Why W3C needs to Remain Neutral and Endorse 'Brand-free' Hardware Security

Drew Thomas, Stephen Wilcox, Pradeep HR, Nizar Jamal, Siva Narendra
Tyfone, Inc.

Abstract

This position paper provides an overview for web integration of smart card secure element chip technology enabling hardware token for strong ID (NIST Level 4) authentication and layered transaction security for applications. The maturity of the smart card chip technology – from market size and breadth, leveraging existing standards, and certification – implies that smart card technology should be the most obvious hardware security component of choice for integrating with next generation user experience and security standards for the World Wide Web.

Smart Card Chip Technology and Myths

A smart card chip is an integrated circuit that includes an embedded secure microcontroller and supports communication via direct electrical contact (ISO/IEC 7816) and/or a contactless radio frequency interface (ISO 14443). With a secure microcontroller, smart cards have the unique ability to securely store large amounts of data and key material, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with computers, mobile phones, and other readers. Smart card technology conforms to various international standards such as ISO. Industry specifications also govern the use of smart card technology for industry specific applications such as EMV.

The term, "smart card," is something of a misnomer. While the plastic card was the initial smart card form factor, smart card technology is now available in a wide variety of form factors, including plastic cards, key fobs, subscriber identification modules (SIMs) used in mobile phones, watches, electronic passports and USB-based tokens.

Contrary to some beliefs:

- Smart card chips are not "old" technology. Instead smart cards are rooted in well-defined standards and evolve through various industry bodies to keeps pace with the practice of Moore's Law.
- Smart card chips are not proprietary. Certified Smart card chips must follow various rigorous international standards (see position paper submitted by Smart Card Alliance). These erroneous opinions on smart cards being proprietary must have come about because many current integrations to web applications have been implemented in the absence of web standards, thereby further supporting the need for such standards.

Absence of 'Brand-free' Web Integration Standards

The current working group's charter explicitly states that "the provisioning of keys in particular types of key storage, such as secure elements or smart cards" is out of scope. While this may have been a practical decision to limit the scope of the working group to a manageable amount of work for the initial version of the API, it is not a viable long-term position and defers a critical standard absolutely necessary for the ecosystem to mitigate security risks.

It is critical that browsers have a standardized method for interacting with these type of hardware tokens. New hardware token standards such as FIDO™ U2F could likely benefit from the use of smart cards as its core security. We recommend that W3C consider supporting a wide array of possible smart

card based technologies, rather than supporting a specific 'branded' new hardware standard which is lacking a global and proven infrastructure and will require significant investment and adoption before it can be widely manufactured and deployed.

Smart card based technologies already support or follow a wide array of standards such as PC/SC, Global Platform, ASSD, smartSD, Java Card, EMV, CAC/PIV, PKCS, and FIPS, just to name a few. There is not yet a standard for consistently and seamlessly integrating web technology to smart card technology, so that the benefits of these two ubiquitous infrastructure can be leveraged by the entire ecosystem. We propose that the W3C define such a standard either in the Web Crypto API WG or in a separate WG.

Applications of Smart Card Chip Technology

Multi-factor authentication is one of the stated use cases supporting the definition of the current Web Crypto API. Smart cards chips are a proven, well-accepted mechanism for securely storing authentication material as well as sensitive key material. This secure storage enhances several applications such as strong authentication (including multi-factor and mutually authenticated TLS connection), digital signatures, data encryption (including DAR/VPN/VoIP), key protection, remote provisioning, and Web RTC.

As browsers have become the point of entry for enterprise and consumer applications in all devices, including mobile phones and tablets, web standards must support a wide variety of applications by developing general standards instead of narrow support. Figure 1 shows the difference between the narrow approach and the broader approach.

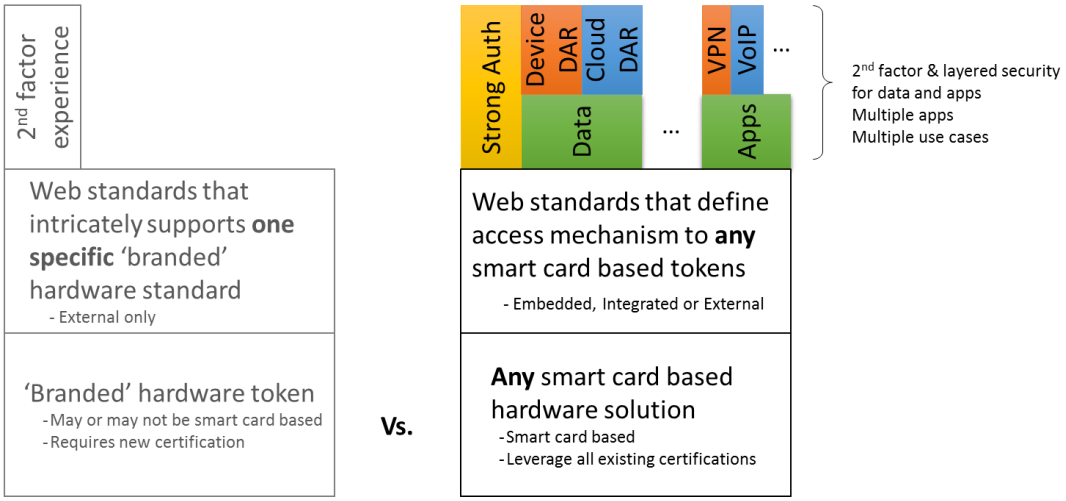

Figure 1. Comparing the limited use of the "branded" hardware token vs. general purpose smart card based hardware solution.

A Working Example of Smart Card Chip Technology Integrated with Firefox

Browser support for smart card-based authentication is available today. As an example of what is possible with existing browser capabilities, we can already demonstrate a smart card based hardware token integrated with off-the-shelf FireFox browser and Tomcat server.

The smart card based token stores client side certificates for strong authentication used to establish a mutually authentication TLS connection, with no need for a central Public Key Infrastructure. FireFox's Security Device Manager only requires the path to a PKCS #11 module. This module is loaded by Mozilla's Network Security Services library to enable FireFox to use credentials stored on the smart card chip contained in any hardware form factor. We will demonstrate at the workshop this Firefox solution on both Windows and Mac operating systems. As Firefox relies on PKCS #11 standard, smart card based cryptographic hardware from other vendors including Gemalto and Oberthur have leveraged such capabilities.

We encourage W3C to standardize such an implementation across all browsers that better leverages the benefits of smart card chip standards. Some recommendations to further enhance such an effort is covered in the next section.

Recommendations to W3C

Browser support for smart card-based authentication is available today and demand for it will increase once the Web Crypto API is released. This working group should recognize this growing demand and step ahead of the curve by establishing extensions and/or new APIs that support credential storage approaches other than the assumed IndexedDB implementation.

We strongly recommend that W3C support the enhancement of the existing Web Crypto API to implement the following concepts:

- Smart Card-backed keystore discovery and registration
- Addition and removal of Smart Card tokens
- Select active keystore
- Strive to be neutral and 'brand' free

Participant's Interest

Tyfone is a vendor of smart card based hardware security tokens. We encourage a 'brand-free' standardized interface be established that browsers and developers can use to interact with all types of smart card based secure cryptographic tokens. This standardization will benefit both the web community and the secure token development community.

About Tyfone

Tyfone is a pioneer in cyber and mobile security and transaction services for financial, government, B2B, healthcare, and other enterprises. It has more than 500 issued invention claims and has more than 90 issued and pending patents that enable ID and transaction security on any device. Tyfone's apps, transaction software and The Connected Smart Card™ (CSC™) security hardware enable ID and transaction security on any OS or device. The Company's platform solution has processed over 30 million transactions and has helped transact over $500 million. Tyfone customers include two of the top 10 member-owned financial institutions (Credit Unions) in the U.S. and the Company signed a strategic agreement with In-Q-Tel in 2012 to bring its mobile security solutions to the U.S. Government. Tyfone's corporate headquarters is located in Portland, Oregon.

Corresponding author contact information

siva.narendra@tyfone.com