Making Client Certificate Authentication Usable

Although HTTPS CCA (Client Certificate Authentication) is available in every browser the limited usability of this scheme has made it quite impopular.

The primary issues with the existing system are:

- Incompatibility with the established web session model including lack of logout
- Quirky UI
- Missing certificate selection mechanism adapted for W3C's WebID-TLS

This presentation describes a system which has some similarities to FIDO Alliance's U2F but is targeted for traditional (and often already deployed) PKI.

The core is a JSON-based challenge-response protocol running on top of a server-authenticated HTTPS connection. That is, there is no need to change TLS in any way.

The scheme outlined here is by no means new; it is rather a "compilation" of a number proprietary browser plugins which are in active use since at least a decade back.

Doing a genuine browser-implementation should not be particularly challenging since the original HTTPS CCA trust and privacy model is essentially kept untouched.

A more detailed description can be found here:
http://webpki.org/papers/PKI/webauth.pdf

A proof-of-concept system for public testing is available at:
https://play.google.com/store/apps/details?id=org.webpki.mobile.android

Anders Rundgren
WebPKI.org

anders.rundgren.net@gmail.com

Montpellier, France, 2014-07-13