Enhancing FIDO Transaction Confirmation with Structured Data Formats

Andre Büttner and Nils Gruschka

University of Oslo, Gaustadalléen 23B, 0373 Oslo, Norway
{andrbut,nilsgrus}@ifi.uio.no

Abstract. FIDO Transaction Confirmation is an extension for the FIDO authentication protocols to enable the verification and signing of digital transactions, e.g., for online banking. The standard currently considers only to include a transaction message text in the assertion which is signed by the user's authenticator. However, this is not useful for more complex transactions and leaves room for ambiguities that might lead to security vulnerabilities. Therefore, we propose to include the transaction information to the FIDO protocols in a structured data format with a strictly defined schema to validate and sign transactions more reliably and securely.

Keywords: FIDO · Transactions · Security

1 Introduction

In recent years, passwords have proven to be not secure enough to withstand attacks, such as phishing, brute-forcing, or other means of compromise [3]. As a consequence, two-factor and multi-factor authentication have been introduced to make authentication more secure [1]. The FIDO Alliance has proposed protocols for using authenticators as an additional factor and even as a passwordless solution. An important extension to these protocols is the *Transaction Confirmation* [2], which allows users to confirm online transactions using a FIDO authenticator. A relying party can include a transaction message or an image to an assertion request, which is displayed to the user and signed by the authenticator. However, research has already shown that it is possible to trick a user into approving a malicious transaction when there is no secure display [9,10].

Further, since the transaction is only represented as a text string or an image without clearly defined semantics, the transaction information leaves room for ambiguities. Therefore, the desirable *What-You-See-Is-What-You-Sign* [7] property is not sufficiently fulfilled. It would be more reliable to use a structured data format that contains a well-formed and self-describing representation of a transaction [4,6]. The contribution of this paper is, therefore, a proposal and discussion on the use of structured data formats for FIDO Transaction Confirmation.

The remainder of this paper is structured as follows. In Section 2, some background on FIDO Transaction Confirmation is provided. Our proposed enhancement for the FIDO transaction extension is described in Section 3. Section

Author version of a paper accepted for NISK 2021.
The original publication is available at https://ojs.bibsys.no/index.php/NIK/article/view/965

4 discusses the advantages and disadvantages of our approach. Finally, in Section 5, our findings are concluded, and suggestions on future work are given.

2 FIDO Transaction Confirmation

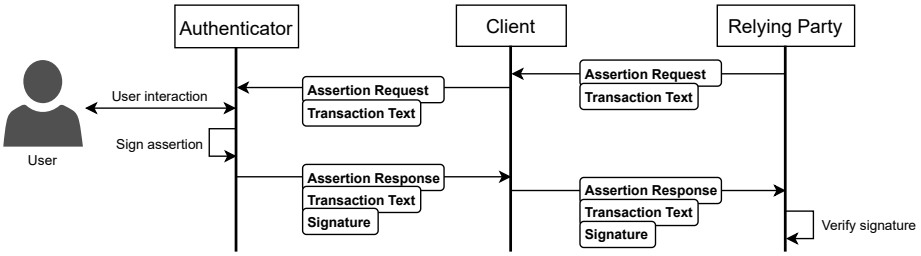

Fig. 1. Transaction Confirmation flow diagram showing the different processing steps.

The FIDO UAF and FIDO2/WebAuthn protocols are based on a challenge-response protocol, where an authenticator, e.g., a smartphone, hardware token, or platform authenticator, registers with a public key against a relying party. For authentication, the authenticator needs to sign a random challenge to proof possession of the corresponding private key.

Transaction Confirmation as an extension of these protocols seeks for "a standardized and secure way of gathering explicit user consent for a specific action" [2]. Consent is based on the user's interaction with the respective authenticator to confirm that he has seen and approved the transaction message. This allows the use of FIDO authenticators for carrying out bank transactions, online purchases, granting access to certain information, and more.

Fig. 1 gives an overview of how a transaction is processed with the FIDO protocols. The relying party sends a FIDO assertion request to the client, which contains a human-readable representation of a transaction in form of a simple text. The user confirms the transaction by interacting with the authenticator. Afterwards, the authenticator creates the assertion response along with the signature created with the corresponding private key. The assertion response is then returned via the client application to the relying party, which finally verifies the signature and executes the requested transaction [5].

3 Structured Data for Transactions

Instead of just plain text, we propose to use a machine-readable representation of a transaction that is converted into a human-readable text by the client or authenticator. One common data format for structured data is the Extensible Markup Language (XML), which is typically defined and validated using the

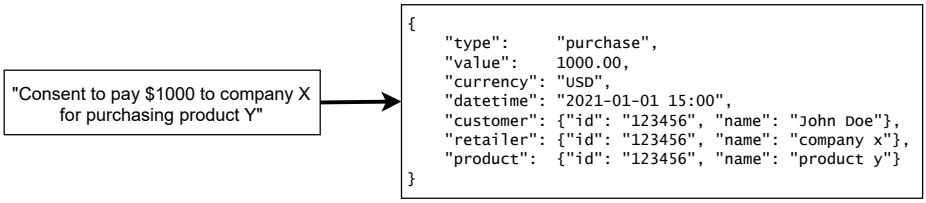

Fig. 2. Example transaction as plain text and structured data.

XML Schema Definition (XSD) language. Also, there are respective W3C standards for signature generation and encryption.

The data formats used in the FIDO protocols are JavaScript Object Notation (JSON) and its binary counterpart, Concise Binary Object Representation (CBOR). FIDO extensions are expected to be in the CBOR format. Thus, we consider this data format to be most suitable for transaction data structures as well. Similar to XSD, there already exists the Concise Data Definition Language (CDDL) which analogously enables the definition and validation of CBOR objects. Signatures, message authentication, and encryption are standardized in the CBOR Object Signing and Encryption (COSE) protocol. In Fig. 2 on the left-hand side, an example mentioned in [2] is shown. With our approach, this can be replaced by a semi-structured representation like presented on the right-hand side. Some information like identifiers and time were added, showing how transactions could easily be extended with relevant information. Also, validation and limitations on each of the attributes could be applied by the authenticator. Further aspects are discussed in the following section.

4 Discussion

Semi-structured data formats like XML, JSON, or CBOR provide properties like well-formedness and being self-describing with clear semantics [8]. This avoids ambiguities from unclear formulations, which is common for plain text. Further, for more complex types of transactions, it might be useful to display only relevant parts to the user before signing. This can be realized more easily with structured data if these parts are separate attributes inside the data structure, e.g., an account number inside a bank transaction. Also, structured data is machine-readable, which also enables to define policies for certain attributes. These can be validated by a client application or the authenticator using CDDL schemas.

FIDO transactions may be manipulated or eavesdropped through XSS or malware on the client. Therefore, it is reasonable to let the relying party sign [9] and encrypt the transaction data. If the CBOR format is used for transactions, the COSE protocol can provide a standardized way of ensuring both integrity and confidentiality on both ends.

An obvious disadvantage of using data structures for FIDO transactions is the complexity and its data overhead. This may especially be problematic for

hardware tokens with limited computation and storage resources. The authenticator would need to perform CDDL schema validation. Ideally, it should also support the COSE signature validation and decryption. Increased latency may be acceptable since registration and normal authentication would not be affected. In case it does not work on hardware tokens, the validation can be outsourced to the client application, however, reducing the security gain.

5 Conclusion and Future Work

The FIDO protocols are a promising step towards more secure authentication and a potential replacement for passwords. Transaction Confirmation is a good example of how these protocols support use cases beyond that. This paper addresses some shortcomings of this extension and proposes to use structured data instead of plain text. As discussed, our approach provides many opportunities, such as allowing an authenticator to validate transactions against policies and using standardized ways to ensure integrity and confidentiality.

In future work, we are planning to test the approach for different applications and different types of authenticators, analyze different attack scenarios, and evaluate the application of CDDL schemas and COSE signature and encryption.

References

1. Dasgupta, D., Roy, A., Nag, A.: Multi-Factor Authentication, pp. 185–233. Springer International Publishing, Cham (2017)
2. FIDO Alliance: FIDO Transaction Confirmation White Paper. Tech. rep. (August 2020), https://media.fidoalliance.org/wp-content/uploads/2020/08/FIDO-Alliance-Transaction-Confirmation-White-Paper-08-18-DM.pdf
3. Florêncio, D., Herley, C., Coskun, B.: Do strong web passwords accomplish anything? HotSec **7**(6), 159 (2007)
4. Gruschka, N., Reuter, F., Luttenberger, N.: Checking and signing xml documents on java smart cards. In: Quisquater, J.J., Paradinas, P., Deswarte, Y., El Kalam, A.A. (eds.) Smart Card Research and Advanced Applications VI. pp. 287–302. Springer US, Boston, MA (2004)
5. Hodges, J., Czeskis, A., Liao, H., Lindemann, R., Balfanz, D., Jones, J., Lundberg, E., Kumar, A., Jones, M.: Web authentication: An API for accessing public key credentials level 1. W3C recommendation, W3C (Mar 2019), https://www.w3.org/TR/2019/REC-webauthn-1-20190304/
6. Jøsang, A., AlFayyadh, B.: Robust wysiwys: A method for ensuring that what you see is what you sign. In: Proceedings of the Sixth Australasian Conference on Information Security - Volume 81. p. 53–58. AISC '08, Australian Computer Society, Inc., AUS (2008)
7. Landrock, P., Pedersen, T.: WYSIWYS?—What you see is what you sign? Information Security Technical Report **3**(2), 55–61 (1998)
8. Nenadi, A., Zhang, N.: Non-repudiation and fairness in electronic data exchange. In: Enterprise Information Systems V, pp. 286–293. Springer (2004)
9. Xu, P., Sun, R., Wang, W., Chen, T., Zheng, Y., Jin, H.: SDD: A trusted display of FIDO2 transaction confirmation without trusted execution environment. Future Generation Computer Systems **125**, 32–40 (2021)

10. Zhang, Y., Wang, X., Zhao, Z., Li, H.: Secure display for FIDO transaction confirmation. In: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. pp. 155–157 (2018)