National eIDs and the Open Web Platform

John Mattsson, Vladimir Katardjiev, Ericsson Research

Abstract. W3C should strive to make identity and authentication part of the Open Web Platform and standardize developer friendly interfaces for web application interaction with national eID systems, and integration between different eID systems. It is also important that eID solutions work well on mobile devices and browsers. The Web community has largely made plug-in for games, audio, video, and real time communication obsolete. Working on open standards to abolish plugins for secure identification and authentication is the logical next step.

1. Background

There is a massive development and deployment of electronic ID (eID) solutions the world over. The trend is driven by a desire for heightened security as well as increasing the convenience for citizens by allowing them to more easily access government systems such as electronic voting and social security systems. A functional and secure eID system is fundamental for the development of the Internet economy, and increases the efficiency of the society as a whole.

However, the market potential for eID is held back by fragmentation, as basically every country uses a national solution without compatibility with other systems. This causes problems as end users can only authenticate to web applications in the same country, and web applications can only authenticate end users from that country. Technically, most solutions use PKI, but some use smart cards for certificate storage and processing, while other use software processing and password protected storage. Smart cards implementations can further be divided into credit card sized cards and implementations on SIM cards, so called Mobile PKI. Since the user is not dependent on a computer or card reader, Mobile PKI schemes has the possibility to further ease the adoption of eIDs [3].

Another problem is that all of these solutions make use of plugins and third party applications in one way or another, leading to solutions that are not developer-friendly, and experiences that are not user-friendly. Apart from the initial effort to install all needed software and hardware, and the frequent need to update these plugins, the end user is disturbed by the requirement to switch from the browser to a native application window that may not even show up before the user has clicked “allow” in a warning notification.

The reliance on plugins means that the eID solutions are often only available for certain browsers, operating systems, and architectures. Mobile browsers and operating systems is often not supported at all. Plugins and native APIs (such as ActiveX, Flash, and Java) have traditionally been very successful attack vectors, diminishing the public trust in browser security as a whole. There is no reason to believe that the proprietary eID plugins are different.

An interesting example is the Korean eID system [1]. In some aspects, it is very successful; Korea is ranked as world leader in ICT Development and e-government, much to the development of a secure and reliable eID system. Technically, the Korean eID system is however not a role model; it is built on proprietary crypto algorithms and ActiveX, forcing users to not only install several separate add-ons, but also forcing users to use Internet Explorer, which still has a near monopoly in Korea. The lack of compatibility, especially with mobile operating systems is currently stirring up controversy in Korea.

Another example is the situation in the European Union [2]. While EU is an economic union with a single market, it still has national (non-interoperable) eID systems [3]. EU has started a project [4] to enable interoperability of different approaches and solutions among the European countries, realizing a single European electronic identification and authentication area.

Electronic ID and signature interoperability encompasses both technical and legal difficulties. A single global solution for high security identification and authentication to government systems such as electronic voting and social services may not be possible due to political and national security concerns. Nations will definitely want to control their own certification authority and the certificate enrollment, and some counties may want to use their own crypto algorithms, but apart from that, much of the APIs and protocols could likely be standardized. Governmental web applications such as e-voting will still have the choice of not accepting certificates and signatures from other countries, while e-commerce and financial applications likely will.

The certificates in current eID solutions are mostly or only used for signing, either for authentication or authorization. This is a missed opportunity, as the systems could just as well be used for encryption, protecting end user confidentiality in e.g. secure email. Even if some governments would not welcome high-security solutions to protect end user confidentiality and privacy, W3C and the Internet community should embrace this and strive to make it happen.

2. Way Forward

The weaknesses with passwords are well known, it's time to move "beyond passwords", not only for high-value environments such as the financial industry and government, but for all types of web applications. To meet the demands from the industry sectors with high security demands as well as ordinary web developers, W3C should strive to make identity and authentication part of the Open Web Platform.

W3C should work on aligning and harmonizing various government projects and standardize developer friendly interfaces for web application interaction with national eID systems, and integration between different eID systems. Authentication needs to be done in a secure, developer-friendly, and user-friendly way. Even small startups should be able to easily use the eID systems for new business ideas.

It is important that essential eID systems are available on as many architectures, operating systems, and browsers as possible. As more and more browsing is done from mobile devices and many people in developing countries only have access to mobile browsers, it is equally important that eID solutions also work well on mobile devices and browsers. The number of mobile broadband subscriptions is currently over 2.3 billion and is predicted to rise to 7.6 billions by 2019 [5].

Interaction with, and the need of, various forms of plug-ins has been an ongoing problem (security, interoperability, and user experience) for the Open Web Platform and W3C. By introducing open standards such as HTML5, WebRTC, and WebGL, the Web community has largely made plug-in for games, audio, video, and real time communication obsolete. Working on open standards to abolish plugins for secure identification and authentication is the logical next step.

A standardized API for interaction with eID systems should enable not only signing, but also encryption, protecting end user confidentiality and privacy. Even if some governments would not welcome this, W3C and the Internet community should strive to make this happen.

To summarize, W3C Should:

- Make identity and authentication part of the Open Web Platform.
- Continue work on the open identity and authentication initiatives.
- Strive for better browser integration with current and future National eID systems.
- Work on aligning and harmonize various eID systems and the integration between them.
- Make sure that eID solutions also work for mobile operating systems and browsers.
- Aim to make the certificates in eID systems usable for encryption as well as signatures.

References

[1] Dongoh Park, "Innovation Faded: Transition into Online ID system in Korea and Conflict in Global Ecosystem", GLOBELICS Academy, 2013
http://www.globelicsacademy.net/2013_pdf/Full%20papers/Park%20full%20paper.pdf

[2] European Commission, Joint Research Centre, "Electronic Identity in Europe: Legal Challenges and Future Perspectives (e-ID 2020)", 2013
ftp://s-jrcsvqpx102p.jrc.es/pub/EURdoc/EURdoc/JRC78200.pdf

[3] UL Transaction Security, "Electronic Identities in Europe", 2013
http://www.ul-ts.com/downloads/whitepapers/finish/6-whitepapers/114-electronic-identities-in-europe

[4] STORK 2.0 (Secure identity across borders linked)
https://www.eid-stork2.eu/

[5] Ericsson, "Ericsson Mobility Report", June 2014
http://www.ericsson.com/ericsson-mobility-report