*Aditya Mitra, et. al. International Journal of Engineering Research and Applications*
*www.ijera.com*
*ISSN: 2248-9622, Vol. 14, Issue 7, July, 2024, pp: 58-63*

RESEARCH ARTICLE OPEN ACCESS

# FIDO2: A comprehensive study on passwordless authentication

Aditya Mitra and Anisha Ghosh
*adityamitra5102@gmail.com, ghoshanisha2002@gmail.com*
*VIT-AP University, Andhra Pradesh, India.*

**Abstract:**
The twenty first century is marked as the digital era. It involves the use of computers and other devices like smartphones in every aspect of life. It is becoming increasingly important to understand the usages of such devices and to protect ourselves from malicious actors on digital platforms. The concept of authentication is not new, it started with Fernando Corbató in the 1960s when he developed the system of passwords for the MIT Compatible Time-Sharing System (CTSS) [1]. However, we have come a long way from using passwords and personal identification numbers (PINs) since they have fallen weak in the face of modern adversaries and attacks like phishing. This paper presents and discusses the FIDO2 standard for passwordless authentication for the protection of digital resources and assets. FIDO2 standard uses cryptographic challenge-response system combined with trusted computing to make the process of authentication truly Phishing resistant [2]. This paper presents a comprehensive view of FIDO2 specification standards and implementation.

## I. Introduction:

A user's online identity is as important as his physical identity in the digital world. The act of proving the identity of oneself while gaining access to an online resource is known as authentication [3]. Authentication is important prior to accessing sensitive information like bank or other financial details, confidential data. A user can prove his identity to a digital system by giving the evidence of:

- Something he knows (knowledge-based factors)
- Something he is (inherence factor)
- Something he has (possession factor)

For stronger authentication systems a combination of two or more factors can be used. This is known as multi-factor authentication. For example, in ATM machines, the user would usually need two factors namely the ATM card which falls under the possession factor, followed by the ATM PIN which is a knowledge-based factor.

For a long period of time, knowledge-based factors involving username and password were used for user authentication. But as time went by, adversarial actors were able to breach the same. There were incidents where databases containing passwords were breached [4], many cases of phishing where the adversarial actors developed fake websites to trick users into revealing their passwords [5], password guessing and more. Various attacks on password-based systems include keylogging, phishing, vishing, social engineering and more.

Inherence-factors involve the use of biometrics, for example facial recognition, fingerprint identification and so on. However, the same is vulnerable to presentation attacks [6]. Presentation attacks involve the use of pictures of the target, 3D models or deepfakes to gain access through the biometric recognition system [7].

Possession-based factors have proven to be secure against such remote attacks. This is because it requires the authorized user to physically connect the device, smart card, security key to the computer or bring it very close to the computer he is authenticating on to prove his identity.

FIDO2 is a possession-based authentication standard for web applications. It involves device attestation [8] with cryptographic challenge-response system to ensure that only the security key or smartcard possessed by the legitimate user can be used to authenticate him. It further uses trusted computing to ensure that the security key cannot be cloned, and the secrets cannot be extracted. This is in adherence to the standards set by the US government [9].

FIDO2: The standard

FIDO2 makes it easier for users to authenticate themselves without having to memorize complex passwords and at the same time makes it more secure against attacks on conventional authentication standards. It is heavily reliant on public key cryptography and uses cryptosystems like RSA [10] or ECDSA [11].

The FIDO2 standard is comprised of two major standards:

- Web Authentication (WebAuthn) [12], a standard that defines how web browsers can access and deal with public key credentials.
- Client to Authenticator Protocol (CTAP) [13], a standard that defines the communication with secure elements and security keys for cryptographic operations.

FIDO2 standard encourages storing private cryptographic secrets on a Secure Element (SE) [14], a Trusted Platform Module (TPM) [15], a Trusted Execution Environment (TEE) [16] or a Hardware Security Module (HSM) [17]. These ensure that the secret stays on the device itself and cannot be cloned or copied to other devices. The private keys never leave the device. These devices can perform cryptographic operations without passing the secrets to the CPU or memory of the host computer and include:

- Secure Element (SE): It is used in physical security keys and smart cards. It is extremely lightweight.
- Trusted Platform Module (TPM): It is mostly used in PCs and laptops. Most modern computers have inbuilt TPM. It can perform a host of cryptographic operations and is used by other authentication systems too, including Windows Hello.
- Trusted Execution Environment (TEE): It is a software defined secure sector on the CPU. It is used mostly in mobile devices that do not have a dedicated CPU. It ensures the cryptographic operations are performed on the specified sector of the CPU only and the keys are not communicated to the other parts of the CPU or memory.
- Hardware Security Module (HSM): These are mostly found in datacenters for storing cryptographic materials. It is a network connected device and is used as a key vault.

FIDO2 has been instrumental and has been implemented in various scenarios like in cases of user authentication in the metaverse [18], for securing physical assets on IoT based lockers [19] and more.

FIDO2 Workflow:

FIDO2 implementation involves a verifier and a claimant. The claimant requests to sign in to a service and the verifier verifies whether the claimant is the one who he claims to be. The 'verifier' is also known as a 'Relying party' (RP). The claimant can also be referred to as the 'user' or 'client'.

FIDO2 has two workflows. One is for a new user registration, also known as registration workflow, sign-up workflow or enrollment workflow. The other is for authenticating users, also known as authentication workflow or sign-in workflow.

Registration workflow: The user requests to enroll a new security key or device to the relying party. The relying party responds with a random cryptographic challenge.

The web browser of the user's device forwards the challenge and the domain name of the relying party (also known as RP ID) to the Cryptographic element. The cryptographic element generates new keypair. It signs the challenge and a hash of the RP ID with the private key. The private key is stored in the cryptographic element itself.

The signed challenge and the public key are then sent back to the relying party. It verifies the signed challenge and the RP ID hash to ensure that it was signed properly and was not subject to any man-in-the-middle attacks. The public key is then stored in the database of the Relying party.

Figure 1 shows the registration workflow.

Authentication workflow: The user requests to authenticate to the Relying party. The relying party responds with a random cryptographic challenge.

The web browser of the user's device forwards the challenge and the domain name of the relying party (also known as RP ID) to the Cryptographic element. The cryptographic element the challenge and a hash of the RP ID with the previously stored private key.

The signed challenge is then sent back to the relying party. It verifies the signed challenge and the RP ID hash with the previously stored public key to ensure that it was signed properly and was not subject to any man-in-the-middle attacks. When it is successful, the relying party authenticates the user successfully.

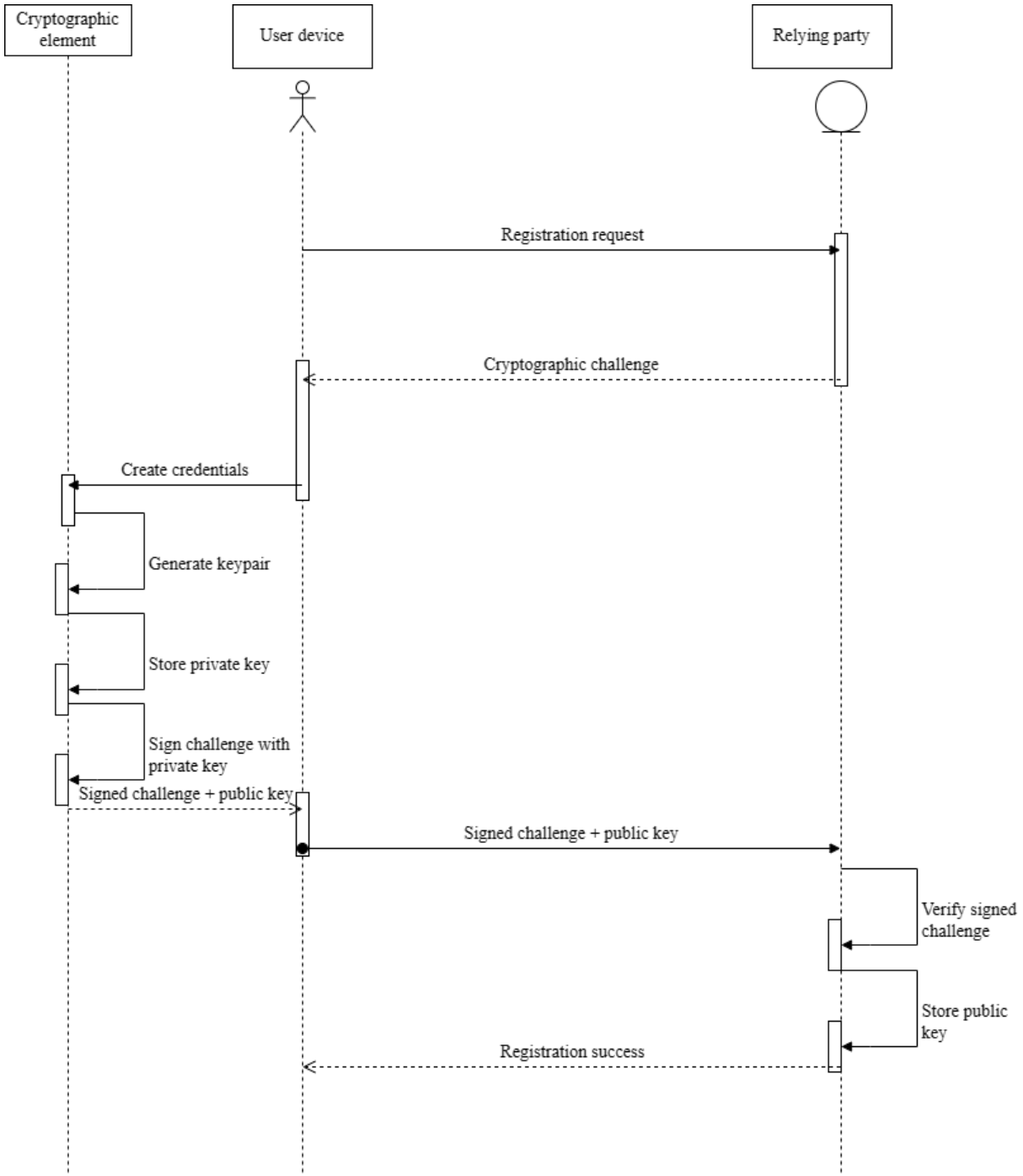


**Figure 1:** Registration workflow.

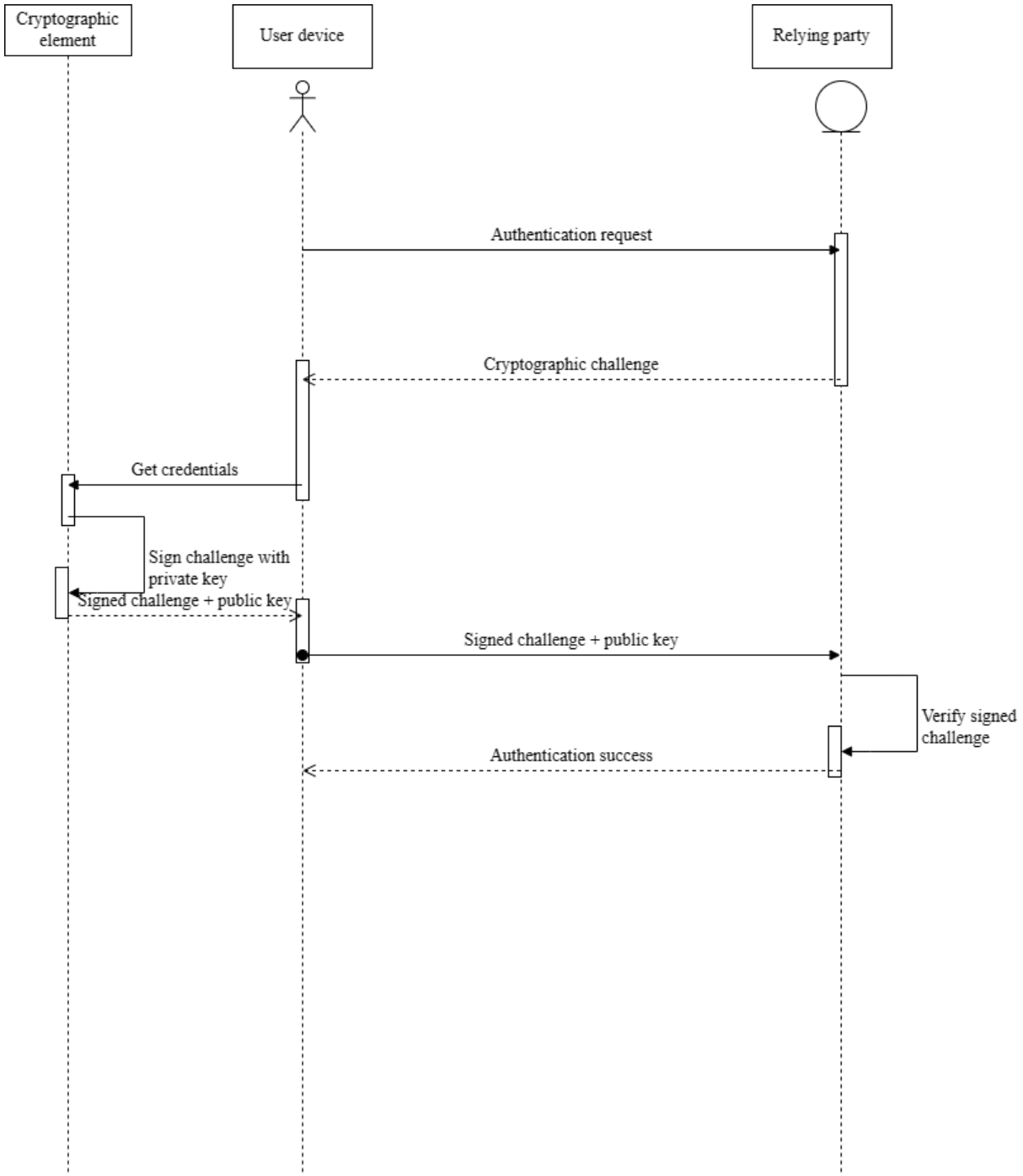


**Figure 2:** Login workflow.

User experience:

The user can use their personal device containing TPM or TEE as their cryptographic device. This includes devices running Android 7 or up, iOS 7 or up, Windows 10 build 1903 or up. The user can further use physical security keys or smartcards as the secure element. Organizations also issue security keys to their employees to ensure secure authentication on internal applications.

Figure 3 shows a physical security key.


Figure 3: FIDO2 security key. (Yubico Security Key)

Further, using the same is extremely convenient for the user. When a user attempts to sign in to a service, the computer prompts to connect a physical security key or to use fingerprint or computer pin to allow authentication. The rest of the process is automated and abstracted from the end user for the sake of simplicity.
Figure 4 shows the computer prompting for fingerprint and figure 5 shows the computer prompting to connect physical security key,

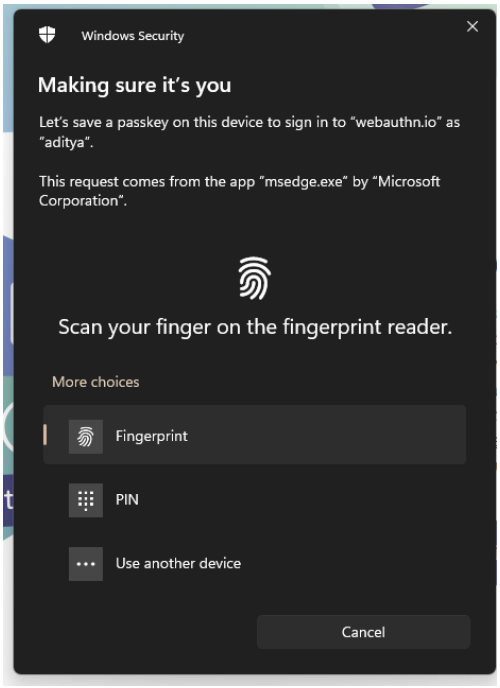


**Figure 4:** Prompt for fingerprint.

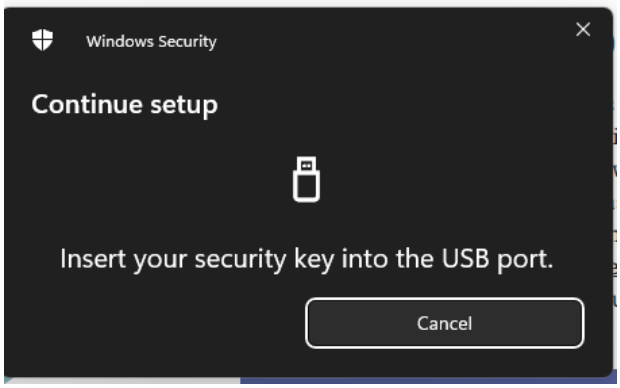


**Figure 5:** Prompt for physical security key.

## II. Conclusion

Hence, we discuss the merits and implementation of FIDO2 based passwordless authentication and identity management. This would be instrumental in mitigating vulnerabilities associated with traditional authentication factors. This would also be instrumental in making sign in process a lot easier and simpler for end users. It can be deployed in any web application with ready to use SDKs delivered by various open-source projects.

## References

[1]. Fano, R. M., & Corbató, F. J. (1966). TIME-SHARING ON COMPUTERS. Scientific American, 215(3), 128–143. http://www.jstor.org/stable/24931051
[2]. Ulqinaku, E., Assal, H., Abdou, A., Chiasson, S., & Capkun, S. (2021, August). Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols. 30th USENIX Security Symposium (USENIX Security 21), 3811–3828. Retrieved from https://www.usenix.org/conference/usenixsecurity21/presentation/ulqinaku
[3]. Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines: revision 3. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-63-3
[4]. Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Kelley, P. G., Invernizzi, L., … Bursztein, E. (2019, August). Protecting accounts from credential stuffing with password breach alerting. 28th USENIX Security Symposium (USENIX Security 19), 1556–1571. Retrieved from https://www.usenix.org/conference/usenixsecurity19/presentation/thomas
[5]. Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers &

Security, 68, 160-196. https://doi.org/10.1016/j.cose.2017.04.006

[6]. Raghavendra Ramachandra and Christoph Busch. 2017. Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey. ACM Comput. Surv. 50, 1, Article 8 (January 2018), 37 pages. https://doi.org/10.1145/3038924

[7]. P. Korshunov and S. Marcel, "Vulnerability assessment and detection of Deepfake videos," 2019 International Conference on Biometrics (ICB), Crete, Greece, 2019, pp. 1-6, doi: 10.1109/ICB45273.2019.8987375.

[8]. O. Arias, F. Rahman, M. Tehranipoor and Y. Jin, "Device attestation: Past, present, and future," 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 2018, pp. 473-478, doi: 10.23919/DATE.2018.8342055.

[9]. Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). Digital identity guidelines: authentication and lifecycle management. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-63b

[10]. Rivest, D. R., Shamir, A., & Adleman, L. (1977). RSA (cryptosystem). Arithmetic Algorithms And Applications, 19.

[11]. Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International journal of information security, 1, 36-63.

[12]. Jones, M, Kumar, A, Lundberg, E. (2023) Web Authenitcation: An API for accessing Public Key Credentials, W3C working draft, https://www.w3.org/TR/webauthn-3/

[13]. [13] Lindemann, R, Bharadwaj, V, Czeskis, A, Jones, M, Hodges, J, Kumar, A, Brand, C, Verrept, J, Ehrensvard, J. (2017) Client to Authenticator Protocol, FIDO Alliance Proposed standard, https://fidoalliance.org/specs/fido-v2.0-ps-20170927/fido-client-to-authenticator-protocol-v2.0-ps-20170927.html

[14]. Schläpfer, T., & Rüst, A. (2019). Security on IoT devices with secure elements. In Embedded World Conference, Nuremberg, Germany, 26-28 Februar 2019. WEKA.

[15]. Tomlinson, A. (2017). Introduction to the TPM. Smart Cards, Tokens, Security and Applications, 173-191.

[16]. Sabt, M., Achemlal, M., & Bouabdallah, A. (2015, August). Trusted execution environment: What it is, and what it is not. In 2015 IEEE Trustcom/BigDataSE/Ispa (Vol. 1, pp. 57-64). IEEE.

[17]. Mavrovouniotis, S., & Ganley, M. (2013). Hardware security modules. In Secure Smart Embedded Devices, Platforms and Applications (pp. 383-405). New York, NY: Springer New York.

[18]. S. C. Sethuraman, A. Mitra, G. Galada, A. Ghosh and S. Anitha, "Metakey: A Novel and Seamless Passwordless Multifactor Authentication for Metaverse," 2022 IEEE International Symposium on Smart Electronic Systems (iSES), Warangal, India, 2022, pp. 662-664, doi: 10.1109/iSES54909.2022.00148.

[19]. S. Chakkaravarthy Sethuraman, A. Mitra, K. -C. Li, A. Ghosh, M. Gopinath and N. Sukhija, "Loki: A Physical Security Key Compatible IoT Based Lock for Protecting Physical Assets," in IEEE Access, vol. 10, pp. 112721-112730, 2022, doi: 10.1109/ACCESS.2022.3216665.