

Microsoft Windows CardSpace and the Identity Metasystem

OLE TOM SEIERSTAD



Ole Tom Seierstad is Chief Security Advisor in Microsoft Norway

Many of the problems on the Internet today, from phishing attacks to inconsistent user experiences, come 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, supplies a unifying fabric of digital identity, uses existing and future identity systems, provides interoperability between them, and enables 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.

CardSpace is Microsoft's implementation of an Identity Metasystem that enables users to choose from a portfolio of identities that belong to them and use them in contexts where they are accepted, independent of the underlying identity systems where the identities originate and are used.

Using CardSpace, 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 issues, benefiting everyone and accelerating the long-term growth of connectivity by making the online world safer, more trustworthy, and easier to use.*)

The Landscape

In the past three decades, information and communications technologies have transformed the global economy and given hundreds of millions of people new ways to work, communicate, learn, shop and play.

eCommerce 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. Greater productivity, more efficient internal processes and new ways of collaborating within organizations and with partners and customers are enabling organizations of all sizes to compete more effectively.

Governments are also taking advantage of these advances to improve the efficiency of their operations and deliver public services more effectively to citizens.

Widely publicized security and data breaches and growing consumer anxiety about identity theft and the privacy of their personal information are eroding public trust in the Internet.

Opportunities and Challenges

But as the value of what people do online has increased, the Internet itself has become more complex and dangerous. Online identity theft, fraud, and privacy concerns are on the rise. And sophisticated practices such as "phishing" are more and more common.

Phishing attacks use social engineering to steal consumers' personal identity data or financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to false websites designed to trick recipients into divulging personal data such as credit card numbers, account usernames, passwords and social security numbers. Figure 1 shows the number of new phishing sites during the last twelve months (<http://www.antiphishing.org>).

One root of some 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 single system meets the requirements of every digital identity scenario. The reality is that many different identity systems are in use today, with still more being invented. The result is an inconsistent patchwork of improvised solutions at every website.

Open 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 (or "system of systems"). This metasystem leverages the strengths of its constituent identity systems, provides inter-

*) The paper is based on whitepapers and blogs from Kim Cameron and Michael Jones – Microsoft Cooperation.

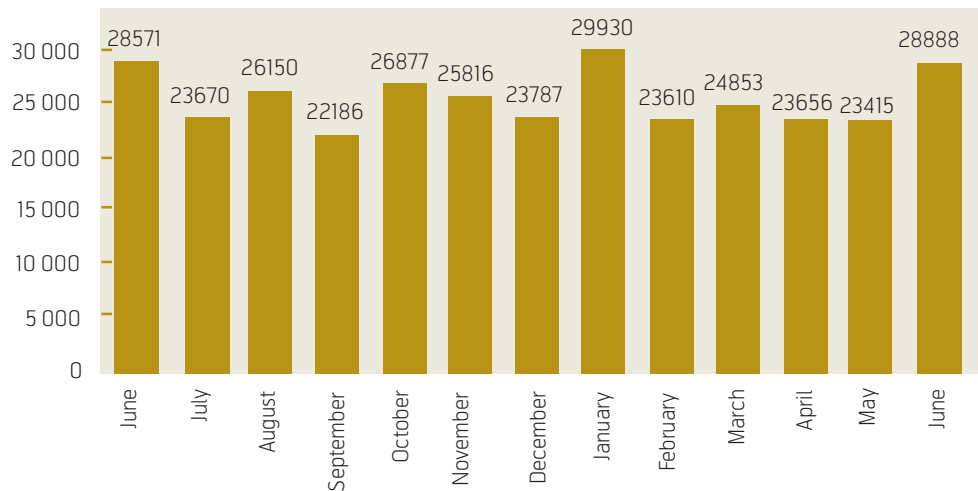


Figure 1 Numbers of new phishing sites (according to www.antiphishing.org)

operability between them, and enables creation of a consistent and straightforward user interface to all. The metasytem 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 is important to note that the identity metasytem 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 metasytem 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 metasytem.

In the same way, the goals of the identity metasytem are to connect individual identity systems, allowing seamless interoperability 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 of a system it connects, the metasytem relies on the individual systems to do its work.

The Identity Metasytem allows users to manage their digital identities, whether they are self-issued or issued by third-party identity providers, and employ them in contexts where they are accepted to access online services. In the Identity Metasytem, identities are represented to users as “Information Cards”.

Maintain the Diversity of Systems

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 cards such as frequent flyer cards. People control which card to use and how much information to reveal in any given situation.

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 account at MSN Hotmail are all clearly in context.

In some cases, the distinction is less clear. You can 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 can use a Social Security Number as a student ID number, but that facilitates 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.

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

stands both technologies and is willing and trusted to do the required translations.

It is important to note that the identity metasytem does not compete with or replace the identity systems it connects. Instead, the goals of the identity metasytem 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. The metasytem relies on the individual systems to do its work.

Principles (“Laws of Identity”)

The open identity metasytem is designed to follow a set of principles (also called “The Laws of Identity”) that have been developed with ongoing feedback and input from a broad community of people active in the digital identity community.

The principles that an identity system should follow are the following.

- *User Control and Consent*
Identity systems reveal information that identifies a user only with the user’s consent.
- *Minimal Disclosure for a Constrained Time*
The identity system solution that discloses the least amount of identifying information is the most stable, long-term solution.
- *Justifiable Parties*
Identity systems disclose identifying information only to parties who have a necessary and justifiable place in a given identity relationship.
- *Directed Identity*
Identity systems 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.
- *Pluralism of Operators and Technologies*
Identity systems channel and enable the inner workings of multiple identity technologies run by multiple identity providers.
- *Human Integration*
Identity systems define the human user to be a component of the distributed system, integrated through unambiguous human-machine communications mechanisms that offer protection against identity attacks.

- *Consistent Experience across Contexts*
Identity systems facilitate negotiation between a relying party and a user of a specific identity. That presents a harmonious human and technical interface while permitting the autonomy of identity in different contexts.

For a complete description of Laws of Identity, please visit Kim Cameron’s blog at <http://www.identityblog.com>.

CardSpace Solution

Windows CardSpace is client software that enables users to provide their digital identity to online services in a simple, secure and trusted way. It is what is known as an *identity selector*: when a user needs to authenticate to a web site or a web service, CardSpace pops up a special security-hardened UI with a set of “information cards” for the user to choose from. Each card has some identity data associated with it – though this is not actually stored in the card – that has either been given to the user by an *identity provider* such as their bank, employer or government, or created by the user themselves.

The CardSpace UI enables users to create *Personal* cards or *self-issued* cards and associate a limited set of identity data. When the user chooses a card, a signed and encrypted security token containing the required information (e.g. name and address, employer’s name and address, or credit limit) is generated by the identity provider that created the card. The user, in control at all times, then decides whether to release this information to the requesting online service. If the user approves then the token is sent on to this *relying party* where the token is processed and the identity information is extracted.

CardSpace is an identity selector for Microsoft Windows. Other operating systems have their own identity selector implementations. The architecture upon which CardSpace has been built – consisting of subjects, identity providers and relying parties – is called “The Identity Metasytem”. This is not just a Microsoft initiative, but rather it is the shared vision of many across the industry as to how we can solve some of the fundamental identity challenges on the Internet today.

The token is opaque as far as CardSpace is concerned. CardSpace is thus security token agnostic: it can be in any format whatsoever. However, the Identity Provider should provide a plain text version of the token – the display token – so that CardSpace can show this to the user and get the user’s consent to give the token to the Relying Party. The user no longer needs a password to login.



Figure 2 CardSpace solution in Windows Vista

Types of Information Cards

There are two types of Information Cards supported by CardSpace: Managed cards and Personal cards (also called self-issued cards).

Managed cards are cards that an Identity Provider has given to the user, who has imported it into Identity Selector. Identity Providers declare the claims they support in their cards using URIs. Separate Identity Providers can collaborate on the URIs they use to declare their claims, or make up ones specifically for themselves.

Personal Cards are cards that the user is also acting as the Identity Provider, and the user provides all the values for the claims. CardSpace provides the facility for the user to create, edit, export, and import Personal Cards. The data for these cards is encrypted and stored on the user's computer. The claims that a Personal Card can support are fixed, so that Relying Parties can accept a common, consistent Information Card.

Open Identity Metasystem Architecture

This section covers the general architecture of an open identity metasystem.

Roles

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

Identity Providers issue identities. For example, credit-card providers might issue identities that enable 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 require identities. For example, a website or online service that uses identities offered by other parties.

Subjects are the individuals and other entities about whom claims are made. Examples include end users, companies, and organizations.

Each person and entity that participate in an identity metasystem can play all the roles, and each person and entity can play more than one role at a time. Often a person or entity plays all three roles simultaneously.

Components

The metasystem is made up of five key components:

Claim	URI
Given Name	http://schemas.xmlsoap.org/ws/2005/05/identity/givenname
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/surname
Street	http://schemas.xmlsoap.org/ws/2005/05/identity/streetaddress
Locality (City)	http://schemas.xmlsoap.org/ws/2005/05/identity/locality
State or Province	http://schemas.xmlsoap.org/ws/2005/05/identity/stateorprovince
Postal Code	http://schemas.xmlsoap.org/ws/2005/05/identity/postalcode
Country/Region	http://schemas.xmlsoap.org/ws/2005/05/identity/country
Phone Number	http://schemas.xmlsoap.org/ws/2005/05/identity/homephone
Other Phone	http://schemas.xmlsoap.org/ws/2005/05/identity/otherphone
Mobile Phone	http://schemas.xmlsoap.org/ws/2005/05/identity/mobilephone
Date of Birth	http://schemas.xmlsoap.org/ws/2005/05/identity/dateofbirth
Gender	http://schemas.xmlsoap.org/ws/2005/05/identity/gender
PPID	http://schemas.xmlsoap.org/ws/2005/05/identity/privatepersonalidentifier
Web Page	http://schemas.xmlsoap.org/ws/2005/05/identity/webpage

Table 1 Schemas

- 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

Identities consist of sets of claims that are asserted about the subject of the identity. For example, the claims on a driver's license might include the issuing state, the driver's license number, a name, address, gender, birth date, the kinds of vehicles the licensee is eligible to drive, and so on. The issuing state asserts that these claims are valid.

The claims on a credit card might include the card issuer's identity, the card-holder's name, the account number, the expiration date, the validation code, and the card-holder's signature. The card issuer asserts that these claims are valid.

The claims on a self-issued identity (such as a business card) might include your name, address, and telephone number. For self-issued identities, you assert that these claims are valid yourself.

Table 1 shows the claims that are available in Personal Information Cards, along with the URIs that represent each of the claims.

Negotiation

Negotiation enables participants in the metasytem to make agreements required for them to connect with one another within the metasytem. 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 negotiate and decide to use X.509 claims with one another. Another type of negotiation determines whether the claims required 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 requires to determine whether there is 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 metasytem. 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 70 or 80 centimeters 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 devel-

opment of a consistent, comprehensible, and integrated user interface for making those choices.

One key to securing the whole system is to present 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 are 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.

WS-* Specifications

As with other features of WCF, the CardSpace technology is built upon a set of open specifications, the WS-* Web Services Architecture. 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 used as they are developed and adopted by the industry.

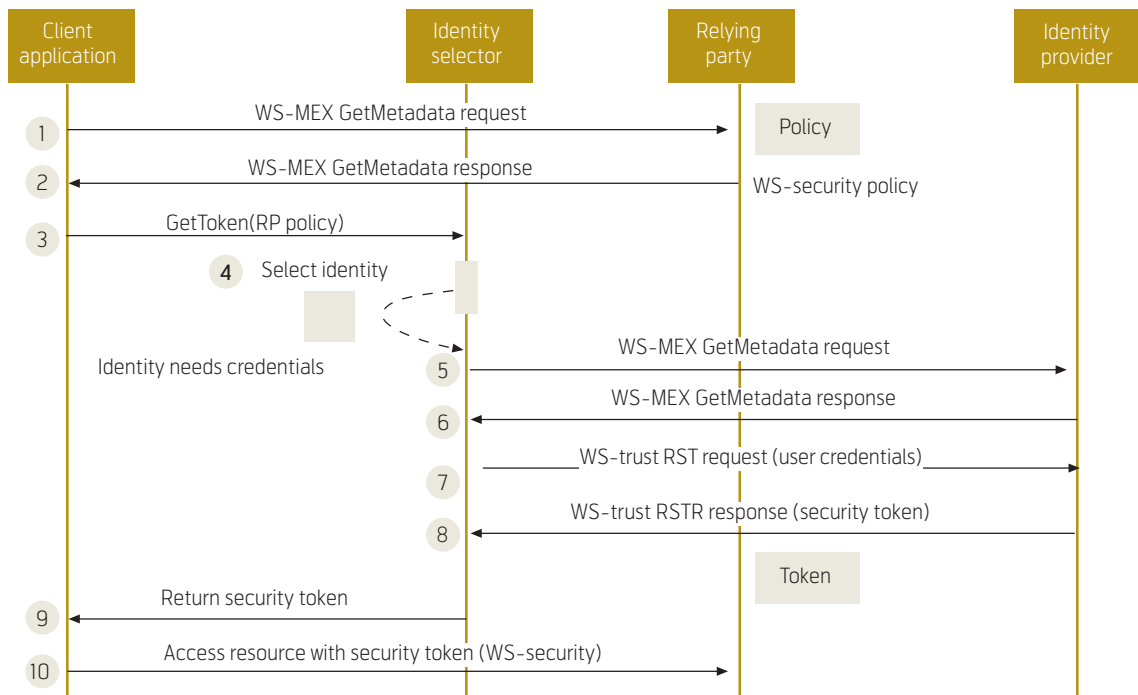


Figure 3 Dataflow in WS*

To promote the interoperability necessary for broad adoption, the specifications for WS-* are published and are freely available, have been and continue to be submitted to open standards bodies, and allow implementations to be developed royalty-free. More information about Web Services Specifications is found at <http://msdn2.microsoft.com/en-us/webservices/Aa740689.aspx>.

Deployments of existing identity technologies can be leveraged in the metasytem by implementing support for the three WS-* protocols above. Examples of technologies that could be utilized via the metasytem 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.

End-to-End Scenario

Figure 4 illustrates the end-to-end processes that occur when you use CardSpace to access a site that requires user validation.

The figure shows information flows through the client machine at the control of the user – this indicates that the metasytem is following law 1.

- In traditional models, identity provider and relying party are confined to the same domain.
- Federated identity allows an organization to consume identities issued by other organizations.

- A metasytem allows identity to be used flexibly and dynamically, with parties negotiating relationships.

Protocol:

- 1 User is asked for identity.
- 2 User chooses an identity provider.
- 3 Identity provider gives user a security token.
- 4 User passes the token to the requestor.
- 5 When the user requests a security token they have to authenticate themselves to their identity provider in some way. The IP does not give a token to just anyone who asks, you have to have the right to ask for the token. The four methods of authentication in CardSpace are X.509, Kerberos, username and password, and self-issued token. Any method that can plug in as an X.509 cert via a Crypto Service Provider will work.
- 6 Token is released to RP; RP reads claims and allows access.

WS-* Metasytem Architecture

Figure 5 depicts sample relationships between a subject, identity providers, and relying parties, showing some of the technologies used by the metasytem and by specific systems utilized through the metasytem.

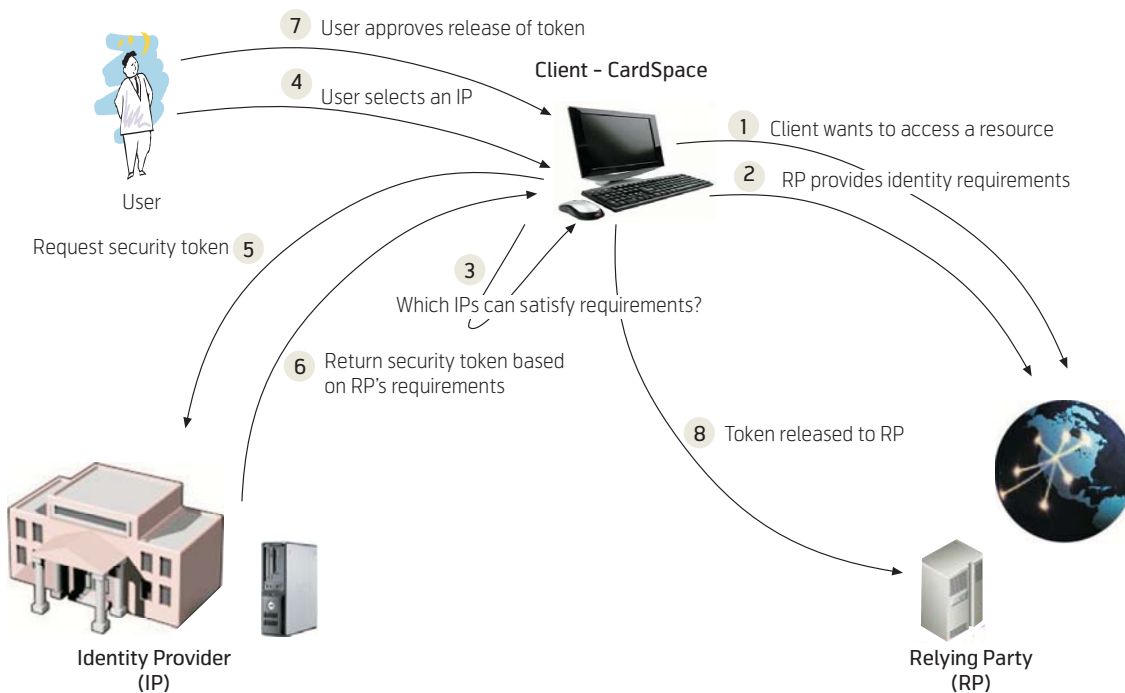


Figure 4 End-to-end scenario

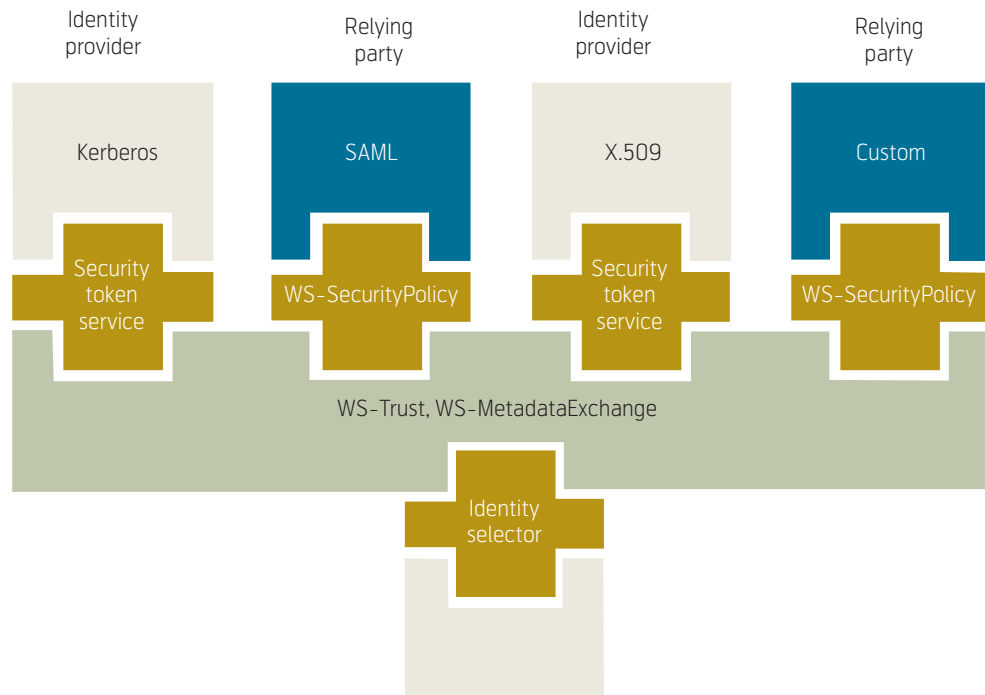


Figure 5

Relying parties express their token requirements via WS-SecurityPolicy (e.g. SAML 1.1 token, X.509-based token).

Identity providers express their token capabilities via WS-SecurityPolicy and do token exchange via Security Token Services (STS) implementing via WS-Trust.

The identity selector pulls everything together, helping the subject match a relying party's requirements to an identity provider's capabilities. 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.

Key Benefits

The key benefits of the identity metasytem are:

- *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 metasytem 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 metasytem 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 metasytem 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 do not 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 metasytem enables new identity technologies to be quickly deployed and utilized within it, 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.

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 smart-cards.

References

Kim Cameron's Identity Weblog. September 21, 2007 [online] – URL: <http://www.identityblog.com>

Microsoft Developer Network. September 21, 2007 [online] – URL: <http://msdn.microsoft.com>

Cardspace in .NET Framework. September 21, 2007 [online] – URL: <http://cardspace.netfx3.com/>

Web Services Specifications. September 21, 2007 [online] – URL: <http://msdn2.microsoft.com/en-us/webservices/Aa740689.aspx>

Microsoft Open Specification Promise. September 21, 2007 [online] – URL: <http://www.microsoft.com/interop/osp/default.mspix>

Acknowledgement

Kim Cameron and Michael B. Jones of Microsoft Corporation.

Ole Tom Seierstad has been with Microsoft Norway for 17 years – his current position is Chief Security Advisor with focus on Microsoft security products and messaging. His previous positions in Microsoft include windows Mobile Evangelist, Technical Support Manager and head of MSN Norway.

email: oles@microsoft.com