

# Hardware Security Tokens In Context Of FIDO2

## Seminar: Advances in Cryptography and IT-Security

Robert Hartings

January 4, 2022  
RWTH Aachen  
Research Group IT-Security

**Organizer:** Ulrike Meyer  
**Supervisor:** Vincent Drury

**Abstract.** The abstract should briefly summarize the contents of the paper in 150–250 words.

## 1 Introduction

Credentials with username and password are still the most common variant of user authentication today, despite their problems with phishing or dictionary attacks, for example. To create secure accounts, it is recommended to use strong passwords (including capital and lower letters, numbers and special characters and a minimum length) while refraining from reuse. The user has to memorize these rather complex different passwords or use a password manager which has its own disadvantages. If credentials are reused on multiple accounts, they are vulnerable to credential stuffing attacks, in which an attacker uses stolen credentials from one service on other services hoping for same or similar credentials, making it easier for him to guess the right combination of username/email and password. Username and password are always vulnerable to phishing, because it cannot be ruled out that even the most experienced user will make a mistake and enter their credentials on a website owned by an attacker.

This problem is challenged by the FIDO Alliance and the W3C by providing a possible solution: The Fast Identity Online 2 (FIDO2) standard. The main difference between the proposed standard and status quo is the paradigm shift from "something a user knows" to "something a user poses". The FIDO2 standard includes a successor to the Universal 2nd Factor (U2F), which was also developed by the FIDO Alliance and, in addition to the familiar Second Factor, also offers the possibility for Single Factor Authentication, making password as we know them superfluous. The cost, inconvenience and unfamiliarity of (hardware) security keys are currently reasons for their low uptake.[LHGU21][GLSN<sup>+</sup>20]

But like other authentication variants, FIDO2 has its own unsolved problems and drawbacks. In this paper I would like to summarize these problems and possible solutions.

## 2 Background

### 2.1 Hardware Security Tokens (HSTs)

HSTs are used to securely store a secret key used for cryptographic functions in a tamper-resistant storage. The main idea is that the secret never leaves the secure storage. The secret key is used for deriving subsequent authentication keys for creation of public / private identities. The derived keys are mainly used to sign received challenges, but can also be used to identify a user.[PMD<sup>+</sup>21]

HST, also called authenticators, can be so called security keys but also integrated authenticators including Trusted Platform Module (TPM), Android keystore and Apple TouchID. Microsoft Hello is one example for the TPM.

Security keys from vendors like Yubico (Yubikey), Feitian (FIDO Key) and Google (Titan Key) are very popular. In the most cases a user has to touch a sensor to verify his presence. They can also be shipped with biometric scanners / sensors, most commonly finger print sensors, to unlock the private key and authentication the requested action. If the authenticator is external, communication with the device takes place via USB (Universal Serial Bus), NFC (Near Field Communication) or BLE (Bluetooth Low Energy).[GLSN<sup>+</sup>20]

### 2.2 Fast Identity Online 2 (FIDO2)

The Fast Identity Online 2 (FIDO2) Project is a joint effort from the FIDO Alliance and the World Wide Web Consortium (W3C). It is an open authentication standard succeeding prior work of the FIDO Alliance on Universal 2nd Factor (U2F). [GLSN<sup>+</sup>20] It consists of two protocols. The WebAuthn protocol, maintained by the W3C, and the Client to Authentication Protocol 2 (CTAP2), maintained by the FIDO Alliance. Members of the FIDO Alliance include Amazon, Google, Meta and Microsoft.

The WebAuthn protocol specifies a JavaScript-based API used for communication between a service provider / WebAuthn relying parties (e.g. websites) and a WebAuthn client like a browser. All major browsers support WebAuthn today.[Aut21] The CTAP2 standardizes the communication between a client and the (external) authentication device.[LHGU21][AWAC20]

The main idea of FIDO2 is to use public-private cryptography instead of known credentials like username and password. Furthermore, it creates a public-private keypair unique to a given application or website, which is used to sign challenges from the service and is only generated and stored on the authenticator. This is realized through a mutual authentication using a service identifier. In case of websites the authenticator receives the domain of the requesting website. Effectively rendering phishing useless, because a relying attacker cannot provide the authenticator with the right domain.[UAA<sup>+</sup>21] Also preventing replay attacks and password theft. Tokens acquired through server breaches cannot be reverted to the original secret key on the authenticator nor can they be used to determine private keys used for other services.

To ensure quality and security the FIDO Alliance setup a metaservice which can be inquired to verify the used authenticator. The relaying party can check if the authenticator meets the FIDO Alliance standards and has no known vulnerabilities.[AWAC20]

### 3 Problems of FIDO

While FIDO2 seems like a optimal solution, there are currently some disadvantages, which cannot be ignored during the evaluation of the usability and usefulness of hardware security tokens.

#### 3.1 Misconceptions

The study by Lassak et al.[LHGU21] about misconceptions in FIDO2 Biometric WebAuthn shows that users are not yet educated enough to understand the basic functionality of FIDO2 HSTs. There are among others misconceptions about storage location, recovery and usage of different devices. The study was held online with 42 participants from the UK and US. All of them were older than 18. The used HSTs were the participant android smart phone.

*Storage Location* The majority of the participants thought that there biometrics were sent (in an encrypted fashion) to the corresponding service provider. Only 14 participants recognized that the biometrics are stored locally and only 2 figured out that the service provider could not get there biometric data, because he is not in possession of the phone (HST).

Likewise, only 24 participants know / guessed that their biometric data are not affected in the event of a database breach on the services provider site.

Overall, only 4 participants were confident that their biometric data did not leave the phone when they used it for authentication.

*Lost HST* Because the private key used for authentication is stored on a phone, losing it can provide an attacker with access to the accounts. From the 42 participants 39 thought that an attacker need their biometrics for the authentication while in fact the private key can be unlocked with fallback mechanism likes PIN, pattern or password.

*Availability* If the unlocking of the phone via biometric fails only five participants were aware that they can unlock the HST with fallback options like PIN, pattern or password. The other participants stated that they have not setup a backup method at the service provider or they have to contact the service provider to recover their account.

*Multiple Devices / Delegating Access* Also, there are misconceptions concerning device sharing. One misconception is that it is possible to use another device (after registering one's biometric data). Only six participants were aware that the login is tied to the authenticating device and that the biometric is only used to decrypt and unlock the private key for the authentication process. Transferring the private key from one authenticator to another is not intended in the current WebAuthn specification. If this kind of behavior is needed a roaming authenticator is needed. Furthermore, it is possible on some services to register more than one HST for a single account.

To grant a trusted person access 39 participants answered that it is not possible since the person would not have the required biometric data. The other participants argued that it would be possible using fallback methods or registering the biometric data of the trusted person on the HST (phone).

*Idea of resolving this problem* To prevent this type of misconceptions, service providers and HST manufacturers should launch an information campaign about HSTs and how they work. If one or both of them fail to do their job or additional advertising is needed, consideration should be given to whether government institutions, such as the BSI (German Federal Office for Information Security), should launch joint / own campaigns to inform the population about better methods of securing their accounts online.

### 3.2 Downgrade Attacks

Besides FIDO different methods of multifactor authentication exist, like One-Time-Passwords (OTP), confirmation SMS and calls and the usage of recovery codes. Commonly the user can choose between the configured MFA schemes, but expect FIDO2 none of the mentioned schemes is secure against real-time phishing. While reviewing Alexa's top 100 websites Ulqinaku et al. found out that most of these websites force users to register at least one different MFA to use FIDO2 in the first place. Effectively creating a vulnerability even when FIDO2 is used, because it undermines the security of FIDO2. Only Google with Google's Advanced Protection offers a program not relying on weak MFA, but it is opt-in and not advertised on the Google Account Dashboard.

A downgrade attack on FIDO2 can only be done if the user has different and weaker MFA registered to his account. The attacker can use this to ignore / skip the authentication via FIDO2. If a user visits a malicious website and tries a login to his account, the attacker can rely on the response to the victim. If the victim chooses to use FIDO2 the attacker simply ignores the response of the client and lets the user choose from a different MFA scheme, which is vulnerable to real-time phishing.

The attacker has to know when and if the user has inserted his security key to continue with the authentication. Normally the browser would present a box above the webpage containing the domain and asking for the security key, but it is also possible via API functions to detect the presence of a HST without displaying this box. The attacker can display such a box with the content he

likes on his website, but this is limited to the page and is not displayed above the content. For a normal user this is not easy to spot.[UAA<sup>+</sup>21]

### 3.3 Threats to HST

### 3.4 Threats to OFA FIDO2

FIDO2 allows the usage of a hardware security key as a single factor (OFA / SFA) or a multi factor (MFA).

### 3.5 More Problems

*Account Recovery*

*Account Suspension*

*Distribution*

*Convenience*

## 4 Conclusion

educate the user / population, support FIDO2 on more websites

## References

- [Aut21] Auth0. Does my browser support webauthn. <https://webauthn.me/browser-support>, 2021. Accessed: 2021-12-22.
- [AWAC20] Fatima Alqubaisi, Ahmad Samer Wazan, Liza Ahmad, and David W Chadwick. Should we rush to implement password-less single factor fido2 based authentication? In *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, pages 1–6, April 2020.
- [GLSN<sup>+</sup>20] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285, May 2020.
- [LHGU21] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "it's stored, hopefully, on an encrypted server": Mitigating users' misconceptions about FIDO2 biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 91–108. USENIX Association, August 2021.
- [PMD<sup>+</sup>21] Katharina Pfeffer, Alexandra Mai, Adrian Dabrowski, Matthias Gusenbauer, Philipp Schindler, Edgar Weippl, Michael Franz, and Katharina Krombholz. On the usability of authenticity checks for hardware security tokens. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 37–54. USENIX Association, August 2021.

- [UAA<sup>+</sup>21] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. Is real-time phishing eliminated with FIDO? social engineering downgrade attacks against FIDO protocols. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3811–3828. USENIX Association, August 2021.