



# FIDO Alliance Overview

---

January 2020

**NovuGens**



# Presentation Summary

1. What is FIDO Alliance?
2. What are the FIDO specifications?
3. How does FIDO work?
4. What are the key benefits of FIDO?
5. Is FIDO the right solution for everyone?
6. Thank you

# What is FIDO Alliance and Key Benefits

## FIDO Alliance

---

- Authentication standards to help reduce the world's over-reliance on passwords and other “shared secrets”.
- Provide login experiences that are more secure than passwords and SMS OPTs
- Simpler for consumers, and easier for service providers to deploy and manage
- FIDO Alliance is driven by hundreds of global tech leaders such as Microsoft, Google, Samsung, Fujitsu, Amazon, Mastercard and Visa.

## Key Benefits

---

- Transmitting private data to a relying party's server introduces an element of risk while the data is in transit. With FIDO, the only data in transit is a string of random characters, which even if stolen, cannot be used to reconstruct anything of value.
- Relieves the relying party of having to possess a “honey pot” of private user data, which can become a target of breach
- User experience of FIDO is significantly faster, since the cryptographic work is being done locally as opposed to on a distant server.
- Reduce the strain on the relying parties' servers, cut costs, and conserve operational resources.

# What are the FIDO specifications?

- The FIDO Alliance specifications are comprised of FIDO2, FIDO, Universal Authentication Framework (FIDO UAF) and FIDO Universal Second Factor (FIDO U2F).
  - **FIDO UAF** supports passwordless authentication experiences, commonly utilizing a mobile device's biometric capabilities
  - **FIDO2**, whose specifications comprises of W3C, WebAuthn, and CTAP, supports passwordless and second-factor use cases, enabling users to leverage biometrics and/or FIDO security keys to easily authenticate to supported web browsers and platforms such as Google Chrome, Microsoft Edge, Mozilla Firefox, Android and Windows.
  - **FIDO U2F** supports the use of a strong second factor such as a FIDO security key, is now part of FIDO2.

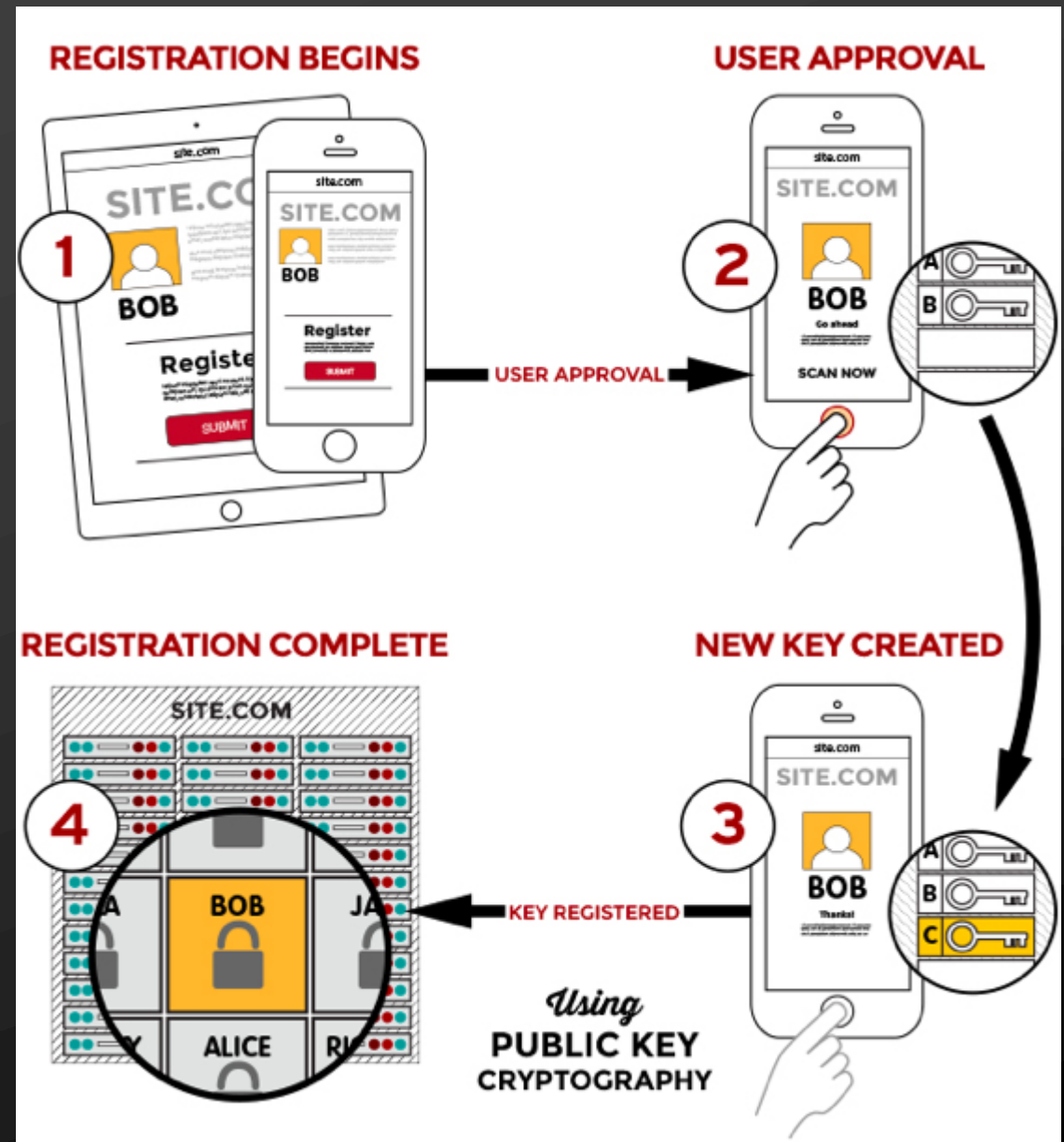
# How does FIDO works?

- FIDO brings the tried-and-true concept of public key cryptography to mobile devices and the web
- For each user, there's an interlocking pair of cryptographic keys, one public and one private
- When you “sign” data using the private key kept secret on your device, anyone can then verify authenticity of the data by referencing your public key.
- In the traditional paradigm, you send your private data off to a relying party's server for authentication, which places your private data in transit (where it can be stolen or phished)
- With FIDO, the private data never leaves your device. Rather your device or browser itself performs the authentication locally, then reports confirmation back to the relying party's server.



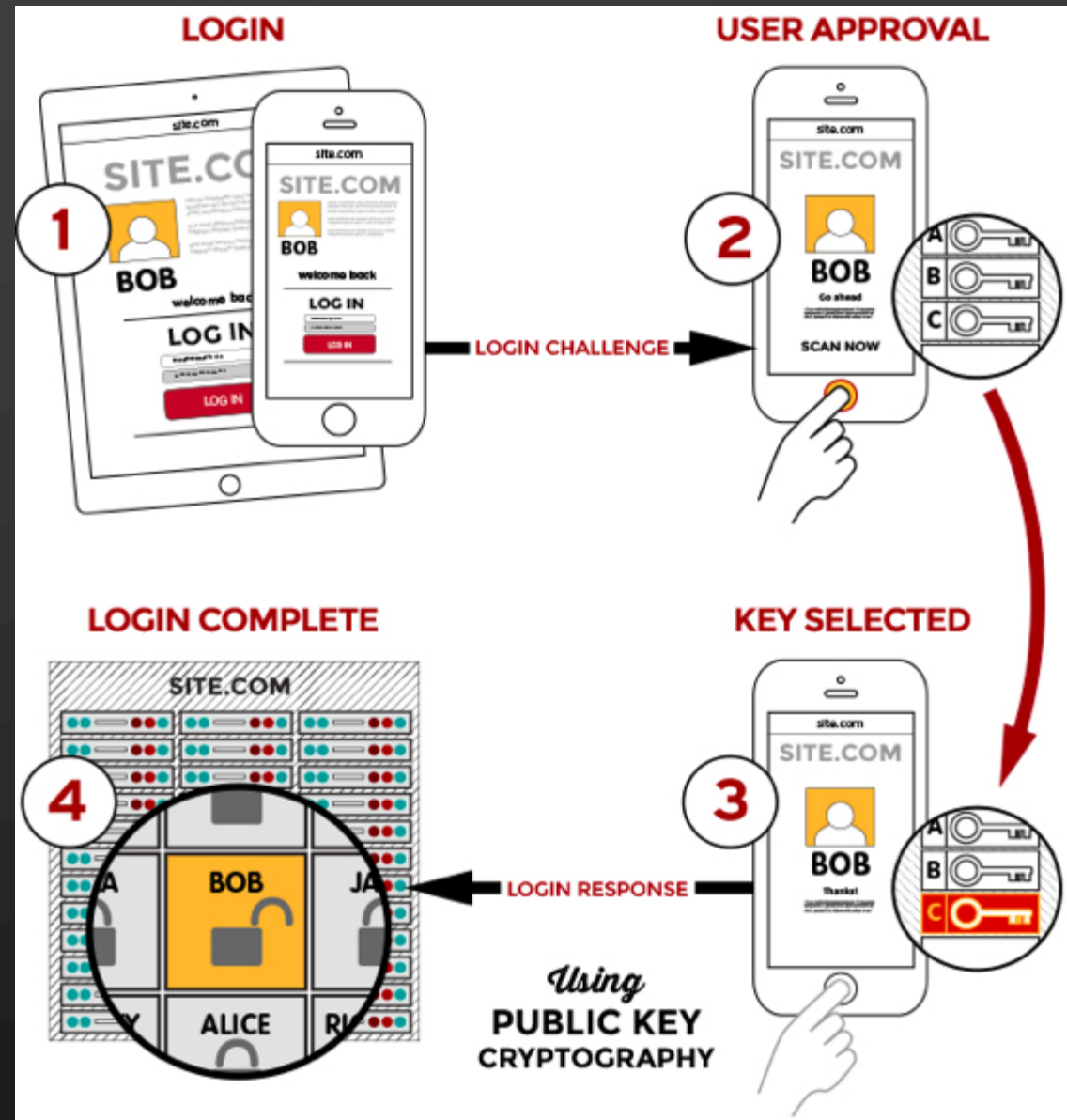
# FIDO Registration

- 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

- 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.



# As a relying party, why would I bother with FIDO

When I could simply integrate my mobile app with the native biometric readers on iOS and Android devices?

- FIDO specifications have been peer-reviewed by many of the world's top public- and private-sector security experts over a period of several years
- New authenticators are being introduced almost daily, and they're being written to the FIDO specifications, which makes FIDO Certified deployments futureproof, while direct integrations with an operating system would need to be perpetually reworked as the market changes.
- FIDO specifications allow for users to choose between several biometric authentication methods (face, voice, fingerprint, palm, etc.), whereas native device authenticators typically push users to a single modality
- In the event a certain biometric modality is ever comprised, FIDO deployments can instantly switch to an alternate authentication method, or layer several biometrics together for added security



# Is it common for relying parties to deploy both FIDO authentication and server-side authentication?

- This is indeed very common and an excellent way to accommodate the widest range of needs and use cases. In some instances, relying parties will combine both types of authentication within a single user session.
- For instance, your bank might allow FIDO authentication for low-risk activities like checking your balance, but then require you to “step up” to server-side authentication before allowing a higher-risk activity like the transfer of funds.

# What is the special significance of FIDO2?

- FIDO2 is the newest FIDO specification, and Daon is among the very first to be certified for the server component. With FIDO2, the advantages of FIDO are now available in web browsers such as Microsoft Edge, Mozilla Firefox and Google Chrome.
- FIDO2 is complementary to UAF, which is still required for the rich mobile application channel.

# Is FIDO the right solution for everyone?

- Certain customers and use cases will require that authentications take place on a server, and not (as with FIDO) on a local device.
- In some industry, the law mandates server-side authentications, exclusively, so that the data can be stored and reviewed by regulators.
- In other cases, relying parties may be particularly concerned about potential collusion between two or more device holders sharing their biometrics on a single device
- Server-side authentication can bring some added efficiencies by allowing biometrics used for enrollment to be re-used across other channels and applications.
  - For example: if you've enrolled your voiceprint in a mobile banking app with server-side authentication, that bank's call center can now validate your identity over a landline phone by comparing your speech to the voiceprint on their server.





NovuGens


Carlos E. Canales  
FOUNDER AND CEO

# Thank you

---

 Carlos Canales

 +1 (202) 230-2339

 [Carlos.Canales@NovuGens.com](mailto:Carlos.Canales@NovuGens.com)

 <http://www.novugens.com/>

## Document Type

This document is considered to be **strictly confidential** as it may contain proprietary information from one or more vendors.

## Disclaimer

The information in this document is subject to change without notice. NovuGens makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. We welcome user comments and reserve the right to revise this publication and/or make improvements or changes to the products or programs described in this publication at any time, without notice. Products sold or licensed by NovuGens are covered by the terms of its contractual agreements, license agreements and any warranties or guarantees therein.

## Validity of Information

NovuGens has made every effort to ensure that all statements and information contained herein are accurate. NovuGens does not warrant that this document is error free.

## Trademark Acknowledgements

NovuGens is a registered Limited Liability Company. Daon is a registered trademark of Daon Holdings limited. Oracle is a registered trademark of Oracle International Corporation. Linux is a registered trademark of Linus Torvalds. Red Hat is a trademark of Red Hat, Inc. Oracle and Oracle11g are registered trademarks of Oracle International Corporation. Microsoft and SQL Server are registered trademarks of the Microsoft Corporation. Windows is a trademark of Microsoft Corporation. Twilio is registered trademark under Twilio INC.

All other brands and products referenced herein are or may be trademarks or registered trademarks of their respective owners.