MEMORY EXPERTS INTERNATIONAL

Security White Paper

Stealth MXP: Comprehensive Digital Identities in One Device

Author: Larry Hamid, CTO
Date: September 30, 2005

Abstract

Security tokens have been used for strong authentication of individuals to systems. They have traditionally come in many forms including smart cards, USB keys, biometric readers, and one-time-password devices. Many tokens have added value to authentication and can perform other security services such as being a secure repository of personal and corporate information and performing cryptographic operations for digital signing, verification, encryption and decryption. Despite the multitude of capabilities and form factors of tokens that have appeared in the market they have all been limited in capacity, application and portability, which poses serious obstacles when facing today's new digital identity requirements. MXP is the first technology of its kind that has the manifold identities, strong authentication, large capacity, flexibility, security and portability to meet the needs of existing systems and the rapidly evolving demands of the identity management and information security industry.

Digital Identity

A digital identity can be defined as a set of claims that characterize a person or thing in a digital realm. A claim is a statement made about someone or something by someone or something.

There are many facets to a digital identity. Generally speaking, each entity that we interact with in the digital world seeks different claims about us. For example, your online bank will identify you by your bank account number while your membership to an online web community may be an email address. In many scenarios your identity could be personal information such as your name, address, and telephone number. Once an identity is confirmed it can be used to access services for which it is authorized to use based on whether the claims meet the service policy.

The number of digital identities that we possess is on the rise. Internally an enterprise has many applications that contribute to the myriad user names and passwords each user is required to remember. Organizations have typically dealt with this issue by deploying single sign-on (SSO) solutions. Most SSO products maintain a bank of digital identities, mostly in the form of usernames and passwords. These are served to the various applications as required.

The web has been another source of digital identity proliferation. People are using the web for everyday tasks such as shopping, banking and entertainment while businesses are delivering more services and content for customers, partners and employees. Each service usually requires its own account identifiers and passwords. The security, privacy, and interoperability of digital identities are the biggest challenges that the web is facing today. This problem is starting to be addressed with emerging standards and technologies such as Web Service Security (WSS) and Liberty Alliance to form an identity management architecture known as Federated Identity.

User Authentication

User authentication is the process of identifying an individual to ensure that the individual is who he or she claims to be.

User authentication is always based on one or more of three factors; knowledge, possession and biometry. Using knowledge a user proves that she knows a secret such as a password. Possession proves identity based on ownership of some object such as an employee badge or a smart card. In biometrics, physical or behavioral traits that are unique to an individual are used to confirm identity. Some examples of biometric traits are fingerprints, iris patterns, voice patterns and faces.

The strength of user authentication is increased substantially by using more than one factor in combination. For example requiring a PIN and a smart card (knowledge and possession), results in stronger authentication than merely requiring ownership of a smart card. Many organizations have implemented strong authentication by deploying smart cards, biometric readers and OTP tokens.

New regulatory compliance initiatives are now being legislated such as Sarbanes-Oxley, HIPAA and Graham-Leach-Bliley. These regulations increase the accountability of individuals and organizations for their actions regarding access and use of sensitive information. Such accountability requires a strong binding of the individual to his digital identity.

The accumulating number of digital identities that we possess along with the growing number of services that these identities access, plus the increasing liability of our actions in the corporate world demand that strong authentication of individuals is an important aspect of the digital identity infrastructure.

Identity Providers and Security Tokens

An identity provider is an entity that issues digital identities. Credit card companies, governments and businesses are all examples of identity providers because they issue identities to their customers and citizens. Individuals are also considered identity providers of self-issued identities when they sign up to memberships on web sites.

To be useful in a digital transaction, identity claims must be asserted in some way or another. The mechanism used is to put the identity claims into what are known as security tokens. Security tokens can be trusted by a relying party via a trust relationship with the token issuer or verified through cryptographic methods. Security tokens take many formats depending on the system that is being used. For example X509 certificates convey identity information to PKI systems, SAML tokens assert claims requested by a WS-Trust relying party, One-Time-Passwords (OTP) are used by remote access servers, while username and passwords can be provided to legacy systems, login dialogs and web pages.

Security tokens are issued after successful authentication of the subject. Sometimes it is the identity provider that performs the authentication as is the case of a web site that verifies a user name and password. Alternatively, the authentication can be delegated to another trusted entity. For example, a smart card can generate an X509 token, which might contain your digital identity issued by an authority such as your employer. The smart card signing operation provides proof that the user owns the private key. The relying party can also check the validity of the certificate by trusting the certificate authority.

The process of issuing a security token using a device such as Stealth MXP is illustrated below.
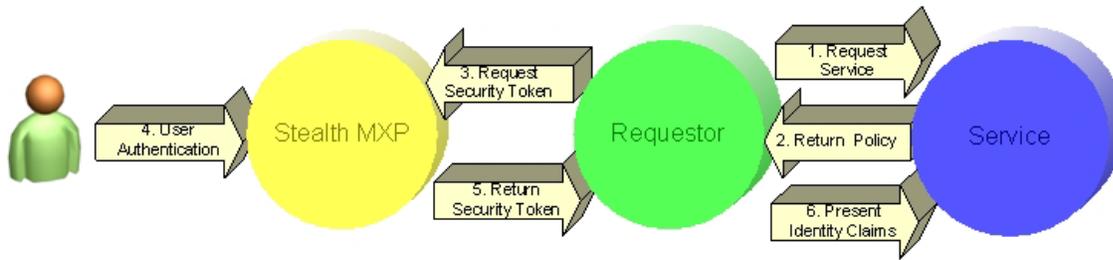

Figure 1: Security Token Flow with Stealth MXP

Microsoft InfoCard and PSTS

Microsoft has recently unveiled InfoCard as part of an identity metasystem. InfoCard allows the user to visualize and control the use of his digital identities, provides a consistent experience across multiple systems and technologies, and provides a safer environment for consumers where attacks such as "phishing" are mitigated.

InfoCard represents digital identities in information cards that can be presented visually to users in a consistent way. Different services seek different claims according to their service policies. For example, the claims that you provide to a financial institution are different than what you would provide for an online community such as a chat or gaming service. During a transaction the InfoCard system will interpret a service policy and display digital identities that are suitable for that service, allowing a user to select the one she wants to use. Once selected, the requested claims are asserted in a SAML token and no information need be entered into a web form. This empowerment of the user coupled with the security of the InfoCard subsystem is believed by many to be crucial to the success of digital identities on the Internet.

MXI and Microsoft are jointly developing an open standard called Portable Security Token Service (PSTS) that specifies how InfoCards can be managed on portable devices that are capable of issuing SAML tokens.

Today's Challenges

There are a number of challenges facing any device that is going to be used today and in the future as an effective digital identity technology.

Multiple Identities and Formats

The ability to carry multiple different identities and provide them in many different formats is difficult to achieve and has not really been addressed in the common tokens we have today.

Smart cards have small capacities resulting in limited numbers of digital credentials that can be maintained. The larger cards today have a total of 64K to 128K bytes for code and data. After code there may only be space left for maybe half a dozen PKI credentials. In terms of formats, smart cards usually support X509 but do not generate SAML tokens. It is worthy to note that SSO solutions have used smart cards extensively to also store application credentials such as usernames and passwords in secure containers.

Even more limited in scope are OTP tokens. Although they provide strong authentication one could argue that OTP tokens do not provide digital identities since they convey no additional claims other than authentication data. Being bound to one authentication server OTP tokens are really dedicated for authenticating one identity to one system.

Many Standards

Many security standards have been developed to address interoperability of applications and devices. PKCS #11 and MS CAPI are two specifications that define a standard interface to cryptographic services and have been used extensively for managing devices that issue X509 security tokens. Extensions to these standards are being proposed to deal with other security objects such as One-Time-Passwords.

WS-Trust is a specification that is now on track for standardization through OASIS that defines security token services and addresses the interoperability of security tokens. This standard will be used extensively for any Web Services Security implementations including Microsoft's InfoCard system. Under the WS-Trust umbrella, the PSTS specification is used to enable users to roam within an identity metasystem.

Identity devices must interface through to many existing and emerging standards if they are to maximize their utility and interoperability.

Portability

Portability has been an elusive feature to achieve. Many digital identity devices are physically portable but not logically portable. The reality today is that most devices only let you roam to where you have deployed software specific to that device. This has been the Achilles' heel of smart cards. Despite their desirable form factor, the smart card must bring with it device drivers, card readers and proprietary middleware in order to make roaming possible. Huge standards efforts have been initiated over the years now to try to deal with smart card interoperability and portability. In most cases, smart card portability is limited to roaming within an organization. Anything more is orders of magnitude harder to achieve.

One must also be wary of the claims of many USB token vendors about portability. Although USB tokens do not require readers, they may in fact still require a device driver or need administrator privileges to operate. Quite often this is not apparent as the devices are frequently evaluated on machines where administrator privileges are present allowing extended functions to be accessed and components to be silently installed, thereby giving a false sense of portability. Many corporate environments do not let users have administrator privileges on their workstations. The same is true for kiosks and machines at internet cafes. True portability must come with no strings attached.

Security and Privacy

Security and privacy are still top requirements for any device that manages digital identities. With increasing pressure from regulatory legislation on access to information and its use, an organization must be more certain that ever before that proper controls are in place to prevent unauthorized access. A strong identity infrastructure is the first step in assuring this control where a false identity claim can have legal repercussions.

Identity theft is the fasted growing crime on the internet. This is threatening the use of the web for business and e-commerce as people become more aware of these threats. One of the drivers of the claims based identity is minimal disclosure of information. That is, only the identity claims that are required to access a service should be provided and no more. Protecting digital identities is critical to the success of e-commerce and the use of the internet for business to business transactions.

Software is much more vulnerable to attacks than hardware. It is desirable to have as much security critical functions as possible done in the token hardware. In particular, strong authentication should be implemented in hardware to protect the authentication data from attacks. Likewise hardware protection of secrets and keys are also crucial to securing the identities contained on a device and therefore also the assets that these identities can access.

The MXP Advantage

The following diagram illustrates Stealth MXP within the framework of digital identity interfaces and consumers.
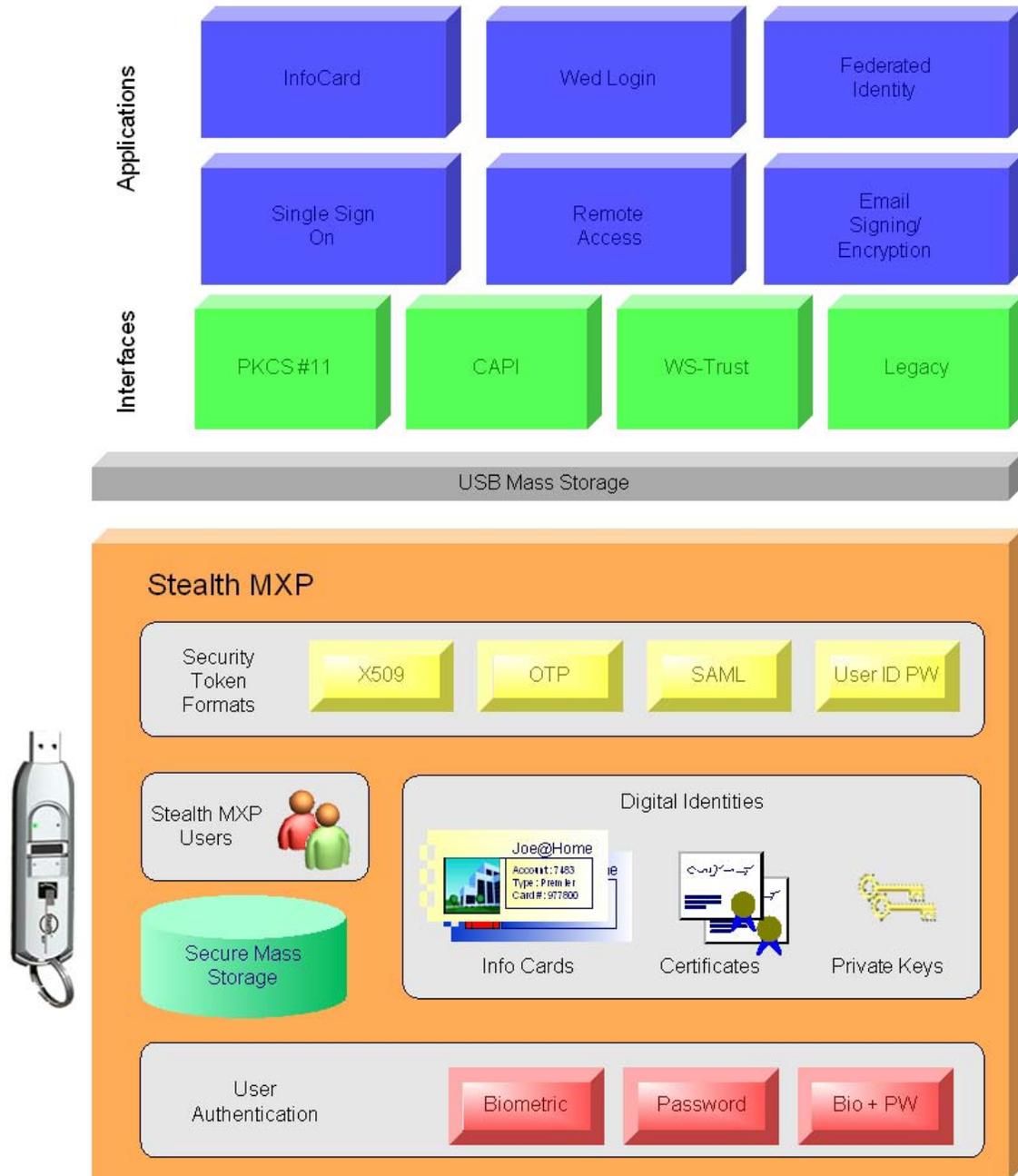
Figure 2: Stealth MXP and the Digital Identity Stack

With regards to capacity, the InfoCard system demands that a unique RSA key pair be generated for each digital credential and target service pair. With many digital identities and target services, the combinations add up rapidly. Stealth MXP has the capacity for hundreds of keys and digital identity claims to meet this need while at the same time providing fast response.

Security tokens in many formats can be generated by Stealth MXP including username and passwords for legacy systems, x509 certificates and proof for PKI systems, One-Time-Passwords for authentication servers, and can generate SAML tokens containing claims requested by a WS-Trust relying party. The interoperability and presentation of these token formats to systems is done through standard interfaces.

Stealth MXP provides strong authentication of users using password, fingerprint or both factors together. These authentication mechanisms occur entirely on the device providing maximal security of the authentication process and assure the strongest possible binding of an MXP user to his keys and digital identities. Moreover, the device also has on board key generation capabilities to ensure that private keys are always secret in hardware.

Stealth MXP is the first device of its kind to achieve 100% portability. The communication protocol does not require any additional drivers or use any extended commands that require administrator privileges on the machine. In fact the protocol of Stealth MXP has been incorporated into the PSTS specification primarily for its ability to achieve complete portability. This makes it possible for secure internet transactions to be performed using a portable device from any machine that has the InfoCard system installed.

Finally, Stealth MXP has additional services to round out its functionality as a complete security device. It can provide generic cryptographic services bound to authenticated users as well as secure mass storage with transparent encryption of private data. It also has administrative functions that allow it to be managed in an enterprise environment where security policies are defined and enforced by an organization. Alternatively Stealth MXP can be managed by individuals for use in their own personal environments.

A device suitable for the expansive demands of digital identities needs to be a comprehensive in its capacity for digital identities, security token formats, interoperability, portability and security. These are the drivers that resulted in Stealth MXP being a single device that meets the digital identity requirements of today and tomorrow.