Fast IDentity Online

Strong Password less (FIDO) Authentication

A white paper April 2015 about a ready to implement Security Key solution joint published by **Quantag Munich and SecureScrypt Germany** based on FIDO's public available information.

The FIDO Alliance is a non-profit 501(c)6 organization founded to address both the lack of interoperability among strong authentication devices, as well as the problems users face with creating and remembering multiple usernames and passwords. The success of the FIDO Alliance ecosystem is predicated upon user trust, with the goal of preserving users' privacy while providing strong authentication to online services. This paper describes the privacy-preserving principles that are a core part of the FIDO Alliance's technologies, and explains how they reinforce the FIDO Alliance's approach to strong authentication. Privacy Privacy means many different things to many different people the world over: even its formal definitions differ across cultural, linguistic, and legislative borders. In the FIDO Alliance context, we use the terms "user verification" to refer to how a device locally interacts with or identifies the user, and "authentication" to refer to how the user is identified to a remote system over the network using FIDO cryptographic protocols. Privacy in the context of FIDO is intrinsically challenging, since a strong user verification system must be able to identify the legitimate account holder, which in turn requires persistently retaining information about that user. The FIDO Alliance's approach to privacy revolves around well-defined collection and use of data that pertains to a specific user. We will refer to this data throughout this document as personal data. Moreover, any use of this data must not be surprising to the user. This also means that user verification information should not be easily combinable with data from other sources, as that would allow persistent identification outside the scope of a FIDO-based user verification process.

While the Association is recommending specifications, it is the task of the members to translate these specification into a workable protocol, client interface, server interface. Using the associations recommendations warrants the interoperability between members individuals solutions and increasing a simple operation for end-users. Quantag / Securescrypt is one of the first companies that has developed a ready to implement client server solution, as add on to existing verification systems.

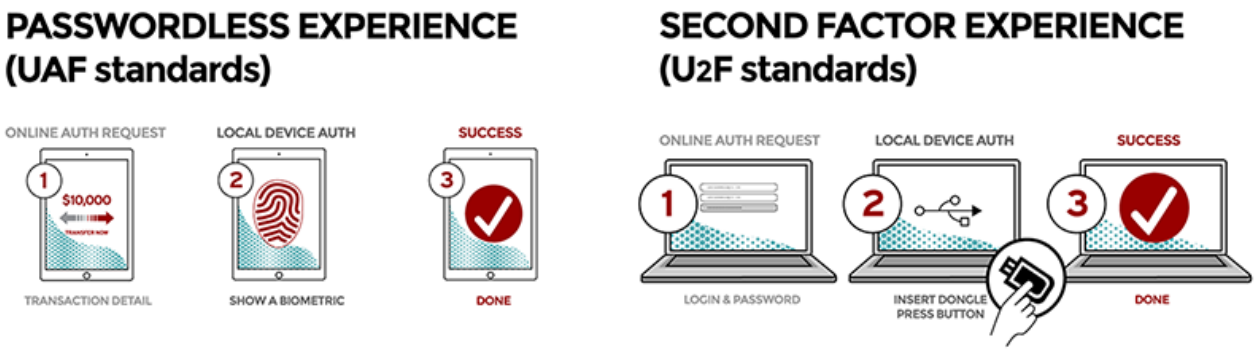
FIDO's aim is that its specifications will support a full range of authentication technologies, including biometrics such as fingerprint and iris scanners, voice and facial recognition, as well as existing solutions and communications standards, such as Trusted Platform Modules (TPM), USB security tokens, embedded Secure Elements (eSE), smart cards, and near field communication (NFC) The USB security token device may be used to authenticate using a simple password (e.g. 4-digit PIN) or by pressing a button. The specifications emphasize a device-centric model.[3]Authentication over the wire happens using public-key cryptography. The user's device registers the user to a server by registering a public key. To authenticate the user, the device signs a challenge from the server using the private key that it holds. The keys on the device are unlocked by a local user gesture such as a biometric or pressing a button.[3]

FIDO specifications provides two categories of user experiences. Which one the user experiences depends on whether the user interacts with the Universal Second Factor (U2F) protocol or the Universal Authentication Framework (UAF) protocol. Both FIDO standards define a common interface at the client for the local authentication method that the user exercises. The client can be pre–installed on the operating system or web browser.

FIDO v1.0 specifications were announced on December 9, 2014

By the end of February 2015, FIDO members included among others BlackBerry, CrucialTec, Discover Financial Services, Discretix, Google, Lenovo, MasterCard,Microsoft, Nok Nok Labs, NXP Semiconductors, Oberthur , Quantag Technologies, PayPal, Synaptics, Egistec,Visa, Feitian, Validity, Yubico, Agnitio, Entersekt, EyeLock, Fingerprint Cards, SurePassId, FingerQ, IDEX ASA, Infineon Technologies and SecureKey.

The FIDO Alliance has two sets of specifications, U2F and UAF.

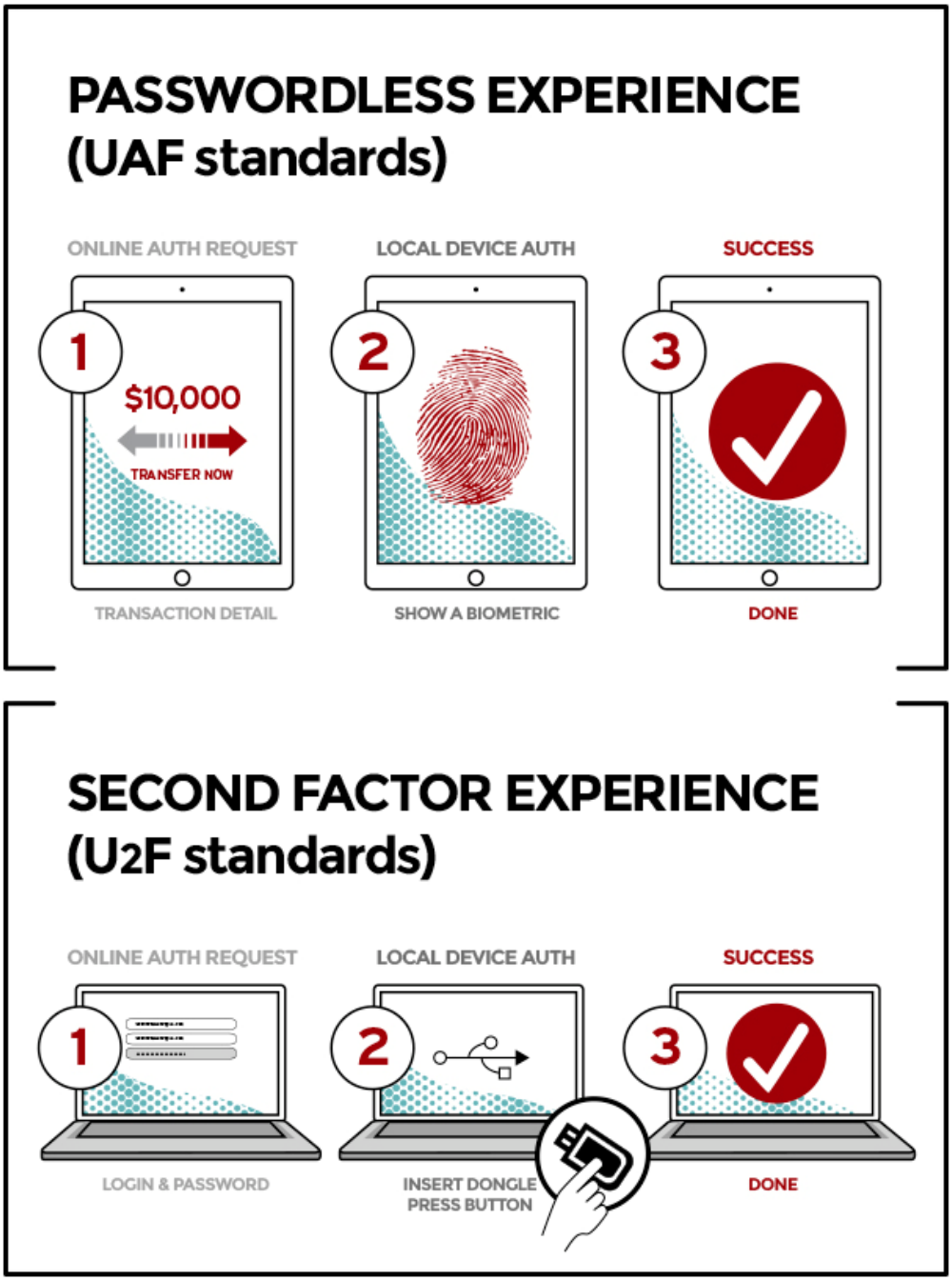


Specifications Overview

The FIDO Alliance has two sets of specifications, U2F and UAF. These specifications are now considered final. The Alliance is providing support for SI deployment of the technology .

The User Experience

FIDO provides two user experiences to address a wide range of use cases and deployment scenarios. FIDO protocols are based on public key cryptography and are strongly resistant to phishing.



Password less UX (UAF)

- User carries client device with UAF stack installed
- User presents a local biometric or PIN
- Website can choose whether to retain password

The password less FIDO experience is supported by the Universal Authentication Framework (UAF) protocol. In this experience, the user registers their device to the online service by selecting a local authentication mechanism such as swiping a finger, looking at the camera, speaking into the mic, entering a PIN, etc. The UAF protocol allows the service to select which mechanisms are presented to the user.

Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms such as fingerprint + PIN.

Second Factor UX (U2F)

- User carries U2F device with built-in support in web browsers
- User presents U2F device
- Website can simplify password (e.g. – 4 digit pin)

The second factor FIDO experience is supported by the Universal Second Factor (U2F) protocol. This experience allows online services to augment the security of their existing password infrastructure by adding a strong second factor to user login. The user logs in with a username and password as before. The service can also prompt the user to present a second factor device at any time it chooses. The strong second factor allows the service to simplify its passwords (e.g. 4–digit PIN) without compromising security.

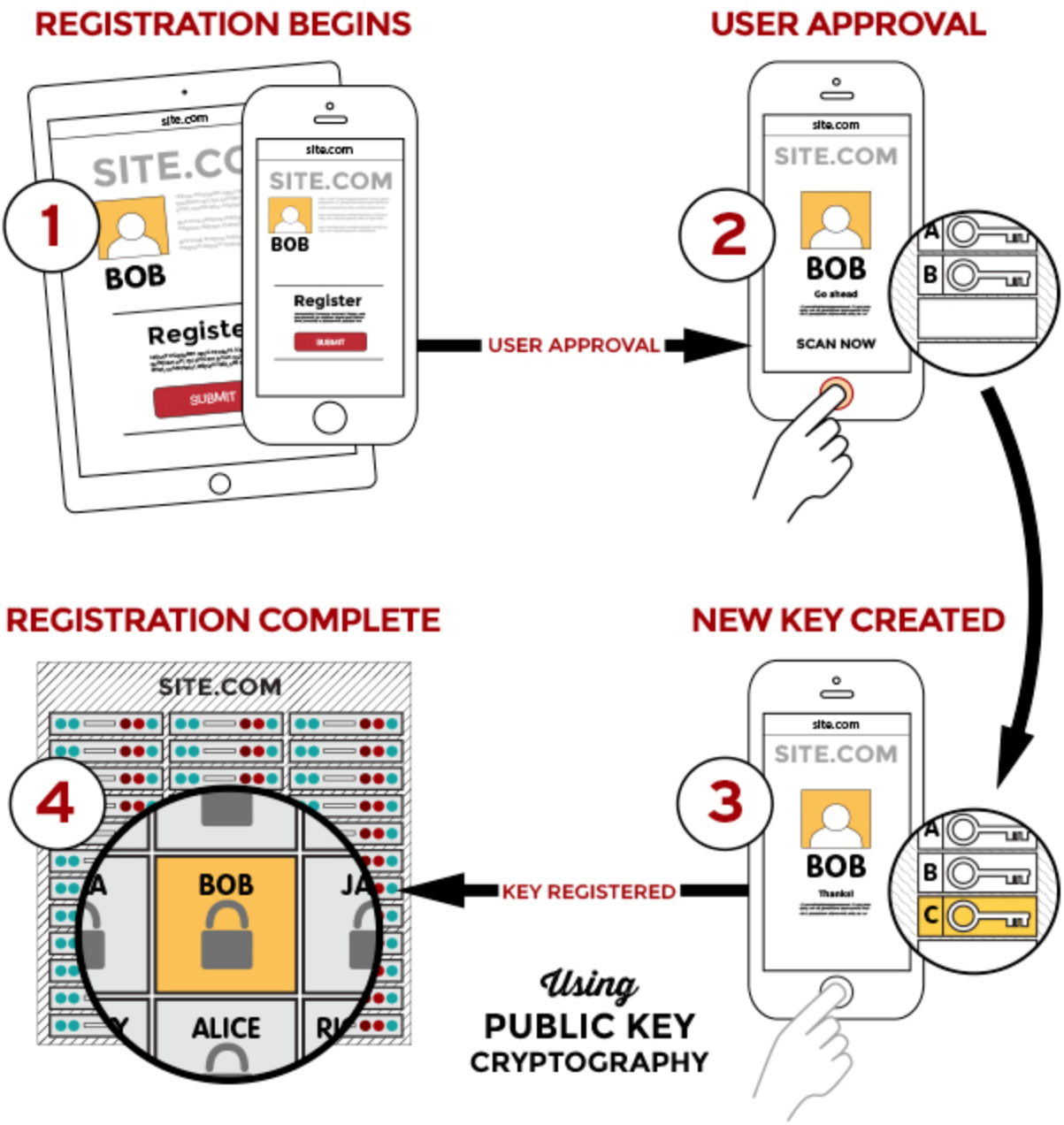
During registration and authentication, the user presents the second factor by simply pressing a button on a USB device or tapping over NFC. The user can use their FIDO U2F device across all online services that support the protocol leveraging built–in support in web browsers.

How FIDO Works

The FIDO protocols use standard public key cryptography techniques to provide stronger authentication. During registration with an online service, the user's client device creates a new key pair. It retains the private key and registers the public key with the online service. Authentication is done by the client device proving possession of the private key to the service by signing a challenge. The client's private keys can be used only after they are unlocked locally on the device by the user. The local unlock is accomplished by a user–friendly and secure action such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second–factor device or pressing a button.

The FIDO protocols are designed from the ground up to protect user privacy. The protocols do not provide information that can be used by different online services to collaborate and track a user across the services. Biometric information, if used, never leaves the user's device.

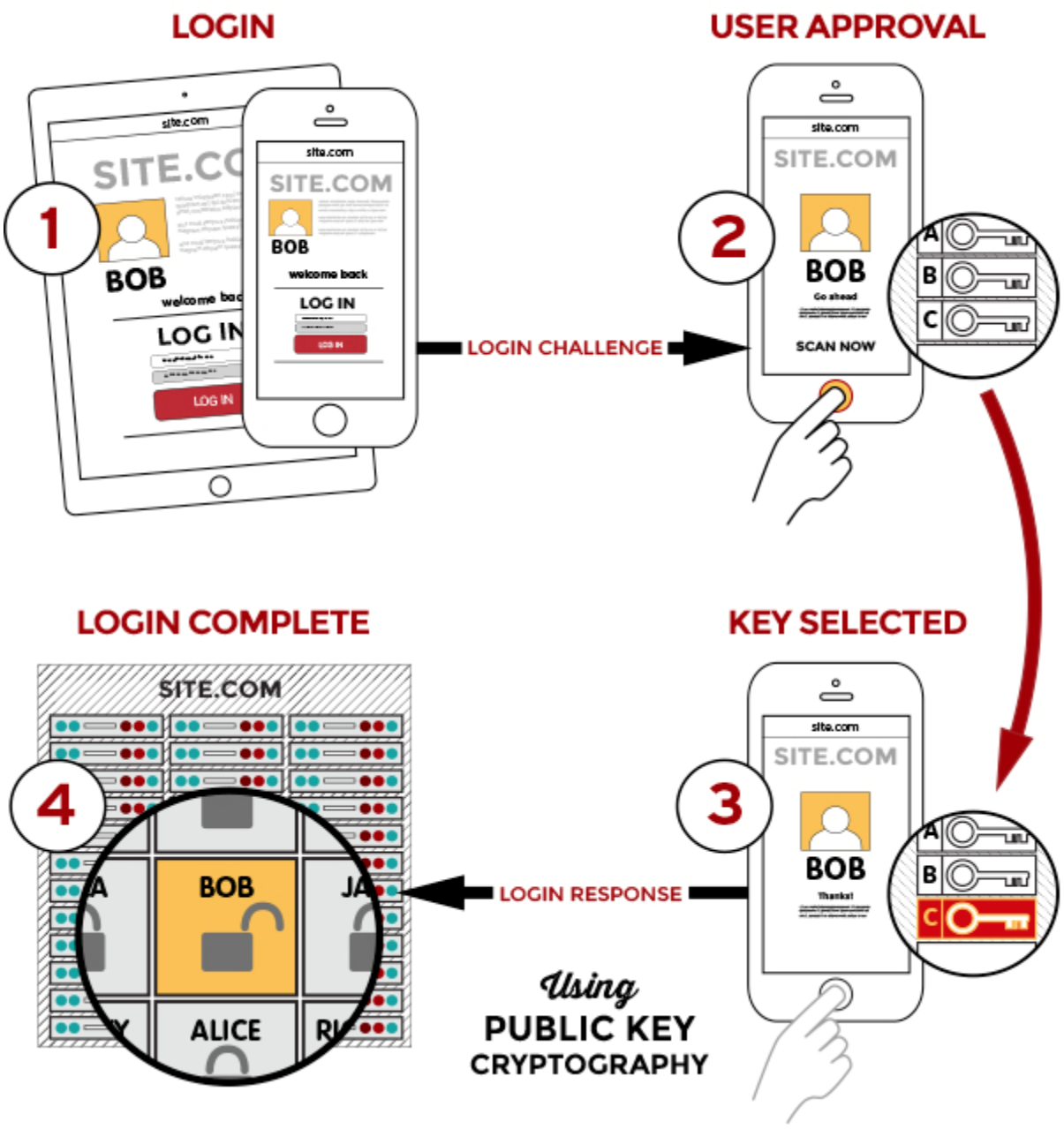
FIDO Registration



Registration:

- User is prompted to choose an available FIDO authenticator that matches the online service's acceptance policy.
- User unlocks the FIDO authenticator using a fingerprint reader, a button on a second–factor device, securely–entered PIN or other method.
- User's device creates a new public/private key pair unique for the local device, online service and user's account.
- Public key is sent to the online service and associated with the user's account. The private key and any information about the local authentication method (such as biometric measurements or templates) never leave the local device.

FIDO Login



Login:

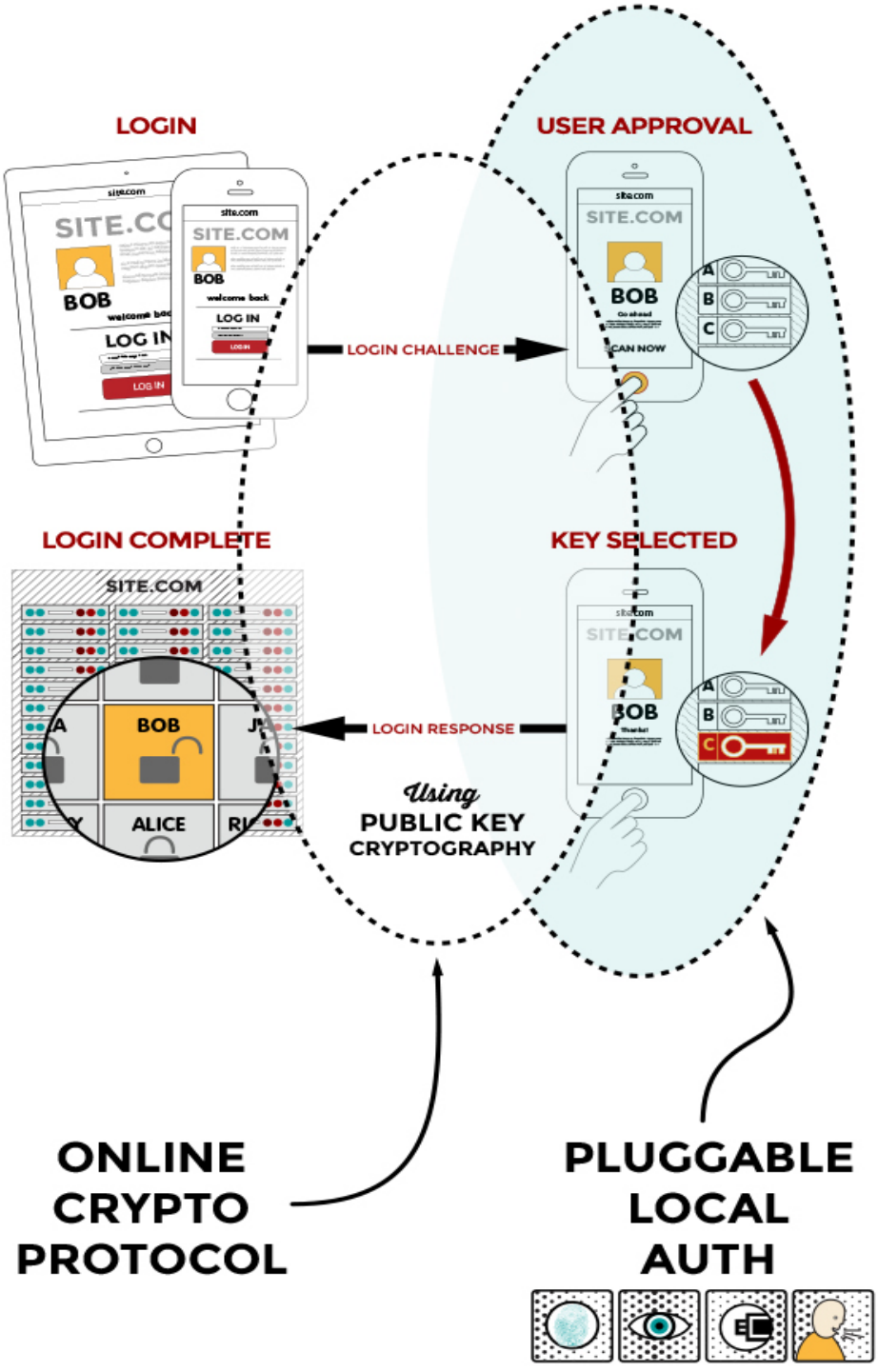
- Online service challenges the user to login with a previously registered device that matches the service's acceptance policy.
- User unlocks the FIDO authenticator using the same method as at Registration time.
- Device uses the user's account identifier provided by the service to select the correct key and sign the service's challenge.
- Client device sends the signed challenge back to the service, which verifies it with the stored public key and logs in the user.

What Makes FIDO Different?

The core ideas driving FIDO are (1) ease of use, (2) privacy and security, and (3) standardization. For implementing authentication beyond a password (and perhaps an OTP), companies have traditionally been faced with an entire stack of proprietary clients and protocols.

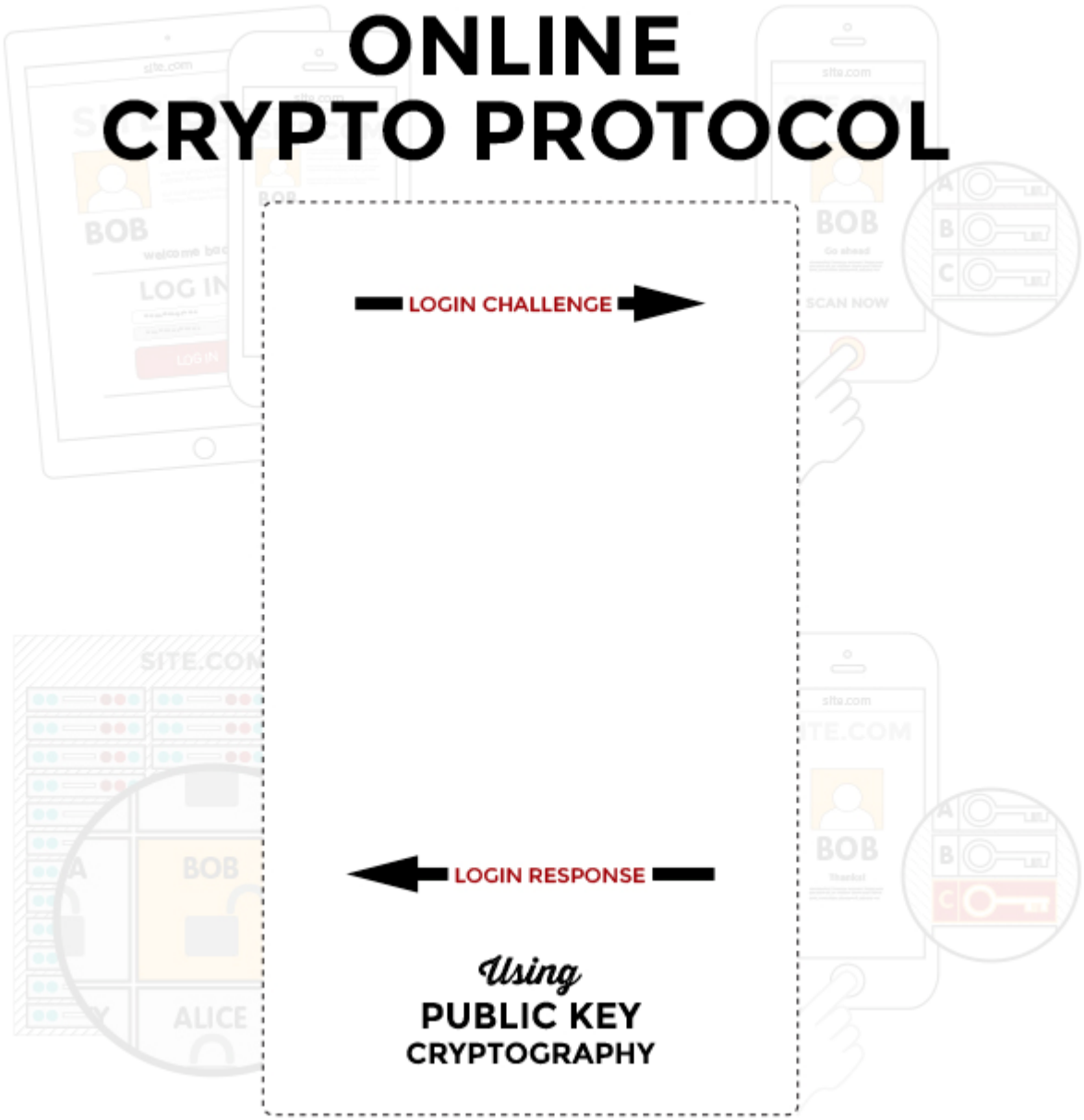
FIDO changes this by standardizing the client and protocol layers. This ignites a thriving ecosystem of client authentication methods such as biometrics, PINs and second–factors that can be used with a variety of online services in an interoperable manner.

FIDO Standardization



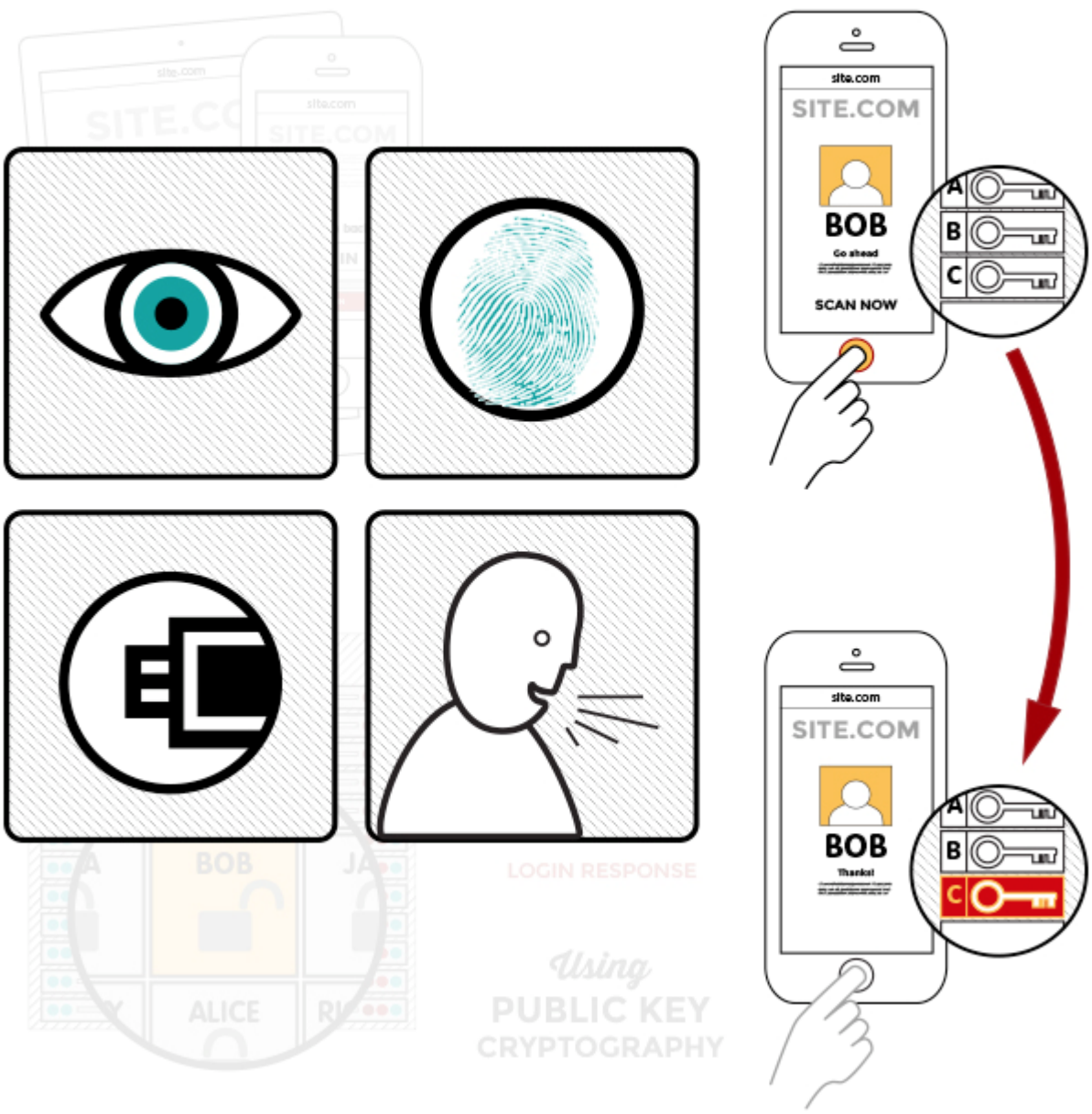
Online Crypto Protocol Standardization

FIDO standardizes the authentication protocol used between the client and the online service. The protocol is based on standard public key cryptography — the client registers a public key with the online service at initial setup. Later, when authenticating, the service verifies that the client owns the private key by asking it to sign a challenge. The protocol is designed to ensure user privacy and security in the current day state of the internet.



Client Standardization for Local Authentication

FIDO standards define a common interface at the client for the local authentication method that the user exercises. The client can be pre–installed on the operating system or web browser. Different authentication methods such as secure PIN, biometrics (face, voice, iris, fingerprint recognition, etc.) and second–factor devices can be "plugged in" via this standardized interface into the client.



Benefits of FIDO Authentication

FIDO authentication provides a number of powerful benefits to each of its constituencies – consumers, online service providers, and enterprises. For consumers, FIDO provides strong security with a superior user experience, all while protecting their privacy. It relieves a major pain by eliminating the need to remember many passwords while providing a higher level of security. It has the potential to enable 4 The FIDO Alliance – December 2014 Whitepaper the use of many mobile applications that are currently hampered by lack of sufficient security. Consider mobile banking, a use case where a bank acts as an online service provider. According to the Federal Reserve, "concerns about the security of the technology were a common reason for not using mobile banking or mobile payments (69 percent and 63 percent, respectively, of non-users)" . With the FIDO authentication model, authentication 3 from mobile devices is secured with low added cost or complexity. According to a 2014 study by Axil Partners , 60 percent of Smartphone or tablet owners 4 who switched primary banks reported mobile banking

capabilities as "important" or "extremely important" in their decision to switch, up from 48 percent in a similar survey in the first half of 2013. Clearly, new services such as mobile banking provide one of the largest potentials for differentiation and growth in the banking industry. Yet there are currently no good solutions that can be effectively implemented to enable secure consumer authentication from mobile devices. For banks and others providing high value mobile services, FIDO represents a major opportunity for differentiation and growth. FIDO has the potential to provide similar benefits for service providers in payments, consumer web services, and other industries. Enterprises also stand to benefit from FIDO protocols. While strong authentication has been deployed by many large enterprises, it is typically implemented via hardware tokens that carry high acquisition costs. According to Gartner , average enterprise authentication implementation for a large enterprise in 2014 was priced at $189,000. In addition, a 2014 survey found that companies lose $420 of productivity annually per employee due to struggling with passwords. FIDO can significantly reduce these costs while improving security.

The FIDO Alliance and FIDO Deployments

The growth of internet technologies and mobile devices have made strong online authentication an increasingly important requirement. Yet, as described earlier in this paper, strong authentication solutions have been complex, expensive and difficult to use. The FIDO Alliance was conceived to transform the nature of online authentication by creating a new model of stronger and simpler authentication.

Back in 2009, Ramesh Kesanupalli (then CTO of Validity Sensors) had a conversation with Michael Barrett (then CISO of PayPal). Ramesh proposed to "fingerprint enable" PayPal, and while Michael was intrigued with the idea he expressed the need for such solution to be vendor agnostic and 3 Consumers and Mobile Financial Services 2014, Board of Governors of the Federal Reserve System, March 2014 4 AlixPartners Mobile Financial Services Tracking Study, March 12, 2014 5 Gartner Magic Quadrant for User Authentication, 1 December 2014 6 Survey by Widmeyer sponsored by Centrify Corporation, 2014 5

The FIDO Alliance – December 2014 Whitepaper standards based. The conversations progressed on from there, more experts got involved, and eventually the FIDO Alliance with six founding members was formed in the summer of 2012 and publicly launched in February 2013. As the vision of transforming online authentication appealed to many industry players, the Alliance experienced explosive growth, adding around 10 members per month to grow to over 150 members strong. Leading online service providers, financial institutions and technology companies joined the Alliance and contributed to the development of FIDO specifications. In February 2014, the Alliance issued draft specifications for public review, and in December 2014, final 1.0 specifications were made available.

In parallel with the specifications work, several mass-scale FIDO deployments were launched in the market during 2014. At the Mobile World Congress event in February 2014, PayPal and Samsung announced the first FIDO deployment, a collaboration that enables 7 Samsung Galaxy S5 users to login and shop with the swipe of a finger wherever PayPal is accepted. The Samsung Galaxy S5 device is equipped with a fingerprint sensor from Synaptics. PayPal and Samsung selected the Nok Nok Labs S3 Authentication Suite to 8 enable the new payment system.

The new service became available in April 2014. In September 2014, Alipay also selected Nok Nok Labs to enable secure online payments 9 via the fingerprint sensor on the Samsung Galaxy S5. In October 2014, Google launched support for the U2F protocol in its Chrome browser, 10 which set the stage for the world's first deployment of FIDO U2F authentication.

With this deployment, Google Chrome became the first browser to implement FIDO standards. In this use case, when signing into a Google Account, the user simply inserts **a Security Key** into their computer's USB port and taps it when prompted. Users can buy a compatible Security Key from any tested and approved FIDO Ready TM U2F vendor (currently, Yubico and Plug-up) and

Quantag / Securescrypt Munich, with its extensive experience in encryption technology and as partner of the **SecureSD Card from Swissbit in Switzerlannd**, is now the first European company that **offers a Security Key for the computers USB port as well a mobile client for Android and other Smart Phone Platforms.**

With the final 1.0 FIDO specifications available and with multiple mass-scale FIDO deployments launched, it is clear that the FIDO Alliance is picking up steam. More important, the new authentication model is changing the world – protecting consumers, reducing the cost of exposure to breaches for online service providers, and lowering infrastructure cost and complexity for enterprises.

FIDO Privacy Principles

The design and implementation of FIDO Authenticators, Clients, and Servers must adhere to the following principles in order to be considered fully compliant. Just as we seek to protect the integrity of users' accounts, we also ensure that FIDO technologies are not used to identify users when they don't want or expect it.

#1 Require explicit,

informed user consent for any operation using personal data This includes collection and use of personal, identifiable data during registration, user verification, and transaction confirmation. A user must not be identified without the user wanting, knowing, or expecting it.

#2 Provide

clear context to the user for any FIDO operations This includes, but is not limited to, explicitly specifying which user identity is being used for a FIDO-related operation and what the server identity is.

#3 Limit

collection of personal data to FIDO-related purposes Only collect FIDO-related personal information that is necessary for the FIDO operation between the user and the Relying Party. FIDO-related personal information is data collected during registration (and potentially during user verification) that is necessary to perform the specific FIDO-related task. We distinguish it from other information that may be collected by a Relying Party at the same time, but that is not part of FIDO operations' scope. At registration time, the Relying Party must disclose the information collected from the user. If any additional information is collected at user verification or transaction confirmation time, the collection must be disclosed to the user as well; if there is no further collection, no explicit further collection disclosure is required.

#4 Use

personal data only for FIDO operations The sole acceptable use of data collected during a FIDO operation is to perform identification— for example registration, user verification, or authorization.

#5 Prevent

identification of a user outside of FIDO operations FIDO-related data must not be used to identify a user other than during a FIDO operation, or a user-desired and user-expected identification operation such as a system login.

#6 Biometric data must never leave the user's personal computing environment

Biometric data, measurements and personally identifying derivations of such data must be protected against extraction from the authenticator, and never transmitted outside the user's personal computing environment.

#7 Protect FIDO-related data from unauthorized access or disclosure

Data related to FIDO operations must be protected appropriately. This will be verified as part of the FIDO Certification Working Group's guidelines.

#8 Allow users to easily view and manage their FIDO Authenticators

It should be easy for users to list the FIDO Authenticators associated with their account and perform standard tasks with this information, e.g. de-register an Authenticator in the event of its loss.

Conclusion

These Privacy Principles reflect the FIDO Alliance's unambiguously strong commitment to protecting our users' privacy. The comprehensive technical mechanisms that pervade FIDO's specifications provide the foundation that makes the FIDO standards as privacy protecting as they are secure.

For more details about ready to use FIDO systems please contact info@securescrypt.com Subject Keyword: FIDO