launched authentication service from competing MFA products based on its enormous global CDN footprint and the fact that it has created a FIDO2-based offering. Regarding reach, so what? Well when we dig deeper into the numbers, Akamai's Intelligent Edge consists of 325,000 servers covering 135 countries. This means that scale and low latency (or a fast, resilient, and self-healing internet, to put it another way) are in its DNA, and MFA can be pushed to a very large target market with the ease-of-implementation silver bullet thus complemented by fast service responses.

In Europe, the FIDO2 set of specifications has considerable importance across multiple industry verticals but particularly for banking and finance companies looking to comply with PSD2. The FIDO standard gives a "privacy by design" approach and aligns with key tenets of the GDPR — user authentication (biometric credentials and private cryptographic keys) with personal info processing taking place locally at the user level; there are no centrally created or managed credentials. Improved user authentication

experience while ensuring the highest levels of privacy and security assurance can therefore only be beneficial to industry.

Akamai MFA is designed to be a complete service (MFAaaS) targeted — at least initially — at workforce identity authentications. The company believes it offers the first efficient means for organizations to implement a secure MFA technology upgrade while avoiding both cross-platform authenticator incompatibilities and incremental expenses related to purchasing hardware tokens. Akamai MFA directly connects the server-side challenge in a WebAuthn exchange to a client-side response using a smartphone app serving as a security key. Core capabilities include:

- SaaS deployment model
- Cross-platform, roaming authentication capabilities
- Push notification to smartphone devices
- Support for multiple identity providers including Microsoft Azure, Okta, Akamai IdP, and Shibboleth
- Support for numerous forms of multifactor authentication technologies
- Support for Secure Shell (SSH) and Windows Login use cases

IDC believes this offering will appeal to many organizations that understand the security exposures associated with other, previously developed MFA solutions and those organizations that desire to just outsource the whole secure authentication headache as part of a web-hosting bundle. Akamai MFA represents smart packaging of updated industry standard technology available through a painless delivery model, but the company still recognizes the value of earlier agreements with push technology partners and will continue to support whatever its Intelligent Edge customers require. While pricing details were not readily disclosed, Akamai has stated that it will be on the more generous side of being competitive — at least for the time being.

**Subscriptions Covered:**
European Security Strategies, Identity and Digital Trust Software

Please contact the IDC Hotline at 800.343.4952, ext.7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC or Industry Insights service or for information on additional copies or Web rights. Visit us on the Web at www.idc.com. To view a list of IDC offices worldwide, visit www.idc.com/offices. Copyright 2021 IDC. Reproduction is forbidden unless authorized. All rights reserved.