W3C Workshop on Authentication, Hardware Tokens and Beyond

Intercede Position Paper

Contact: Peter.Cattaneo@Intercede.com

Introduction

Many of the uses of the web crypto API are linked to an identity. Intercede has been active for many years in building standards-based software and solutions for management of identities and associated credentials. These solutions carefully link identities in the physical world to directories, databases, physical access systems, and the cryptographic credentials used to access them.

The first area of engagement covered by this paper is ensuring that the existing world of centrally managed digital identities will be usable through the web crypto API. A common form for these credentials is a smart card used as a badge containing one or more digital certificates with associated private keys. There is real value in enabling the use of the credentials on these badges, carried by many government officials, corporate employees and some citizens, with the web crypto API.

We would also like to enable the emerging world of crypto-based user-managed identity. The logic is the same as for the centrally issued and managed credentials, just the source and control is different. In particular, the issues around the management of credentials, such as device replacement or migration, remain the same.

In both of these cases, the goal is to have a persistent identity, even as credentials with limited life spans are created, revoked and expire.

The web crypto API should gracefully work with a wide variety of crypto stores. The migration to mobile devices has changed the details as the employee badge or bank card disappears into one of the available secure areas. There are many options: UICC, NFC secure element, TPM, TEE, microSD, etc.

While it may be beyond the scope of this workshop, all of these issues will also be revisited in emerging contexts such as mobile to mobile interactions and IoT.

Intercede

For more than 15 years, Intercede has been a leading developer of identity and credential management software. As a U.K. company, Intercede delivers software in many countries and complies with a wide range of international standards. In the US, Intercede was the first provider of FIPS 201 compliant electronic personalization software that can enroll

identities and provision cryptographic credentials to smart cards to create a fully certified PIV or PIV-I card.

Intercede's MyID software creates, provisions, and manages symmetric keys, asymmetric keys, digital certificates and other cryptographic credentials. It also manages related biographic and biometric information used in the conjunction with the cryptographic keys. In addition to managing the credentials, MyID also interfaces with directories, databases, authentication servers, and other systems that will be used to authenticate the identities.

The MyID software is a central point for policy enforcement. Simple workflows allow both central and self-service administration carefully limited to compliant actions. The software maintains an audit trail to prove compliance. The product has been through code audits and penetration testing to validate the level of security.

Intercede products are compliant with standards from ISO, NIST, ETSI, GlobalPlatform, and other relevant organizations.

Centrally-Managed Identities

Billions of identities around the world and established and managed centrally. These are increasingly in the form of digital credentials. Out of this very large set, a sensible starting point for W3C engagement is identity-specific PKI credentials. These are widely issued today as employee badges by both corporate and government entities, where the credentials are used for physical access and for cyber access, whether logon to a local computer or web-based access. The U.S. Federal government has issued such credentials to all of its employees and contractors. Corporates from Aerospace & Defense, financial services, manufacturing, and others segments also issue PKI badges. Since these credential holders all regularly use web browsers, enabling use of these credentials is a natural starting point for web crypto API integration.

Support for the NIST FIPS 201 standards should be included in the discussion. The current population of PIV, PIV-I, and CIV cards based on these standards is over 10 million users. Since much of the standard is mandatory for PIV and PIV-I cards, there is interoperability among these cards. And motivation for vendors to supply compliant hardware and software. In addition, there are policies for the appropriate use of the credentials.

Outside of the U.S., most of the deployments use ISO 7816-4 compliant smart cards. Because of the broadness of the specifications, it will require additional work to ensure usability. The cards usually implement a sub-set of 7816-4 that varies from vendor to vendor. The credentials stored, their location, and suitable policies are often set on a project-by-project basis.

User-Managed Identities

There is an emerging segment around user-managed identities. In this segment, each user creates their own identity and registers it with the server of their choice. Historically, this has been done with user name / password, or self-enrolled OTP. No exposed crypto functions were used. Due to the demand for higher security and improved user convenience, new protocols such as those recently released by the FIDO Alliance are being developed. Intercede encourages support for and interoperability with these emerging standards.

Intercede also believes that these standards need to be extended to enable the same degree of lifecycle management of credentials are have been traditionally used in systems with centralized issuance. Users will experience the same challenges with lost/stolen devices, the need to migrate to a new device, multiple devices, etc..

Credential Stores

Smart cards and USB tokens have been used for many years for the storage and use of identity credentials. They provide strong security, both at rest and during crypto operations, as well as a good user experience. Smart card chips are also now being packaged in newer form factors such as microSD. With billions in daily use, these devices will continue to play an important role going forward and should be included as supported crypto devices.

Desktop and laptop computers have long included TPM chips. Recently these have come into use as “virtual smart cards”. The software interfaces are converging towards those for physical smart cards.

Many modern mobile devices include some form of secure element. Every mobile phone contains a SIM card. The larger memory versions support additional Java Card applets. Many types of applets have been adapted for use in the UICC, including payment and identity. The same is true for NFC secure elements found in some phones. And microSD cards. The mobile TPM is in discussion. And with the proliferation of devices, there is starting to be overlap between traditional “Win/Tel” devices with standard TPMs and mobile devices. The ARM TrustZone architecture is now supported by GlobalPlatform standards for a Trusted Execution Environment, “TEE”. The TEE provides more capabilities, including control of the user interface in a more secure environment. With SOC manufacturing, there are many options for enhanced credential security.

Since access to secure elements in mobile devices may require a business agreement with a mobile operator and a handset manufacturer, there are a number of options for secure elements that are independently controlled. A microSD card is such an option if the handset contains an open slot. Smart card readers for mobile devices are available in a number of form factors including phone sleeves and small folding devices. NFC-capable phones can also use credentials stored in contactless smart cards. This is anticipated in NIST FIPS 201-2 with support for layered security for the NFC communication and extended access to credentials over the contactless interface.

Virtually every mobile device includes a Bluetooth interface that is under the control of the user. 3rd party vendors such as Tyfone, are now offering portable credential stores that can be used with multiple mobile devices. Such devices promise a new level of user convenience and portability as they connect wirelessly

Derived Credentials

In cases where a user identity is issued including credentials on an employee badge. There will be use cases that call for the use of that badge with those credentials. In the mobile world, there are cases, where the government agency or employer may prefer to issue an *additional* credential specifically for use in a secure element on a mobile device. This process is being standardized by NIST using the term “Derived Credentials” in their Special Publication 800-157. These derived credentials can serve the same purposes and are stored in the same set of secure elements as primary credentials. The web crypto API should support the use of Derived Credentials.

User Agent Use Cases

The primary use cases for code running in a User Agent are: signing, encryption, and authentication. If the user is carrying one or more credentials associated with their identity, those credentials should be available for these purposes.

In many cases, the use of the credentials should be limited to an appropriate set of apps. This can be through mechanisms such as code signing or URL-association. In some of these scenarios, it may be useful or necessary to modify the credentials to enable securing this binding. Intercede is in a unique position to contribute to this process. As our primary focus includes creating and managing credentials, we are familiar with the processes and with the associated standards. These types of extensions may be either by practice or through enhancements to other standards. For example, enabling logon to Windows systems requires adding UPN information to the certificates in a format that is consistent with X.509 but is defined and managed by Microsoft.

For the centrally issued credentials, the credential issuer will want to have a mechanism to control the set of applications and devices. For user-managed credentials, the current approach is to register a credential with one or more organizations, typically through a web site. The restriction should then to be the organization the credential is registered with.

It is also important that these use cases function where the web crypto credential use is in addition to the use of the same credentials in the same device, possibly at the same time for the same purpose. An authentication key made available through the web crypto API for in-app authentication may also be used to authentication the VPN or TLS session that is securing that app. In addition to addressing security, there are user interface issues as most

of these credentials will require a PIN or biometric presentation to enable authentication. In some cases, these UI issues are also linked to policy requirements

W3C Web Crypto - Engagement Points

To address the use cases and issues summarized above, we have identified the following potential points of engagement. We look forward to a discussion of these and other points to help increase the value and usage of the APIs.

1. Insuring that centrally-managed credentials can be accessed from relevant web crypto APIs, ideally supporting all physical cases, from smart cards, to SIM cards, to Bluetooth tokens, through an interface that can be used be future credential stores as well.

2. Alignment with FIDO and potentially other emerging user-managed identity standards

3. Development of appropriate links between applications using web crypto APIs and existing credentials. These links need to address issues such as discovery, association, and mutual authentication. While addressing the user experience and security issues.

4. An understanding of issues when a credential is used for authentication both at a lower level such as a VPN or TLS connection, and for additional authentication using the web crypto API. These issues include policy compliance, credential use/reuse, pin/biometric unlocking, and user experience.