

# Journal Entry 3: FIDO

Name: Leah Drew


Date: 10/13/2019

## Details

FIDO stands for “Fast IDentity Online” and was created as a potential solution to issues with password management. Prior to 2012, strong authentication technologies were overly complex for the user and resulted in less secure behavior. FIDO was formed to address this problem and provide an alternative (Shamas, 2019). According to [fidoalliance.org](https://fidoalliance.org), the alliance is “working to change the nature of authentication with open standards that are more secure...and easier for service providers to deploy and manage” (“FIDO Alliance Overview - Changing the Nature of Authentication,” n.d.). Essentially, they offer organizations a secure alternative to normal authentication methods that is standardized and easy to use. They also have a certification program that validates the security of companies that follow their specifications. Overall, they aim to make authentication simpler for the user and stronger against attackers (“FIDO Alliance Overview - Changing the Nature of Authentication,” n.d.).

According to CioDive, standardization is at the forefront of the alliance’s efforts, with ease of access as one of the main goals (Eide, Schwartz, & Hickey, 2018). They recognize that in order to ensure that users are secure, having fewer passwords and fewer systems to learn to navigate is ultimately better. Rather than making every login system require a unique password, FIDO aims to eliminate passwords and replace them with more secure, universal methods of authentication. In this way, FIDO “wants to create an ecosystem of authentication, which extends across hardware, mobile and biometrics to access applications and websites” (Eide et al., 2018).

In general, users rarely follow password rules set by organizations. They commonly write down their passwords or find other ways of circumventing the rules, which ultimately makes the system less secure (Choong, Theofanos, & Liu, 2014). FIDO aims to fix this by eliminating the need for complex passwords altogether and unifying everything under one system, making things more convenient for users. They improve security by only storing data on the user’s device, and address the issue of privacy by having each website have unique keys for users,



making it impossible to track them across multiple sites. These strategies reduce password theft and phishing, and ultimately make things more secure for the system as a whole (Shamas, 2019).

## References

- Choong, Y., Theofanos, M., Liu, H. (2014). *United States Federal Employees' Password Management Behaviors – a Department of Commerce Case Study*. Retrieved October 13, 2019, from <https://drive.google.com/file/d/1nYwfFwRc7IZPMIcCwgJL0ULJ0pf7xAD7/view>.
- Eide, N., Schwartz, S., & Hickey, A. (2018) *5 password management trends businesses need to know*. Retrieved October 13, 2019, from <https://drive.google.com/file/d/1zp1sLwvmYCc5rBun3qiH68JQxouMPNWf/view>.
- FIDO Alliance Overview - Changing the Nature of Authentication. (n.d.). Retrieved October 13, 2019, from <https://fidoalliance.org/overview/>.
- Shamas, M. (2019). *W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins*. Retrieved October 13, 2019, from <https://drive.google.com/file/d/1JAI6QFdTJ6ozasUuhyFQGSHSsdBcd3wA/view>.