Transaction Authorization with FIDO2

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Gerhard Hassenstein

FIDO2 provides simple yet strong user authentication based on public-key cryptography. But authentication might not be enough as sessions could get compromised. Transaction authorization is the state of the art to secure delicate operations. Is FIDO2 ready for this? Can FIDO2 facilitate transaction authorization in contexts of high-security requirements?

Introduction

Several major players of the computer industry united their forces in the FIDO Alliance to establish a common standard for strong and simple user authentication. In early 2019, FIDO2 was born. The standard was built extensible, with transaction authorization already in mind. On an authenticator device, equipped with a secure display, the user can verify the transaction details before confirming them with a cryptographic signature. However, to date, FIDO2 is only employed for user authentication. Hence, the transaction authorization extension was abandoned from the latest draft of the specification.

Objectives

This thesis scrutinizes FIDO2‘s simple transaction authorization extension. Is the extension implementable with the current specification? Is the specification complete and sound? How about the security of the extension?

Methods

The specifications are challenged through theoretical and practical analysis. While a proof of concept aims to implement the simple transaction authorization extension, it reveals some of its weaknesses and shortcomings. An existing authenticator is extended with a trusted display so the user can verify the transaction details. A theoretical, attack driven examination assesses the security.

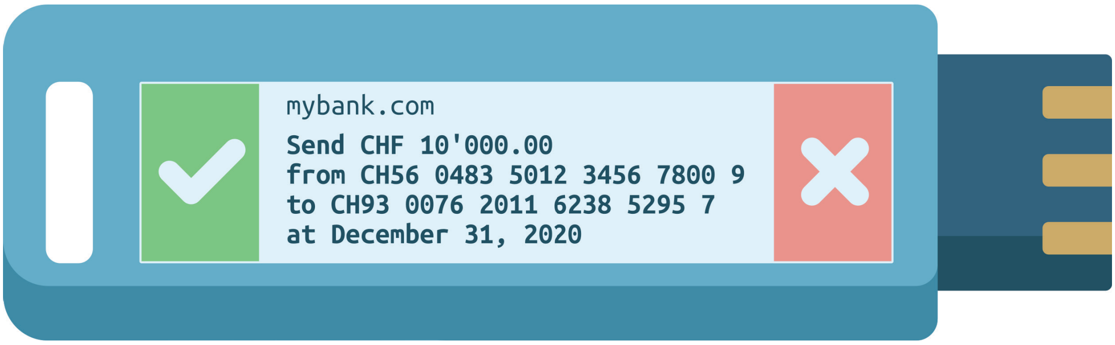
Results

The specification lacks crucial parts for the implementation of the simple transaction authorization extension. The extension is defined only for the server-side (WebAuthn) but missing in the standard of the authenticator‘s protocol (CTAP2). Substantial points like the maximum length of the transaction details as well as rules to detect hardware errors of the secure display are missing. The security meets the goals specified by the FIDO Alliance. However, there is still room for improvement, especially concerning the confidentiality of the transaction details. In relation to the non-repudiation property, the registration process must be defined precisely in order to protect the user from dishonest service providers. If a transaction authorization may be judged secure even without prior user authentication, is shown to be solely a matter of the user authentication method.

Conclusion

The potential of a secure, simple, and uniform transaction authorization mechanism is enormous, and technically, FIDO2 could fill the gap. However, an extra effort is needed to complete the extension‘s specification and push it back into the standard.

Cyrill Alexander Bolliger
mail@cyrill.me



mybank.com
Send CHF 10'000.00
from CH56 0483 5012 3456 7800 9
to CH93 0076 2011 6238 5295 7
at December 31, 2020

Transaction authorization on a FIDO token