Clavertus - FIDO Authenticator for Android

Degree programme: BSc in Computer Science
Thesis advisor: Prof. Dr. Benjamin Fehrensen
Expert: Dr. Alain Hiltgen (UBS Business Solutions AG)

Passwordless authentication using public-key cryptography is becoming increasingly popular, raising important questions about where keys are stored. With Clavertus we demonstrate how a smartphone can be used for key storage. Clavertus is an open source FIDO authenticator for Android that follows the Client to Authenticator Protocol (CTAP 2.2) specifications. It uses an encrypted tunnel service to communicate with the client and Bluetooth Low Energy to verify proximity.

Overview

Passwordless authentication based on the FIDO2 (WebAuthn + CTAP 2.2) standard is becoming more popular. While this solution offers higher security and resistance to phishing, it requires a more complex infrastructure than traditional passwords. For key management, hardware tokens are an option but require purchase. Using smartphones could simplify the process, as most people already own one. However, proprietary solutions from major tech companies lead to platform lock-in, restricting flexibility and data ownership.

Goal

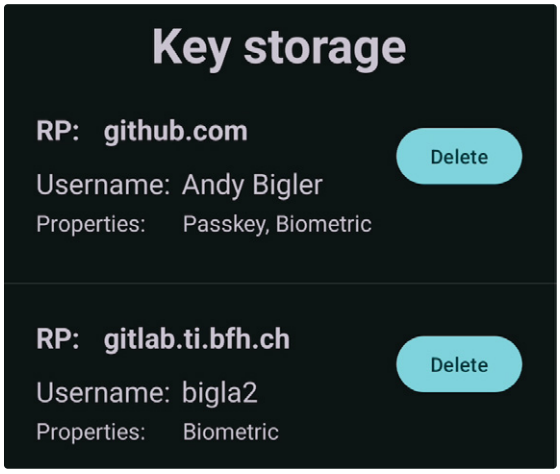
Our goal was to develop an Android application that functions as a FIDO2 authenticator. The app must securely generate and store cryptographic keys directly on the user's device and requires a communication interface to be usable. We wanted to implement the new hybrid transport flow, which, to our knowledge, would be the first open source implementation for Android. This flow involves network communication through an encrypted tunnel service and Bluetooth Low Energy advertisements to confirm proximity, allowing the authenticator to connect to client platforms.

Result

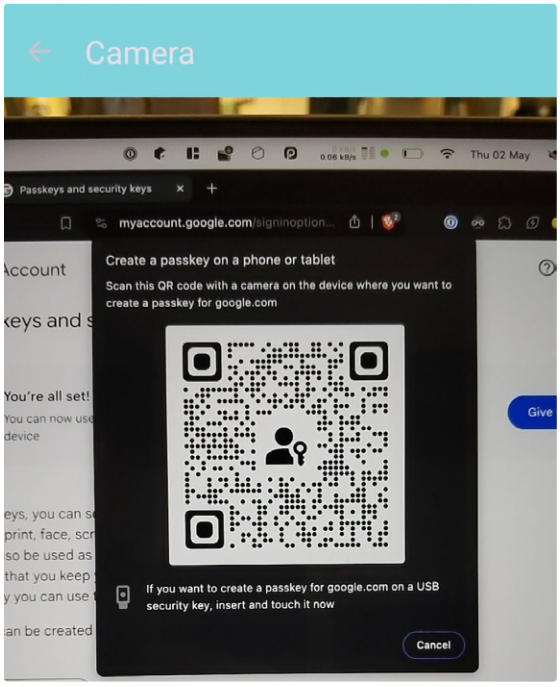
We could build a FIDO2 authenticator app that supports all essential functions to make it usable. This thesis thoroughly explored the idiosyncratic interpretation of the CTAP protocol, leading to the exclusion of authenticators or losing device attestation.

Future

To drive adoption and trust, public awareness and understanding of passwordless authentication technologies must increase. The ecosystem must be open and give users complete control over their data. Multiple opportunities exist to build on this foundation via extensions, such as implementing protected confirmation or selective disclosure.
https://github.com/Clavertus-Authenticator



List available keys with properties



QR code scanning to setup a tunnel

Andy Bigler
IT Security
andy@eyou.ch

Lars Hostettler
IT Security
lars.hostettler@pm.me