Microsoft’s Vision for an Identity Metasystem

A Microsoft Whitepaper

Digital Identity: The Challenge

For users and businesses alike, the Internet continues to be increasingly valuable. More people are using the web for everyday tasks, from shopping, banking, and paying bills to consuming media and entertainment. E-commerce is growing, with businesses delivering more services and content across the Internet, communicating and collaborating online, and inventing new ways to connect with each other.

But as the value of what people do online has increased, the Internet itself has become more complex, criminalized, and dangerous. Online identity theft, fraud, and privacy concerns are on the rise, stemming from increasingly sophisticated practices such as “phishing”. The multiplicity of accounts and passwords users must keep track of and the variety of methods of authenticating to sites result not only in user frustration, known as “password fatigue”, but also insecure practices such as reusing the same account names and passwords at many sites.

The root of these problems is that the Internet was designed without a system of digital identity in mind. In efforts to address this deficiency, numerous digital identity systems have been introduced, each with its own strengths and weaknesses. But no one single system meets the needs of every digital identity scenario. And even if it were possible to create one system that did, the reality is that many different identity systems are in use today, with still more being invented. As a result, the current state of digital identity on the Internet is an inconsistent patchwork of ad hoc solutions that burdens people with different user experiences at every web site, renders the system as a whole fragile, and constrains the fuller realization of the promise of e-commerce.

What is the Identity Metasystem?

Given that universal adoption of a single digital identity system or technology is unlikely ever to occur, a successful and widely employed identity solution for the Internet requires a different approach — one with the capability to connect existing and future identity systems into an **identity metasystem**. This metasystem, or system of systems, would leverage the strengths of its constituent identity systems, provide interoperability between them, and enable creation of a consistent and straightforward user interface to them all. The resulting improvements in cyberspace would benefit everyone, making the Internet a safer place with the potential to boost e-commerce, combat phishing, and solve other digital identity challenges.

In the offline world, people carry multiple forms of identification in their wallets, such as driver’s licenses or other government-issued identity cards, credit cards, and affinity cards such as frequent flyer cards. People control which card to use and how much information to reveal in any given situation.

Similarly, the identity metasystem makes it easier for users to stay safe and in control when accessing resources on the Internet. It lets users select from among a portfolio of their digital identities and use them at Internet services of their choice where they are accepted. The metasystem enables identities provided by one identity system technology to be used within systems based on different technologies, provided an intermediary exists that understands both technologies and is willing and trusted to do the needed translations.

It's important to note that the identity metasystem does not compete with or replace the identity systems it connects. Rather, it plays a role analogous to that of the Internet Protocol (IP) in the realm of networking. In the 1970s and early 1980s, before the invention of IP, distributed applications were forced to have direct knowledge of the network link, be it Ethernet, Token Ring, ArcNet, X.25, or Frame Relay. But IP changed the landscape by offering a technology-independent metasystem that insulated applications from the intricacies of individual network technologies, providing seamless interconnectivity and a platform for including not-yet-invented networks (such as 802.11 wireless) into the network metasystem.

In the same way, the goals of the identity metasystem are to connect individual identity systems, allowing seamless interoperation between them, to provide applications with a technology-independent representation of identities, and to provide a better, more consistent user experience with all of them. Far from competing with or replacing the identity systems it connects, the metasystem *relies* on the individual systems to do its work!

Identities Function in Contexts

The identities held by a person in the offline world can range from the significant, such as birth certificates, passports, and drivers' licenses, to the trivial, such as business cards or frequent coffee buyer's cards. People use their different forms of identification in different contexts where they are accepted.

Identities can be in or out of context. Identities used out of context generally do not bring the desired result. For example, trying to use a coffee card to cross a border is clearly out of context. On the other hand, using a bank card at an ATM, a government-issued ID at a border, a coffee card at a coffee stand, and a Passport Network (formerly .NET Passport) account at MSN Hotmail are all clearly in context.

In some cases, the distinction is less clear. You could conceivably use a government-issued ID at your ATM instead of a bank-issued card, but if this resulted in the government having knowledge of each financial transaction, some people would be uncomfortable. You could use a Social Security Number as a student ID number, but that has significant privacy implications, even facilitating identity theft. And you can use Passport accounts at some non-Microsoft sites, but few sites chose to enable this; even where it was enabled, few users did so because they felt that Microsoft's participation in these interactions was out of context.

Studying the Passport experience and other digital identity initiatives throughout the industry led us to work with a wide range of industry experts to codify a set of principles that we believe are fundamental to a successful, broadly adopted, and enduring digital identity system on the Internet. We call these principles "The Laws of Identity".

The Laws of Identity

The "Laws of Identity" are intended to codify a set of fundamental principles to which any universally adopted, sustainable identity architecture must conform. The Laws were proposed, debated, and refined through a long-running, open, and continuing dialogue on the Internet. Taken together, the Laws define the architecture of the identity metasystem.

They are:

1. **User Control and Consent:** Identity systems must only reveal information identifying a user with the user's consent.
2. **Minimal Disclosure for a Constrained Use:** The identity system must disclose the least identifying information possible, as this is the most stable, long-term solution.
3. **Justifiable Parties:** Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
4. **Directed Identity:** A universal identity system must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
5. **Pluralism of Operators and Technologies:** A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers.
6. **Human Integration:** Identity systems must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.
7. **Consistent Experience Across Contexts:** The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

The Laws of Identity are discussed in more detail in The Laws of Identity whitepaper. To join in the discussion of the Laws of Identity, visit www.identityblog.com.

Roles within the Identity Metasystem

Different parties participate in the metasystem in different ways. The three roles within the metasystem are:

- **Identity Providers**, which issue digital identities. For example, credit card providers might issue identities enabling payment, businesses might issue identities to their customers, governments might issue identities to citizens, and individuals might use self-issued identities in contexts like signing on to web sites.
- **Relying Parties**, which require identities. For example, a web site or online service that utilizes identities offered by other parties.
- **Subjects**, which are the individuals and other entities about whom claims are made. Examples of subjects include end users, companies, and organizations.

In many cases, the participants in the metasystem play more than one role, and often all three.

Components of the Identity Metasystem

To build an identity metasystem, five key components are needed:

1. A way to represent identities using claims.
2. A means for identity providers, relying parties, and subjects to negotiate.
3. An encapsulating protocol to obtain claims and requirements.
4. A means to bridge technology and organizational boundaries using claims transformation.
5. A consistent user experience across multiple contexts, technologies, and operators.

Claims-Based Identities

Digital identities consist of sets of claims made about the subject of the identity, where "claims" are pieces of information about the subject that the issuer asserts are valid. This parallels identities used in the real world. For example, the claims on a driver's license might include the issuing state, the driver's license number, name, address, sex, birth date, organ donor status, signature, and photograph, the types of vehicles the subject is eligible to drive, and restrictions on driving rights. The issuing state asserts that these claims are valid. The claims on a credit card might include the issuer's identity, the subject's name, the account number, the expiration date, the validation code, and a signature. The card issuer asserts that these claims are valid. The claims on a self-issued identity, where the identity provider and subject are one and the same entity, might include the subject's name, address, telephone number, and e-mail address, or perhaps just the knowledge of a secret. For self-issued identities, the subject asserts that these claims are valid.

Negotiation

Negotiation enables participants in the metasystem to make agreements needed for them to connect with one another within the metasystem. Negotiation is used to determine mutually acceptable technologies, claims, and requirements. For instance, if one party understands SAML and X.509 claims, and another understands Kerberos and X.509 claims, the parties would negotiate and decide to use X.509 claims with one another. Another type of negotiation determines whether the claims needed by a relying party can be supplied by a particular identity. Both kinds of negotiation are simple matching exercises; they compare what one party can provide with what the other one needs to determine whether there's a fit.

Encapsulating Protocol

The encapsulating protocol provides a technology-neutral way to exchange claims and requirements between subjects, identity providers, and relying parties. The participants determine the content and meaning of what is exchanged, not the metasystem. For example, the encapsulating protocol would allow an application to retrieve SAML-encoded claims without having to understand or implement the SAML protocol.

Claims Transformers

Claims transformers bridge organizational and technical boundaries by translating claims understood in one system into claims understood and trusted by another system, thereby insulating the mass of clients and servers from the intricacies of claim evaluation. Claims transformers may also transform or refine the semantics of claims. For example, a claim asserting "Is an employee" might be transformed into the new claim "OK to purchase book". The claim "Born on March 22, 1960" could be transformed into the claim "Age is over 21 years", which intentionally supplies less information. Claims transformers may also be used to change claim formats. For instance, claims made in formats such as X.509, Kerberos, SAML 1.0, SAML 2.0, SXIP, and others could be transformed into claims expressed using different technologies. Claims transformers provide the interoperability needed today, plus the flexibility required to incorporate new technologies.

Consistent User Experience

Many identity attacks succeed because the user was fooled by something presented on the screen, not because of insecure communication technologies. For example, phishing attacks occur not in the secured channel between web servers and browsers — a channel that might extend thousands of miles — but in the two or three feet between the browser and the human who uses it. The identity metasystem, therefore, seeks to empower users to make informed and reasonable identity decisions by enabling the development of a consistent, comprehensible, and integrated user interface for making those choices.

One key to securing the whole system is presenting an easy-to-learn, predictable user interface that looks and works the same no matter which underlying identity technologies are employed. Another key is making important information obvious — for instance, displaying the identity of the site you're authenticating to in a way that makes spoofing attempts apparent. The user must be informed which items of personal information relying parties are requesting, and for what purposes. This allows users to make informed choices about whether or not to disclose this information. Finally, the user interface provides a means for the user to actively consent to the disclosure, if they agree to the conditions.

Benefits of the Identity Metasystem

Microsoft recognizes that the identity metasystem will only gain widespread adoption if participants filling all roles in the metasystem stand to benefit from their participation. Fortunately, this is the case. Key benefits of the identity metasystem include:

- **Greater user control and flexibility.** Users decide how much information they disclose, to whom, and under what circumstances, thereby enabling them to better protect their privacy. Strong two-way authentication of identity providers and relying parties helps address phishing and other fraud. Identities and accompanying personal information can be securely stored and managed in a variety of ways, including via the online identity provider service of the user's choice, or on the user's

PC, or in other devices such as secure USB keychain storage devices, smartcards, PDAs, and mobile phones

- **Safer, more comprehensible user experience.** The identity metasystem enables a predictable, uniform user experience across multiple identity systems. It extends to and integrates the human user, thereby helping to secure the machine-human channel.
- **Increases the reach of existing identity systems.** The identity metasystem does not compete with or replace the identity systems it connects, but rather preserves and builds upon customers' investments in their existing identity solutions. It affords the opportunity to use existing identities, such as corporate-issued identities and identities issued by online businesses, in new contexts where they could not have been previously employed.
- **Fosters identity system innovation.** The identity metasystem should make it easier for newly-developed identity technologies and systems to quickly gain widespread use and adoption. Claims transformers can allow new systems to participate even when most participants don't understand their native claims formats and protocols.
- **Enables adaptation in the face of attacks**. New technologies are needed to stay ahead of criminals who attack existing identity technologies. The metasystem enables new identity technologies to be quickly deployed and utilized within the metasystem as they are needed.
- **Creates new market opportunities.** The identity metasystem enables interoperable, independent implementations of all metasystem components, meaning that the market opportunities are only limited by innovators' imaginations. Some parties will choose to go into the identity provider business. Others will provide certification services for identities. Some will implement server software. Others will implement client software. Device manufacturers and mobile telephone players can host identities on their platforms. New business opportunities are created for identity brokers, where trusted intermediaries transform claims from one system to another. New business opportunities abound.

A benefit we will all share as the identity metasystem becomes widely deployed is a **safer, more trustworthy Internet**. The metasystem will supply the widely adopted identity solution that the Net so desperately needs.

Participants in the identity metasystem can include anyone or anything that uses, participates in, or relies upon identities in any way, including, but not limited to existing identity systems, corporate identities, government identities, Liberty federations, operating systems, mobile devices, online services, and smartcards. Again, the possibilities are only limited by innovators' imaginations.

An Architecture for the Identity Metasystem: WS-* Web Services

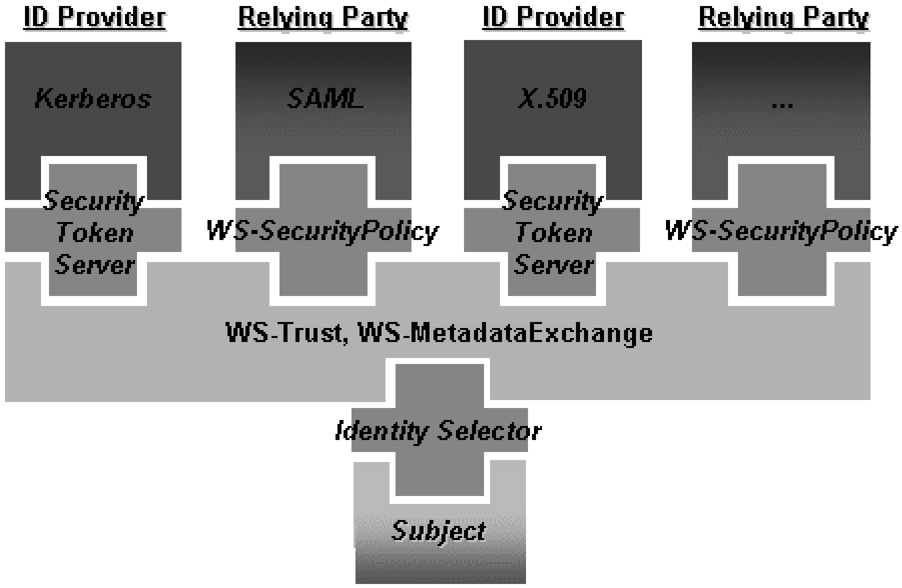
Microsoft has worked for the past several years with industry partners on a composable, end to end architecture for Web Services. The set of specifications that make up this architecture have been named the WS-* Web Services architecture by the industry (see http://msdn.microsoft.com/webservices/). This architecture supports the requirements of the identity metasystem.

The encapsulating protocol used for claims transformation is WS-Trust. Negotiations are conducted using WS-MetadataExchange and WS-SecurityPolicy. These protocols enable building a technology-neutral identity metasystem and form the “backplane” of the identity metasystem. Like other Web services protocols, they also allow new kinds of identities and technologies to be incorporated and utilized as they are developed and adopted by the industry.

To foster the interoperability necessary for broad adoption, the specifications for WS-* are published and are freely available, have been or will be submitted to open standards bodies, and allows implementations to be developed royalty-free.

Deployments of existing identity technologies can be leveraged in the metasystem by implementing support for the three WS-* protocols above. Examples of technologies that could be utilized via the metasystem include LDAP claims schemas, X.509, which is used in Smartcards; Kerberos, which is used in Active Directory and some UNIX environments; and SAML, a standard used in inter-corporate federation scenarios.

Identity Metasystem Architectural Diagram



This figure depicts sample relationships between a subject, identity providers, and relying parties, showing some of the technologies used by the metasystem and by specific systems utilized through the metasystem.

- The *Security Token Server* implements the WS-Trust protocol and provides support for claims transformation.
- Relying parties provide statements of requirements, expressed in terms of the WS-SecurityPolicy specification, and made available through the WS-MetadataExchange protocol.
- The Identity Selector implements the consistent user experience. After being invoked by an application, it performs the negotiation between relying party and identity provider(s), displays the identities of “matched” identity providers and

relying parties to the subject (e.g. the end user), obtains claims, and releases them to the application under the supervision of the subject.

Microsoft's Implementation Plans

Microsoft plans to build software filling all roles within the identity metasystem (while encouraging others to also build software filling these roles, including on non-Windows platforms). Microsoft is implementing the following software components for participation in the metasystem:

- **"InfoCard" identity selector:** "InfoCard" is the code-name for a WinFX component that provides the consistent user experience required by the identity metasystem. It is specifically hardened against tampering and spoofing to protect the end user's digital identities and maintain end-user control. Each digital identity managed by "InfoCard" is represented by a visual "Information Card" in the client user interface. The user selects identities represented by "InfoCards" to authenticate to participating services.
- **"InfoCard" simple self-issued identity provider:** "InfoCard" also includes a simple identity provider that enables individual PC users to create and utilize self-issued identities, enabling password-free strong authentication to relying parties. A self-issued identity is one where the user vouches for the information they are providing, much like users do today when registering with a Web site. We are implementing the simple self-issued identity provider to help bootstrap the identity metasystem; we believe self-issued identities will continue to be accepted for certain classes of services. Identities hosted in the simple self-issued identity provider will not include or store sensitive personal information, such as Social Security numbers (or other national ID numbers if these are developed) or credit card numbers. Self-issued identities are not intended to provide the full range of features that a managed identity provider can offer - the market is wide open for companies to provide managed identity solutions to consumers.
- **Active Directory identity provider:** This is a managed identity provider integrated with Active Directory. It includes a full set of policy controls to manage the use of Active Directory identities in the identity metasystem. Active Directory Federation Services, a new Active Directory feature shipping in Windows Server 2003 R2, is the first step to integrating identities in Active Directory with the identity metasystem.
- **"Indigo":** The code-named "Indigo" web services run time provides developers a way to rapidly build and deploy distributed applications, including relying party services in the identity metasystem.

The identity metasystem preserves and builds upon customers' investments in their existing identity solutions, including Active Directory and other identity solutions. Microsoft's implementation will be fully interoperable via WS-* protocols with other identity selector implementations, with other relying party implementations, and with other identity provider implementations.

Non-Microsoft applications will have the same ability to use "InfoCard" to manage their identities as Microsoft applications will. Non-Windows operating systems will be able to be full participants of the identity metasystem we are building in cooperation with the industry. Others can build an entire end-to-end implementation of the metasystem without any Microsoft software, payments to Microsoft, or usage of any Microsoft online identity service.

What we've Learned from Passport

Microsoft's best-known identity effort is almost certainly the Passport Network (formerly .NET Passport). Microsoft has learned a great deal from building one of the largest Internet scale authentication services in the world, and applied these hard-won lessons in developing the Laws of Identity, the identity metasystem, and several of our products.

Passport was originally intended to solve two problems: to be an identity provider for the MSN and Microsoft properties, and to be an identity provider for the Internet. It succeeded at the first, with over 250 million active Passport accounts and over 1 billion authentications per day. As for the second original goal, it became clear to us through continued engagement with partners, consumers, and the industry that in many cases it didn't make sense for Microsoft to play a role in transactions between, for instance, a company and its customers.

Apart from its input to our thinking on the Laws of Identity, it is worth mentioning that operating the Passport service has helped Microsoft gain a deep understanding of the operational and technical challenges that large-scale identity providers face. These experiences have helped us ensure that our identity products meet the needs of large-scale deployments.

The identity metasystem is different from the original version of Passport in several fundamental ways. The metasystem stores no personal information, leaving it up to individual identity providers to decide how and where to store that information. The identity metasystem is not an online identity provider for the Internet; indeed, it provides a means for all identity providers to coexist with and compete with one another, with all having equal standing within the metasystem. Finally, while Microsoft charged services to use the original version of Passport, no one will be charged to participate in the identity metasystem.

The Passport system itself has evolved in response to these experiences as well. It no longer stores personal information other than username/password credentials. Passport is now an authentication system targeted at Microsoft sites and those of close partners – a role that is clearly in context and with which our users and partners are very comfortable. Passport and MSN plan to implement support for the identity metasystem as an online identity provider for MSN and its partners. Passport users will get improved security and ease of use, and MSN Online partners will be able to interoperate with Passport through the identity metasystem.

Conclusions

Many of the problems on the Internet today, from phishing attacks to inconsistent user experiences, stem from the patchwork nature of digital identity solutions that software makers have built in the absence of a unifying and architected system of digital identity. An identity metasystem, as defined by the Laws of Identity, would supply a unifying fabric of digital identity, utilizing existing and future identity systems, providing interoperability between them, and enabling the creation of a consistent and straightforward user interface to them all. Basing our efforts on the Laws of Identity, Microsoft is working with others in the industry to build the identity metasystem using published WS-* protocols that render Microsoft's implementations fully interoperable with those produced by others.

We believe that many of the dangers, complications, annoyances, and uncertainties of today's online experiences can be a thing of the past. Widespread deployment of the identity metasystem has the potential to solve many of these problems, benefiting everyone and accelerating the long-term growth of connectivity by making the online world safer, more trustworthy, and easier to use. Microsoft is working with others in the industry to define and deploy the identity metasystem. We hope that you will join us!

For More Information

The Laws of Identity whitepaper.

Join the identity discussion at http://www.identityblog.com/.

This paper as it appears on MSDN.

Read more about Web services at http://msdn.microsoft.com/webservices/.