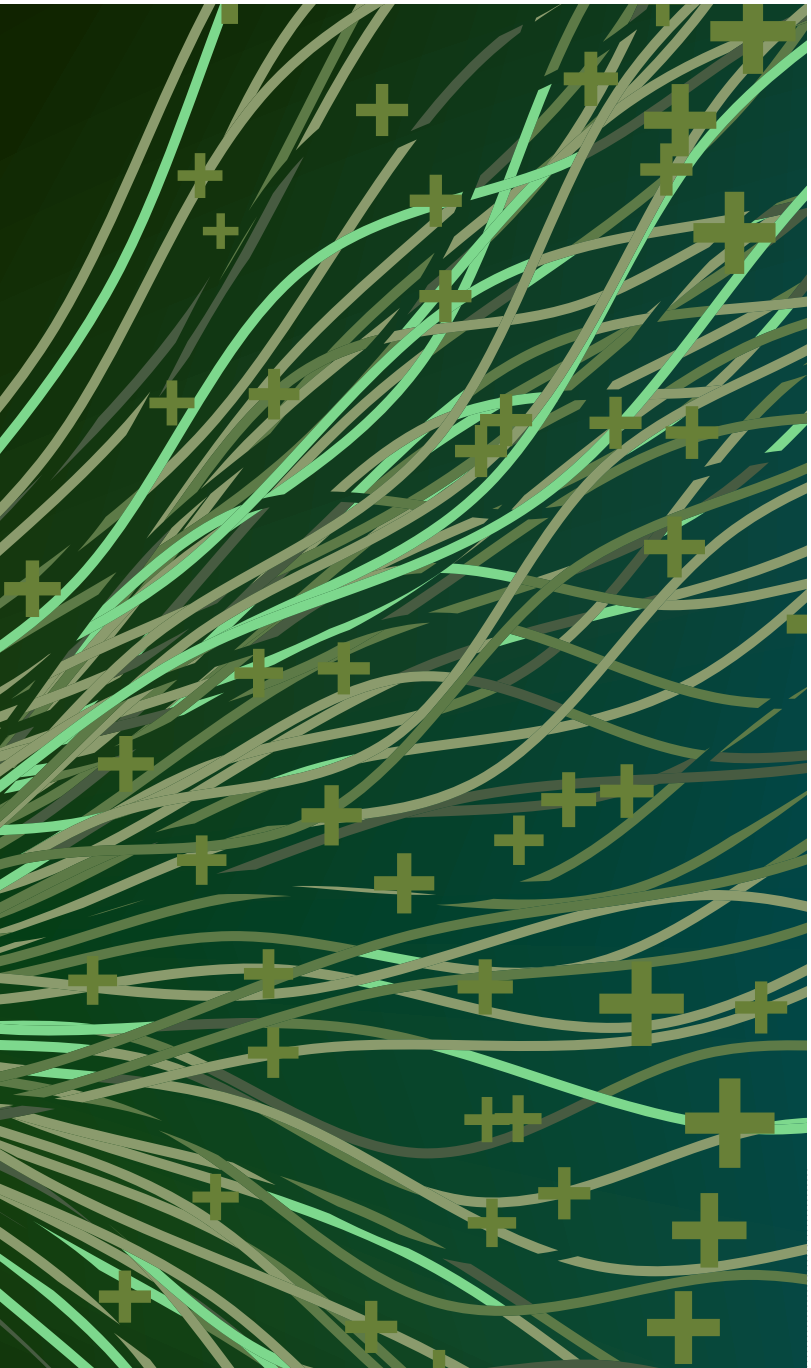
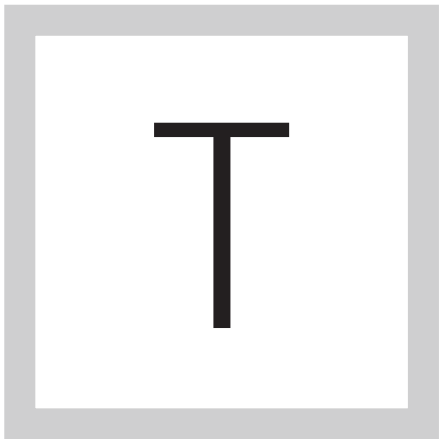


E-Guide

ADOPTING FIDO

TechTarget | SearchSecurity



HE INABILITY OF passwords to keep online accounts secure has been recognized for quite some time, but the IT industry has struggled to establish a practical alternative.

ADOPTING FIDO

Author (optional): Michael Cobb, CISSP-ISSAP

Strong authentication products, long thought to be the solution to single-factor password-based authentication, have been around for years, but are no panacea for preventing the compromise of credentials. Stumbling blocks like cost, lacking interoperability, vendor lock-in and inconvenience to users have hindered adoption to the point where the only industry to use them on any scale is financial services. Not to mention they offer little protection from credential theft via phishing and man-in-the-middle attacks.

Thankfully a long-term solution may be on the horizon, as a consortium of 150 companies called the Fast IDentity Online Alliance, or FIDO, is pushing for the adoption of a new technical specification that aims to make accessing online accounts and services more secure and private while being easier to use than passwords. It is an open and interoperable set of specifications based on standard public-key cryptography.

The FIDO specification is a device-centric model but is not designed for any specific type of authentication technology. It is positioned as complementary to

Home

Adopting FIDO

federation protocols such as OAuth, a token-based authentication technology being used by firms such as Twitter to connect users' accounts to third-party services without obliging them to share their passwords. As cameras, microphones, and fingerprint readers already exist in many mobile devices, biometrics is likely to become the most common method of authenticating users using FIOD, but other options include USB security tokens, TPM, and Near Field Communication chips to support multi-factor authentication.

Enterprises should take this initiative seriously, as it's led by major Internet and technology players such as PayPal, Samsung, Lenovo, Microsoft, Google and MasterCard. PayPal has already implemented secure payments using FIDO authentication, and it's available to users on a range of amsung devices, starting with the Galaxy S5. China's online giant Alibaba has also just endorsed FIDO authentication. Alipay, an Alibaba group company, is also offering secure payments based on FIDO authentication to 600 million users.

FIDO provides two ways to authenticate users: Passwordless UX and Second Factor UX (UX stands for user experience). The registration process for both methods is the same. The user's FIDO-enabled device creates a new key pair, and the public key is shared with the online service and associated with the user's account. The service can then authenticate the user by requesting

Home

Adopting FIDO

the registered device to sign a challenge with the private key. The private key and any information about the authentication method, such as biometric measurements, never leave the user's device, and there is no information given out that can be used by different online services to collaborate and track a user across the Internet, even though the same device can be used for logging in to any number of services.

Using Passwordless UX, a registered user simply repeats the action performed during registration, such as swiping a finger, looking at the camera, or speaking into the mic – no password is needed. Second Factor UX involves using a PIN in conjunction with a USB dongle or an NFC-enabled phone or tablet. Google Chrome is the first Web browser to implement support for Second Factor UX, which means Google can offer an alternative to the one-time passcodes it sends users during the login process. Instead of typing in a six digit passcode, users simply insert a FIDO-compliant USB key into their computer and tap it when asked to do so by the browser.

Even though major enterprises are already up and running with FIDO, the specification is still actively being edited and refined. Nevertheless, large organizations should follow developments closely and even begin their own testing. It's too soon to say that FIDO will become the global de facto standard

for authentication, but the omens are good. It's supported by the world's leading technology players, and they all desperately need better authentication. The Internet of Things will also need something better than passwords to avoid becoming a security disaster. FIDO embraces several authentication technologies, so innovation and competition hopefully will thrive whilst remaining interoperable and the FIDO Alliance has stated that it is committed to submitting the protocols to a recognized standards development organization such as the IETF or W3C. As more users discover the joy of being free from passwords, and hopefully appreciate the added security FIDO authentication provides online services left relying on passwords may well begin to lose out.

MICHAEL COBB, CISSP-ISSAP, is a renowned security author with over 20 years of experience in the IT industry. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. He has also been a Microsoft Certified Database Manager and registered consultant with the CESG Listed Advisor Scheme (CLAS). Mike has a passion for making IT security best practices easier to understand and achievable. His website www.hairyitdog.com offers free security posters to raise employee awareness of the importance of safeguarding company and client data, and of following good practices.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.