Possibilities for Hardware Tokens in the Web

Richard Barnes, Mozilla

What are we trying to do?

Lots of people are proposing support for various tokens

What function are these proposals trying to realize?

- Crypto acceleration?
- Identity?

Whatever API we build should be function-specific, not platform-specific

Let’s look at identity*…

* since WebCrypto was born out of Web Identity, after all

Passwords are Bad

All the identity system cathedrals today are built the sandy foundation of passwords

Prominent breaches of password data provide frequent reminders of the risks that passwords pose

We need a non-password authenticator for the Web

Point Solutions are Also Bad

Lots of point solutions in this space

- Persona, OpenID, OAuth, …
- Smart Cards*, SIM Cards, FIDO, …

There is no common, universally-agreed identity protocol

Implementing point solutions is not good for the web architecture

A General API could be Good

Whatever we add to the web API needs to be:

1. general enough not to be tied to a specific identity system, and
2. capable of plugging in specific solutions

Some prior art: WebRTC, EME, PKCS#11

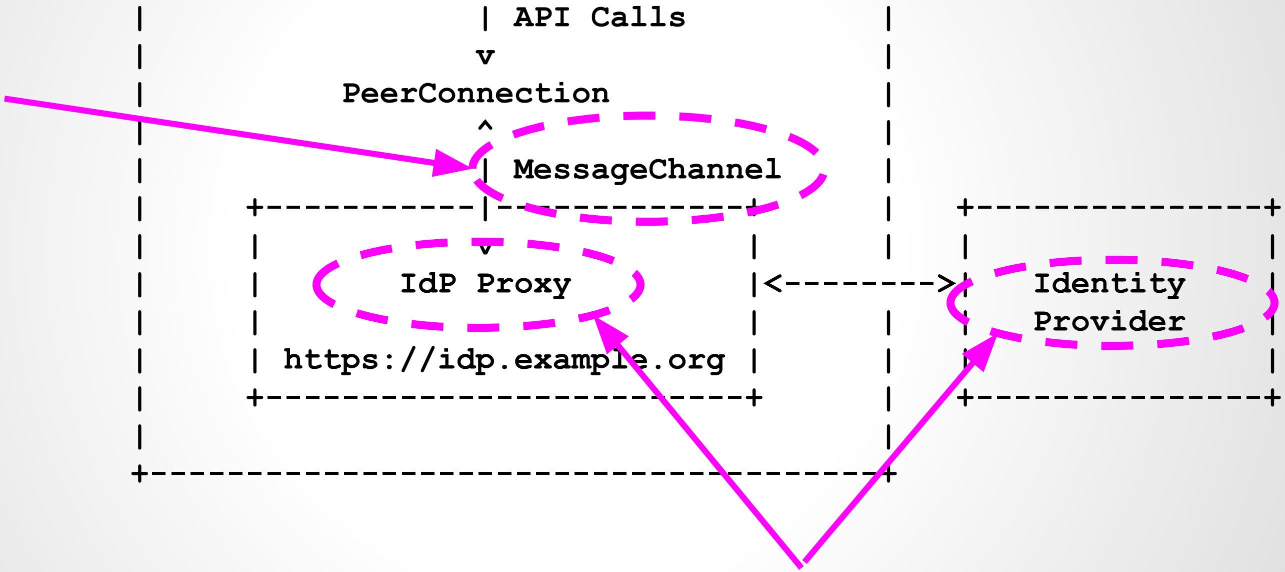
Build a box with a standard interface to contain the specifics

Just need to agree on what the API to the box is

WebRTC is a Positive Example

```
|                 | API Calls          |
|                 v                    |
|          PeerConnection              |
|                 ^                    |
|                 | MessageChannel     |
|     +-----------|-------------+      |   +---------------+
|     |           v             |      |   |               |
|     |       IdP Proxy         |<-------->|   Identity    |
|     |                         |      |   |   Provider    |
|     | https://idp.example.org |      |   |               |
|     +-------------------------+      |   +---------------+
|                                      |
+--------------------------------------+
```

WebRTC is a Positive Example



```
|                 | API Calls          |
|                 v                    |
|          PeerConnection              |
|                 ^                    |
|                 | MessageChannel     |
|     +-----------|-------------+      |   +---------------+
|     |           v             |      |   |               |
|     |       IdP Proxy         |<--------->|   Identity    |
|     |                         |      |   |   Provider    |
|     | https://idp.example.org |      |   |               |
|     +-------------------------+      |   +---------------+
|                                      |
+--------------------------------------+
```

GENERAL
IDENTITY API

INSERT SPECIFIC
SOLUTION HERE

From this implementor’s perspective

Discussing a “SIM API” or a “smart card API” or a “FIDO API” is not useful

Let’s talk about the **function** we’re trying to achieve, instead of the various **implementations** of that function

Make an box that implementations can go in, and make an API for the box