A Proposal to Use Hardware Tokens for Web Authentication

Ullrich Martini, Giesecke & Devrient, ullrich.martini@gi-de.com

This paper proposes a specific implementation of the FIDO protocol for use in those web authentication purpose where values are protected, like in e-Commerce transactions for example. It is fully within the scope of the FIDO protocol.

A very specific subtopic of identity management is addressed here: How to connect a virtual identity to a real identity with a street address and a bank account? Of course, there are many cases where such a close relation is undesirable. However, whoever tries to run an e-Commerce business over the internet will be target of online fraud sooner or later. The purpose of this paper is to suggest how this connection could be created.

A related proposal [1] has been submiited. This proposal gives more details of one possible implementation of using FIDO for Web authentication.

Why FIDO and Digital Signatures?

The complexity of standard e-commerce solutions shows that it is difficult to transfer offline systems to the online world. One prominent example for this is PCI-DSS, a framework to protect credit card data, which is effective with respect to “Chip-and-PIN” payment cards, but puts a huge burden on e-Commerce services that have to protect the credit card data from of transactions they have performed.

The FIDO alliance [2] suggests a protocol [3] that can be used to authenticate a person, display the contents of a transaction to this person, obtain the approval of that person and finally formulate this approval as a digital signature on this transaction.

The e-commerce operator mentioned above will verify this signature and proceed with his or her activity. Using digital certificates the e-commerce operator may also verify that signature was indeed created by the user and device that is claimed in the digital signature.

There are two properties of digital signatures which are very relevant in this context:

1. Non-Reputability: The receiver has proof that the transaction was approved
2. No global secrets: There is limited damage if data is stolen from e-Commerce services.

Using FIDO on smartcards helps to achieve these objectives.

Why Smartcards?

A digital signature refers to a piece of secret data, the private key of the key pair. This private key must be protected against theft and misuse. A smart card will perform the following procedure:

1. Authenticate the user via biometrics via on-card-matching or a PIN. Any user authentication will profit from the fact that the smartcard can limit the number of authentication attempts. This relieves the user from memorizing complex passwords or changing them frequently.
2. Sign the transaction internally without revealing the private key to anyone. Because the smartcard uses technical countermeasures against leakage of the key or cloning of the whole card the owner remains in possession of the private of the key as long as he doesn’t lose the card

These two steps are a standard procedure for modern smartcards and form the basis for a reliable online transaction.

A SIM card is a special example of a smartcard, where functionality has been added to allow access to a mobile phone network. Not all SIM cards support digital signatures, therefor this proposal refers to advanced SIM cards that can be used to implement the FIDO protocol.

Why Mobile Phones?

Mobile phones contain two important ingredients:

1. A hardware security token, namely the SIM card
2. A user interface that can be used to obtain the user approval for a transaction.

In addition to the SIM card a mobile phone may contain more secure elements: an embedded secure element, a trusted execution environment , a virtualization environment or a pure software security solution. All of these can be used if the strong connection between a person and a SIM card is not necessary or even not desired.

Installing the solution as an app on a smartphone circumvents all security and compatibility issues that might arise if the solution is installed into a browser on a personal computer. The integration of the authentication protocol into HTML5 is certainly desirable and would be fully in line with this proposal, but out of its scope.

How to Roll Out?

The mobile network operators (MNOs) issue subscriber identity module (SIM) cards to their customers. If the SIM card uses a JavaCard™ OS [4] the MNO or someone authorized by the MNO can remotely install and configure additional applications on the SIM card. Such an application would implement the relevant parts of the FIDO protocol, the user authentication and the digital signature. Customers of the MNO may then ask for that functionality and have it remotely installed and personalized. The remote management tools which are required here are readily available from the NFC ecosystem.

Using a standard protocol like FIDO solves a great market introduction challenge: How does a new solution survive the phase where it is still small and growing? The e-commerce operators only need to implement FIDO . They can use it with different security levels at the same time and utilize the technical strength of a digital signature in their risk management system.

[1] Strong Authentication In and Beyond the Browser, propodsal to the W3C Workshop on Authentication, Hardware Tokens and Beyond

[2] Fido alliance https://fidoalliance.org/

[3] Fido UAF https://fidoalliance.org/specs/fido-uaf-v1.0-rd-20140209.zip

[4] JavaCard™ http://www.oracle.com/technetwork/java/embedded/javacard/overview/index.html