NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

APRIL 2022 | #33

The VAULT

FIDO & AUTHENTICATION TECHNOLOGIES

FEATURED ARTICLE

Delegated Authentication – Abandon friction, not the cart
FIDO Alliance

ALSO IN THIS ISSUE

Mühlbauer Group
Close-up on a passport's heart

Infineon Technologies
FIDO –Secure authentication with bite!

FIDO Alliance
SMS authentication is bad (what to do instead)

authenton – an AIXecutive Company
authenton#1 – the secure multi-purpose authentication token

cryptovision
Enhancing eID documents with FIDO authentication

TrustSEC
PKI and FIDO2 – the perfect match

Our eID solutions* are flexible, secure, certified. So you can do things just the way you want. Our Government ID experts and our global network of qualified partners will lead the way. Find out more on **cryptovision.com/eID**

*Java Card™ Applet Suite | Personalization | Middleware | Certificate Management

Enhancing eID DOCUMENTS with FIDO *AUTHENTICATION*

By Klaus Schmeh and Mikhail Gordeev, cryptovision (an Atos company)

FIDO authentication has become a popular solution for secure authentication on the internet. Electronic identity documents can be used for the same purpose. However, the two technologies, though both based on asymmetric cryptography, follow different concepts: While FIDO authentication implements an anonymous client-server-based approach, eID documents are inherently tied to a personal identity and based on the more general concept of a Public Key Infrastructure (PKI). Nevertheless, combining FIDO and eID technology is possible and makes sense.

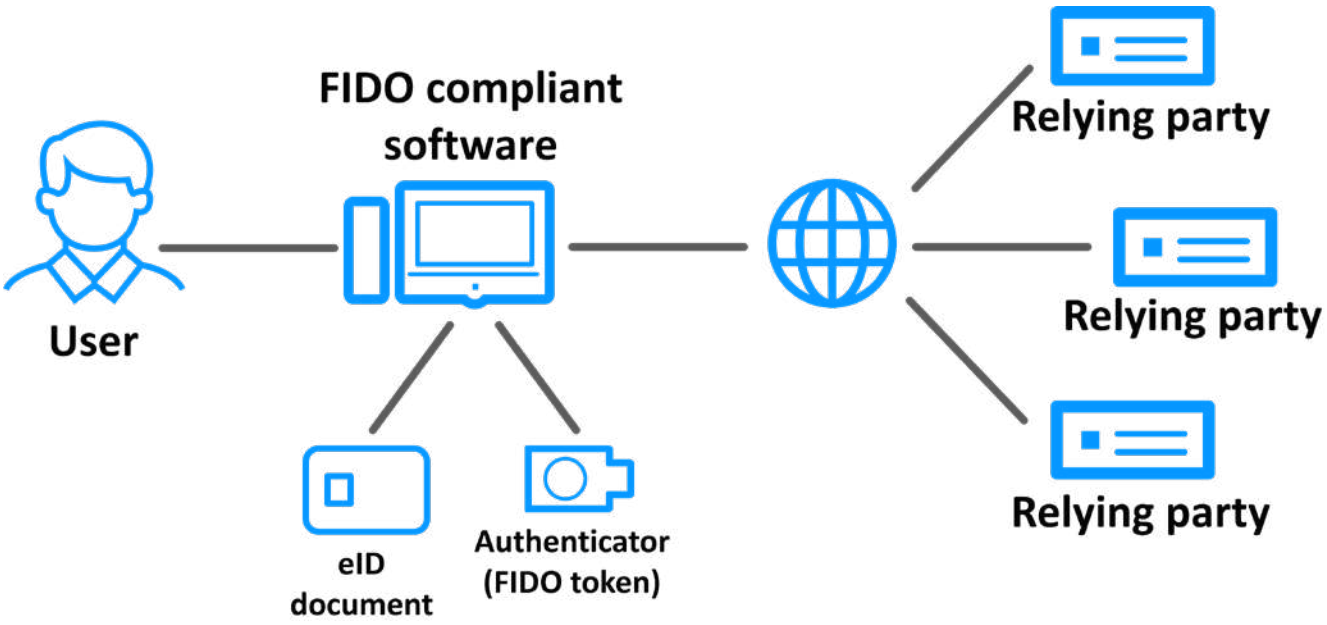
☐ FIDO authentication

You authenticate with what you know, what you have or what you are. This simple principle has been known among IT security experts at least since the 1990s. However, decades later, there are still two major short-comings when it comes to online authentication: First, the by far most popular method is still "what you know", although the drawbacks of passwords and PINs have long been known; and second, most authentication systems are still isolated solutions, which results in a typical user having to memorize dozens of secret access codes.

To solve this problem, the FIDO Alliance was founded. The goal of this organisation is to establish interoperable, token-based authentication in the online world. For this purpose, the FIDO Alliance has created a challenge-response authentication protocol as well as an authentication device specification with different form factors, known as "authenticator" or "FIDO token". Meanwhile, numerous governments and enterprises around the world are recognizing and deploying the FIDO scheme, making it a de-facto standard for advanced online authentication.

The FIDO approach to authentication is based on asymmetric cryptography. A user can securely authenticate to online services (referred to as "relying parties") that support the FIDO standard. For this purpose, they need an authenticator and FIDO compliant software, such as an internet browser. For initialisation, the user registers their token at a particular relying party. This requires that trust has been previously established, for instance by a verification link sent from the relying party to the user by email. For every relying party, a different private/public key pair is generated, which grants that a user has different identities at different servers with no possibility to match these.

Source: Tony Webster, Wikimedia Commons
When it comes to online authentication, FIDO tokens, which have been created to replace passwords with a more secure technology, represent an attractive alternative to PKI-based eID documents.



A FIDO user can authenticate to relying parties that support the FIDO standard. A PKI-based eID document can serve as the foundation of the initial registration process.

FIDO and eID: Two different philosophies

Of course, the FIDO scheme is not the only technology that has been put forward to solve the authentication problem. Another one is represented by electronic identity documents. Although there are many different designs, varying from country to country, eID documents usually provide a private key that can be used for online authentication. Authenticity is established via a Public Key Infrastructure (PKI), which means that each key pair is connected to a digital certificate.

While a FIDO token and an eID card both implement authentication based on asymmetric cryptography, the concepts underlying them are different. FIDO authentication is targeted for a client authenticating against a server. eID documents, on the other hand, are made to support more general peer-to-peer scenarios. While it is an important goal of the FIDO specifications to establish a different anonymous identity for every service, an eID document is generally designed for representing one identity.

For FIDO tokens, authentication is the only use case, while the private keys on eID cards can also be used for digital signatures or even encryption.

FIDO authentication is especially popular in a number of countries not issuing national electronic identity documents, such as the USA and the United Kingdom. On the other hand, the FIDO Alliance website lists government deployments and recognitions in countries like Malaysia and Hong Kong, which have issued electronic identity documents to their citizens. Some users even have to bother with two kinds of tokens.

Bringing the two approaches together

In spite of all differences, there are interesting approaches to combine FIDO and eID technology. Especially, it appears attractive to use an eID card as a FIDO authenticator. This means that the standard identification functions of an eID card are complemented with a privacy-by-design authentication feature.

> *The FIDO authentication schemes profit from the already established trust provided by an eID system.*
>
> *– Ben Drisch, cryptovision (an Atos company)*

Several initiatives aiming to achieve such an integration have been started. For instance, the FIDO Alliance and the Asia PKI Consortium have published a common white paper on how the two approaches can be connected. In Europe, there are activities with the goal to combine FIDO with the electronic signature directive eIDAS.

However, using an eID card as a FIDO token is far from a no-brainer. "The different nature of the two technologies makes it difficult to employ the same private key for FIDO and eID authentication", explains cryptovision's Ben Drisch. "This is because FIDO keys are created separately and anonymously for each server, while eIDs typically use one key for authentication-related purposes."

The simplest schemes implement FIDO and eID functions on the same document, but with separate infrastructures. In more advanced systems, enrolment and other processes are synchronized. There are even specifications that use the same key for both technologies, though this requires an additional layer of sophistication.

A more pragmatic approach is to use the eID and its infrastructure to register a user at the relying party – a procedure that is, of course, much more secure than a confirmation link sent by email. Says Ben Drisch: "In such a scenario, the FIDO scheme profits from the already established trust provided by an eID system. eID enrolment and FIDO registration need not take place at the same time."

Activities aiming to integrate FIDO and eID systems are still at an early stage. The urge for secure and standardized online-authentication will certainly further push the use of the FIDO standard. The need for secure initial registration at a relying party might bring eID documents into play. On the other hand, support of FIDO registration makes eID documents more attractive by adding functionality that is relevant in the online world. In any case, it can be said: FIDO represents a natural enhancement to eID documents that supports their multi-purpose use in online environments. ☒