The Identity Metasystem: Towards a Privacy-Compliant Solution to the Challenges of Digital Identity

October 2006

Microsoft

Contents

Executive Summary

Just as individual identity is fundamental to our face-to-face interactions, digital identity is fundamental to our interactions in the online world. Unfortunately, many of the challenges associated with the Internet stem from the lack of widely deployed, easily understood, and secure identity solutions. This should come as no surprise. After all, the Internet was designed for sharing information, not for securely identifying users and protecting personal data. However, the rapid proliferation of online theft and deception and the widespread misuse of personal information are threatening to erode public trust in the Internet and thus limit its growth and potential.

Microsoft believes that no single identity management system will emerge and that efforts should instead be directed toward developing an overarching framework that connects different identity systems and sets out standards and protocols for ensuring the privacy and security of online interactions. Microsoft calls this concept the Identity Metasystem. The Identity Metasystem is not a specific product or solution, but rather an interoperable architecture that allows Internet users to use context-specific identities in their various online interactions.

This paper describes the Identity Metasystem and shows how it can meaningfully advance Internet user privacy. In particular, it will show how Microsoft's contribution to the engineering of the Identity Metasystem—the Information Card technology—promotes privacy in three primary ways:

- *First, it helps users stay safe and in control of their online identity interactions by allowing them to select among a portfolio of digital identities and use them at Internet services of their choice. These digital identities may range from those containing no or very little personal information (perhaps nothing more than proof of an attribute such as age or gender) to those with highly sensitive personal information needed for interacting with financial, health institutions, or obtaining government benefits. The key point is that a web site or service only receives the information it needs rather than all of the personal information an individual possesses.*
- *Second, it helps empower users to make informed and reasonable decisions about disclosing their identity information by enabling the use of a consistent, comprehensive, and easily understood user interface. Moreover, this technology implements a number of advanced security features that help safeguard users against identity theft by reliably authenticating sites to users and users to sites.*
- *Third, and more generally, Information Card technology is hardwired to comply with data privacy laws and conforms to key requirements in the European Union's privacy regime, including legitimate and proportionate processing, security, and restraints on secondary use.*

In short, this new framework and new technology offer a cutting-edge solution to the digital identity debacle that is stifling the growth of online services and systems.

Introduction

The Internet has fundamentally altered the way people communicate and exchange information. One change is the extent to which individuals share personal information with others—individuals, businesses, and governments. This, in turn, has created a need for reliable and efficient tools to verify the identity of individuals and organizations so relationships between parties can grow and lead to desired ends.

An Internet user today cannot get far online without having to make certain claims about his digital identity, which in turn will affect his ability to purchase goods or services, communicate with others, and even access his personal information. These identity claims might be weak and lack any independent verification (such as submitting a user name to a Web site). Or they might be stronger claims backed by the assertions of other parties (such as a government-issued identifier or a credit card number). The identity claims required in any given situation will vary depending on the needs, desires, and aims of the parties involved.

The type and amount of information we deem appropriate to disclose about ourselves online depends on the particular relationship we have with the other party. This is not unlike the physical world, where we are accustomed to a multitude of identity management systems and a variety of identifying "tokens"—credit cards, loyalty cards, passports, identity cards, club membership cards, and so on. Adapting this familiar diversity of tokens for secure, private and convenient online use has not been easy.

This paper will describe Microsoft's approach to the problem of identity management on the Internet, which is based on the concept of the Identity Metasystem—a framework intended to connect different identity systems and offer standards and protocols for ensuring privacy and security online. It will also show how identity management solutions that conform to the Identity Metasystem will offer better privacy safeguards than solutions that rely on a monolithic approach.

Note on Terminology

The Identity Metasystem has *components* and *operators*.

The *components* include an identity selector (in Microsoft's case, we refer to this as "**Windows CardSpace**") as well as software used by identity providers and relying parties (again in Microsoft's case, we refer to this as "the **Windows Communications Framework**").Other software providers including IBM, Sun Microsystems, and many others are building similar components relying on the WS-* family of open web services protocols, including WS-Trust, WS-SecurityPolicy, and WS-MetadetaExchange. These components taken together are also referred to as "**Information Card technology**."

The *operators* are various entities or organizations providing services by operating Identity Metasystem components (e.g., banks, governments, individuals, web sites, ISPs and so on).

An "**Information Card**" is the visual icon and underlying metadata that is associated with a given digital identity. Thus, an operator who deploys Information Card technology might instruct a user to "Log in with your Information Card". In this case, the user might be running MacOS, Linux, Windows, or be using a mobile phone, and the non-Windows identity selector software could show a set of Information Cards, just as would the Windows CardSpace software. Operators might also display a logo that represents a generic Information Card, as in "Information Cards accepted here."

Existing ID Card Schemes

Most people routinely use cards to pay for goods and services, enter the workplace, obtain cash from a bank machine, or identify themselves to government agencies. These ID card systems use various techniques to protect the security and integrity of personal data stored on the card, and they use a variety of standards and technologies to fulfill the authentication requirements of the issuing organizations.

For example, many European governments are implementing programs to issue electronic national ID cards to citizens for various purposes such as border control, proving employment status, and facilitating citizens' online transactions with government departments. Although these ID card schemes have led to greater convenience in the delivery of services and have lowered certain risks of identity theft, they are not without controversy. For instance, they might lead to collection of more personal information than is needed or lead third-party organizations to make the ID card a prerequisite for receiving services. Most people are oblivious to such risks or simply accept them as unavoidable drawbacks of such schemes.

Anonymity, Privacy, and Security

Anonymity means that others do not know one's personal identity (or personally identifiable information). Many of us are uncomfortable with the prospect of having our personal information shared with others without our knowledge or approval. In a world characterized by intrusive direct marketing and unsolicited e-mail and telephone communications, our ability to remain anonymous or simply retain a sense of control over our personal information is threatened. By guarding our anonymity judiciously—both online and in the offline world—we can reduce the likelihood of identity theft, avoid the intrusion of unwanted solicitations, and protect our physical and emotional security.

Although ID card schemes are intended to offer a reliable means of identifying individuals and communicating identity claims, they also can allow others with whom we have no desire to form a relationship to acquire information about us. This is a form of ID creep, where the original ID takes on a further use that was never intended. In the United States, for example, the government-issued Social Security number (SSN), which was intended to be used solely for administering social insurance entitlement, is often used by employers to identify employees, by universities to identify students, and by businesses to identify customers. In the UK, the government has proposed a National Identity Register scheme whereby UK residents would have their biometrics enrolled in a central database and a log-file entry would be created each time a national ID card is used to access public or affiliated private-sector services.[1]

Such large-scale identity systems also tend to involve a centralized authentication service or information hub, leading to a concentrated risk of unwarranted and improper data sharing among organizations connected to the hub. It is technically simple for information about an individual's transactions to be pooled from different sources. For example, information held by the government about each card holder as passport owner, benefit claimant, taxpayer, patient, and resident might be aggregated at a single point of reference, with all the attendant risks of improper information sharing, data mining, and profiling by government agencies and even private enterprises.[2] The use of centralized data repositories carries the added risk of having a single point of failure.

Privacy intrusions can also arise from the process of applying for an ID card, such as when an applicant is required to submit more information than is appropriate or relevant given the card's intended function. For instance, it would be unduly intrusive and improper for a retailer to demand that customers divulge information about their religious beliefs in order to obtain a store credit card. In principle, technological advances that produce "smarter" ID cards can address all of these problems, but in practice, privacy risks receive insufficient attention at the design stage.[3] Or they may arise from disproportionate and improper processing of the card holder's personal information by third parties who are not part of the original

---

[1] See *The Identity Project: An Assessment of the UK Identity Cards Bill and Its Implications*, London School of Economics, June 2005 (http://is2.lse.ac.uk/idcard/identityreport.pdf), for a detailed discussion of the UK Government Identity Card proposal.

[2] See *Who Goes There?: Authentication Through the Lens of Privacy*, National Academies Press, 2003, for a discussion of privacy concerns in authentication systems.

[3] See Recommendation 3 in Tony Mansfield and Marek Rejman-Greene, *Feasibility Study on the Use of Biometrics in an Entitlement Scheme (for UKPS, DVLA and Home Office)*, February 2003 (http://www.identitycards.gov.uk/library/feasibility_study031111_v2.pdf`) (link now defunct).

identity relationship but instead misuse the card as a convenient way to identify the card holder. For example, a hotel should not insist upon a government-issued benefits identification card in order to rent a room for the night. The hotel has no reason to collect or store the information in such a card and doing so only heightens the risks of improper data use.

The Identity Metasystem

The Identity Metasystem[4] is based on the premise that no single, universal identity management system will emerge on the Internet, and that attempts to create one are misguided and, in fact, counterproductive with respect to security and privacy. What is needed instead is an overarching framework that enables identity systems to interoperate with one another by exchanging context-specific tokens of identity in online interactions.

The Identity Metasystem is a set of protocols that will connect existing identity systems, in the same way that the advent of TCP/IP in the 1980s enabled the interoperability of networks that used Ethernet, Token Ring, ArcNet, or Frame Relay as the underlying layer. The system will allow a variety of technologies from many IT vendors to recognize each other and publish their service requirements and capabilities through a common set of standards and design principles.[5] Existing vendor-neutral communication standards based on SOAP and XML will make this possible. These include WS-Security, WS-Trust, WS-MetadataExchange, and WS-SecurityPolicy.[6] And, from a privacy perspective, the Identity Metasystem does not entail Microsoft or anyone else acting as a central repository of users' personal information, or as a "root of trust" for verifying identity. Instead, a multiplicity of public and private institutions will manage digital identities using a plurality of technologies from many IT vendors.

The Seven Laws of Identity

The Identity Metasystem is based on seven universal design principles developed by Kim Cameron of Microsoft, which he has named the "Laws of Identity."[7] Long experience has proven that these principles are essential to maintaining good online security and privacy.

1. User control and consent
2. Minimal disclosure for a defined use
3. Justifiable parties
4. Directional identity
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts

Systems that breach these laws tend to fail, both functionally and commercially. Moreover, all of the laws together are necessary to safeguard against the security and privacy problems associated with centralized, monolithic ID systems.

We describe each law briefly below:

---

[4] See "Microsoft's Vision for an Identity Metasystem" (May 2005), http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/identitymetasystem.asp.

[5] See Michael B. Jones, "The Identity Metasystem: A User-Centric, Inclusive Web Authentication Solution," Position Paper for the W3C Workshop on Transparency and Usability of Authentication (2005), http://research.microsoft.com/~mbj/papers/InfoCard_W3C_Web_Authentication.pdf.

[7] Microsoft's recently announced Open Specification Promise (OSP) covers this (and other) specifications. See "Microsoft Open Specification Promise" (September 2006), http://www.microsoft.com/interop/osp. The OSP is intended to assure that the broadest audiences of developers and customers working with commercial or open source software can implement the covered specifications.

[7] See Kim Cameron, "Laws of Identity," http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/lawsofidentity.asp.

User control and consent (Law 1). The user must be able to verify that parties requesting identity-related claims are legitimate, and the purposes for which the information is sought must be transparent to the user. This principle recognizes that without user control and consent, an identity system will fail to earn the user's trust or sustain it over the long term.

Minimal disclosure for a constrained use (Law 2). Identity systems should solicit only the amount of identifying information needed for a given context and limit use of that information to purposes relevant to that context. For example, an identity system should not procure or retain an address and telephone number simply because they might prove useful at some future time.

Justifiable parties (Law 3). Personal information should be disclosed only to parties who have a necessary and justifiable place in the identity relationship. Users must be aware of whom they are interacting with when making identity claims and who will receive their identifying information.

Directed identity (Law 4). The system must support both omni-directional identifiers, which act as a "beacon" to all the world (such as company URLs) and uni-directional identifiers, which are limited to a particular relationship between two parties (such as a user interacting with a bank online).

Pluralism of operators and technologies (Law 5). The system must accommodate diverse technologies used by different operators in different contexts. In fact, it should encourage the coexistence of a plurality of operators and technologies.

Human integration (Law 6). To be truly secure, the system must be perceived by human users as highly reliable and predictable. The more subjective, ambiguous, or complex the user interfaces are, the less secure the entire system will be.

Consistent user experience across contexts (Law 7). Diverse identity systems should interact with users in a consistent and uniform manner while still allowing for different underlying technologies. Ideally, people will develop a reliable intuition about how to manage a plurality of digital identities safely, just as people manage a wallet filled with cards or a ring of keys. As in the real world, people can pick and choose the identity that suits them best for each occasion.

Roles

The Identity Metasystem includes three central roles. (A given party can assume more than one of these roles.)

- **Identity provider:** The person or organization that issues a digital identity, either on its own or on another's behalf. For example, an online bookseller might issue identities to its customers, a government might issue identities to its employees, or a third-party service might issue identity tokens verifying age for use at another site.
- **Relying party:** The person or organization requiring a digital identity before granting access to a user or processing a customer order. A relying party can specify the identity claims it requires and the formats it accepts and process credentials from multiple identity providers.
- **Digital subject:** The individual or entity about whom identity claims are made.[8]

Microsoft's Information Card Technology: Windows CardSpace

The general architecture of the Information Card technology is fairly straightforward. It uses the metaphor of an ID card to describe a digital identity. An Information Card does not contain personal data.

[8] See Kim Cameron and Michael B. Jones, "The Design Rationale Behind the Identity Metasystem Architecture," http://www.identityblog.com/wp-content/resources/design_rationale.pdf, for further discussion of roles in the Identity Metasystem and related architectural issues.

Rather, it acts as a pointer to the identity provider of the card, which in turn supplies encoded identity claims about the user when a relying party requests them and the user authorizes their release. Microsoft refers to its processing engine for this operation as Windows CardSpace. It determines which of the user's available Information Cards can meet the relying party's identity requirements. When a user clicks on an Information Card from her portfolio of identities, Windows CardSpace obtains security tokens containing identity claims from the identity provider that issued the card.

The Information Card architecture is best understood by observing its operation. The following sections describe the two primary scenarios in which Information Card technology interacts with Web sites. In the most basic case, the Web site provides all the relying party functionality via HTML extensions transported over HTTPS. The second case is similar except the relying party employs Security Token Server (STS).[9]

Scenario One: Basic Protocol Flow

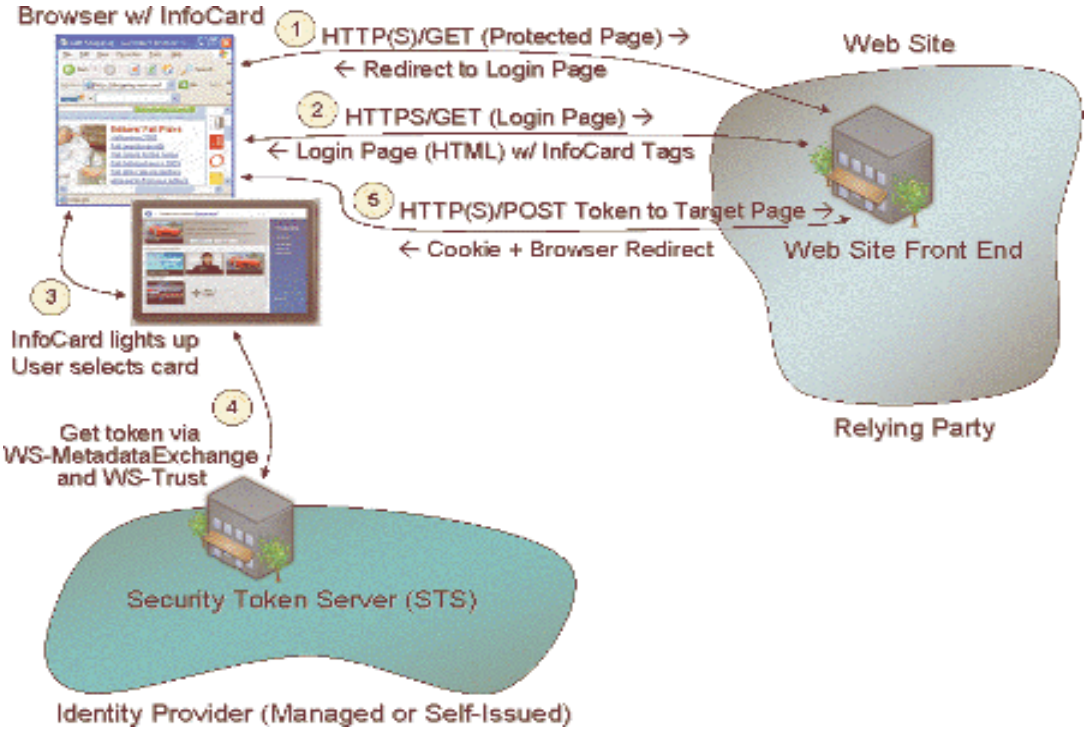


Figure 1: Basic protocol flow when using an Information Card for authentication at a Web site

Figure 1 shows an example of the basic protocol flow when using an Information Card to authenticate an individual at a Web site that employs no relying party STS. Steps 1, 2, and 5 are essentially the same as for a typical forms-based login. The key difference is that the login page returned to the browser in step 2 contains an HTML tag that allows the user to choose an Information Card for authentication at the site. When the user selects this tag, the browser invokes the Information Card protocols and user experience, and it triggers steps 3 through 5.

In step 3, the browser invokes Windows CardSpace, passing it parameter values supplied by the Information Card HTML tag. With Windows CardSpace, the user then chooses an Information Card and authenticates herself at that site. Step 4 uses standard Identity Metasystem protocols to retrieve a security token that represents the digital identity selected by the user from the STS as the identity provider for that identity.

[9] See Michael B. Jones, "A Guide to Supporting InfoCard v1.0 Within Web Applications and Browsers," (Microsoft whitepaper, March 2006), http://msdn.microsoft.com/windowsvista/reference/default.aspx?pull=/library/en-us/dnwebsrv/html/infocardwebguide.asp.

In step 5, the browser posts the token back to the Web site using a HTTP(S)/POST. The Web site validates the token, completing the user's Information Card–based authentication to the Web site. Following authentication, the Web site typically writes a client-side browser cookie and redirects the browser back to the protected page.

Note that this cookie is likely to be exactly the same cookie that the site would have written back had the user been authenticated via some other means, such as a forms-based login using a username and password. The impact on Web sites is minimal. Other than its authentication subsystem, the bulk of a Web site's code can remain completely unaware that Information Card–based authentication has been used. The site just uses the same kinds of cookies that it always has.

Scenario Two: Protocol Flow with Relying Party STS

In the previous scenario, the Web site communicated with Windows CardSpace using only the HTML extensions enabling Information Card use, transported over the normal browser HTTP or HTTPS channel. In this second scenario, the Web site also employs a relying party STS to do part of the work of authenticating the user, passing the result of that authentication to the login page via HTTP(S) POST.

A site might choose this solution for a number of reasons. One reason might be that the same relying party STS can be used to do the authentication work for both browser-based applications and smart client applications that use Web services. Second, this solution allows the bulk of the authentication work to be done on servers dedicated to this purpose, rather than on the Web site's front-end servers. Finally, this solution enables front-end servers to accept site-specific tokens rather than the potentially more general or more complicated authentication tokens issued by identity providers.

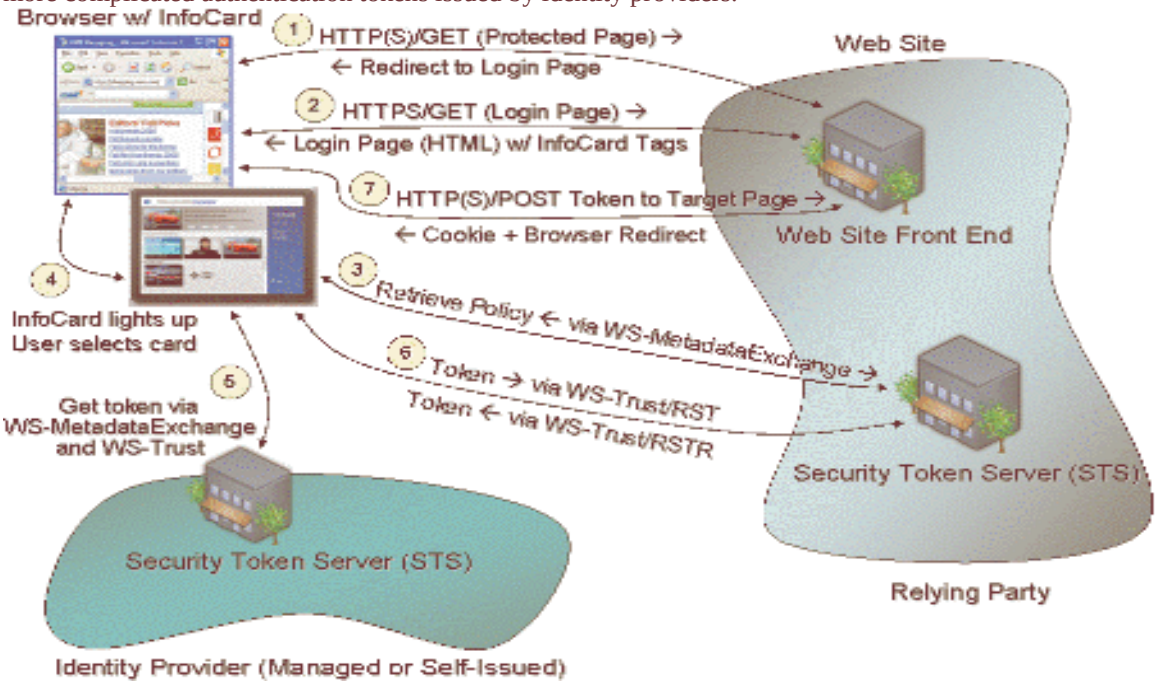


Figure 2: Protocol flow when using an Information Card to authenticate at a Web site that employs a relying party STS

This scenario is similar to the previous one, with the addition of steps 3 and 6. The differences start with the Information Card information supplied to the browser by the Web site in step 2. In the previous scenario, the site encoded its WS-Security Policy information using Information Card HTML extensions and supplied them directly to the Information Card–extended browser. In this scenario, the site uses different Information Card HTML extensions in the step 2 reply to specify which relying party STS should be contacted to obtain the WS-Security Policy information.

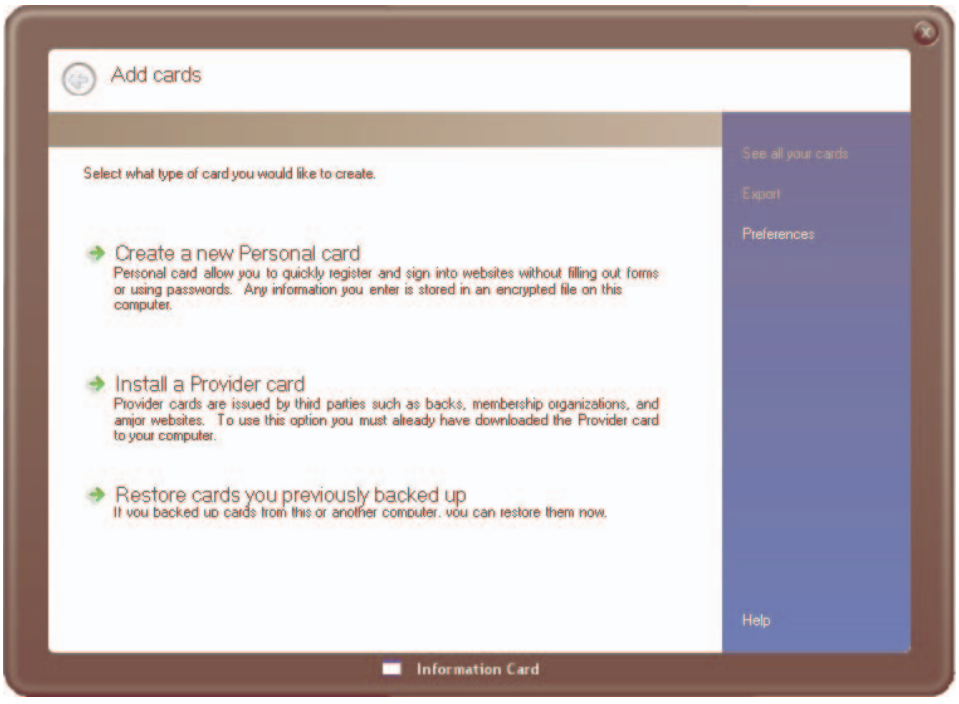
In step 3, Windows CardSpace contacts the relying party STS specified by the Web site and obtains its WS-Security Policy information via WS-Metadata Exchange. In step 4, the Windows CardSpace user interface is shown and the user selects an Information Card to use at the site. In step 5, the identity provider is contacted to obtain a security token for the selected digital identity. In step 6, the security token is sent to the Web site's relying party STS to authenticate the user, and a site-specific authentication token is returned to Windows CardSpace. Finally, in step 7, the browser posts the token obtained in step 6 back to the Web site using HTTP(S)/POST. The Web site validates the token, completing the user's Information Card–based authentication to the Web site. Following authentication, the Web site typically writes a client-side browser cookie and redirects the browser back to the protected page.

User Experience

The Information Card user experience at Web sites is intended to be intuitive and natural enough that the users' perspective will simply be "That's how you log in." Web sites that require authentication typically ask the user to supply a username and password at login. With Information Cards, they instead ask users to supply an Information Card. Some sites will choose to accept only Information Cards, while others will give users the choice of using Information Cards or other forms of authentication. In any event, as the following discussion illustrates, users will find it easy to create, manage, and submit Information Cards for login purposes.

Creating an Information Card

Even novice users will find it relatively easy to create an Information Card. The process is launched with the following dialog box.



Users can select between two types of Information Cards:

- **Personal card:** Commonly referred to as a *self-issued card*, this is created and maintained by the user in the Information Card user interface. It has a small and fixed set of claims.[10] Personal cards are stored locally, as is the personally identifiable information associated with the cards.

[10] Personal cards are limited to a select number of commonly used claims, including name, address, e-mail address, date of birth, gender, and phone number. They contain no sensitive data such as national ID numbers or credit card

- **Provider card:** Commonly referred to as a *managed card*, this card is supplied to the user by an identity provider (such as an employer, financial institution, or government) in the form of a signed .crd file and installed in the Information Card system by the user. The set of claims associated with a provider card is not limited in any way but is instead determined by the identity provider. (For example, an employer might provide an employee number claim, a bank might provide an account number claim, and so on.) Once installed, provider cards are stored locally, but the personally identifiable information associated with a card is not stored on the user's computing device. Rather, the data is stored by the identity provider that supplied the card.

After the user selects the type of card to create, a series of additional dialog boxes prompts for the entry of relevant data. Once the card has been created, the user can view the entered information in the Card Details dialog box:

Although the dialog box states that the card "contains" the data entered and that the card "has never been sent," the card itself contains only claim metadata (in this case, a First Name claim, a Last Name claim, a Locality claim, and so on). Also, the card is *never* sent unless the user explicitly exports it and e-mails it to someone. Instead, the card contains information about how to generate a security token containing the claim data, and it is this security token that travels over the wire, *not* the card. From the user's perspective, however, it is most intuitive to imagine that the card is presented to a Web site or service. This is our experience in the real world, so this is the language and metaphor used in the user interface.

Logging In with an Information Card

Sites that accept Information Cards will typically have a login screen that contains a button with a label such as "Sign in with an Information Card" or "Log in using an Information Card." If the user clicks this button, the subsequent site verification screen (upon first use of Information Cards at a site) will look something like this:

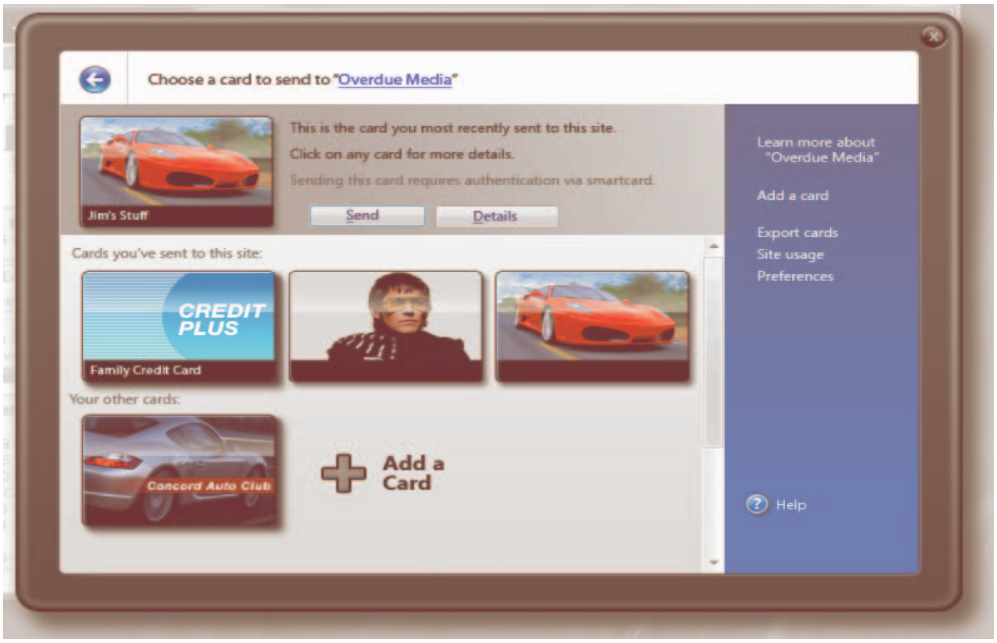
information. See Appendix A in "A Guide to Integrating with InfoCard v1.0" (Microsoft whitepaper, August 2005), http://msdn.microsoft.com/winfx/reference/infocard/default.aspx.

As this example shows, the site verification screen can include the organization's name, location, Web site URL, and logo. It can also include the name and logo of the organization that has verified this information. To help the user make good decisions about which sites to trust, the user interface will vary depending on what kind of certificate is provided by this identity provider or relying party. If a so-called Extended Validation certificate is provided, the screen can indicate that the organization's name, location, Web site, and logo have been verified. This indicates to a user that the organization deserves a higher level of trust. If only an SSL certificate is provided, the screen will indicate that a lower level of trust is warranted. If an even weaker certificate or no certificate at all is provided, the screen will indicate that there is no evidence that this site is what it claims to be.

The site verification screen is presented only the first time that Information Cards are used by the user at that site. Once the user has confirmed the identity of the site, he is taken straight to the card selector screen upon subsequent uses.

Submitting an Information Card

The card selector screen enables a user to select an Information Card to use at a site:



As this screen shows, each digital identity is displayed as an Information Card. Each card represents a digital identity that the user can present to a relying party and contains information about a particular digital identity—including what identity provider to contact to acquire a security token for this identity, what kind of tokens this identity provider can issue, and exactly what claims these tokens can contain. By choosing to use a particular card, the user is actually choosing to request a specific security token with a specific set of claims created by a specific identity provider. But from the user's perspective, she is simply selecting an Information Card to use at a site. In any event, once the user selects a card and submits it to the site, she is logged in and can use the site just as she would after submitting a username and password.

Example of Information Card Interaction

The Information Card–based interactions described in the previous section are best illustrated with a real world example. John Kane is an employee of Fabrikam, Inc. Fabrikam has a partnership with Blue Yonder Airlines, which makes travel arrangements for Fabrikam employees and offers tickets at specially discounted prices.

Fabrikam has issued Information Cards to all its frequent-traveler employees, including John, to prove that they are employees of Fabrikam. It also runs an STS at the address *http://fabrikam.com/employee/sts*, which issues security tokens for the issued Information Cards. Fabrikam has also given those employees smart cards to use as strong two-factor credentials for authenticating to the employee STS when using their Information Cards. Employees of Fabrikam use a special travel reservation smart client application for requesting travel arrangements from Blue Yonder Airlines, which runs a travel portal and airline reservation service at the address *http://fabrikam.com/employee/sts*

When John runs the smart client reservation application on his PC to make travel reservations with Blue Yonder Airlines, the following interactions occur.

1. The travel reservation client application obtains the security policy of the airline reservation service at *http://fabrikam.com/employee/sts*using the WS-MetadataExchange protocol. The travel portal service policy requires that the client application submit a security token issued by the user's employer STS, namely the Fabrikam STS at *http://fabrikam.com/employee/sts***.** (There is a trust relationship between the airline reservation service and each partner company STS with which it federates.)

2. The travel reservation client application requests the Windows CardSpace component on John's PC to produce a security token that can satisfy the reservation service policy. Windows CardSpace displays the matching Information Card (the one given to John by his employer), and John selects and approves it for use.
3. The CardSpace on John's PC obtains the security policy of John's employee STS at *http://fabrikam.com/employee/sts* using the WS-MetadataExchange protocol to determine the security binding to use for the message channel for requesting the security token.
4. The employer-issued Information Card selected by John specifies the required authentication mechanism to be X509 certificate based, and the CardSpace user interface prompts John to insert his corporate smart card into the reader and enter his PIN.
5. CardSpace authenticates to the Fabrikam employee STS at *http://fabrikam.com/employee/sts* using the X509 certificate from John's smart card, and it requests a security token with the required claims specified by the airline reservation service. Upon successful authentication, it receives the security token.
6. CardSpace hands the requested security token to the travel reservation application running on John's PC.
7. The travel reservation application running on John's PC presents the token obtained from CardSpace and presents it to the travel portal service along with proof of possession to gain access.
8. John can look at his travel options and request reservations.

Privacy Benefits of Windows CardSpace and the Information Card Model

The Information Card model of identity management readily demonstrates the Laws of Identity at work. For instance, consistent with the Law of User Consent and Control, users will be responsible for selecting and submitting an appropriate set of identity claims and using them to acquire services over the Internet, where Relying Parties accept them as sufficient proof of identity. If users feel uncomfortable making the disclosures accompanying a particular card, they can decline to use it. Users can also create self-issued Identities – i.e., act as their own Identity Providers. Because users will have an array of cards, all containing different amounts of identifying information, it will help ensure that Relying Parties only obtain and process an appropriate amount of identifying information from the user.

In line with the Law of Pluralism of Operators and Technologies, users will be able to construct multiple digital identities -- differing in the amount and quantity of identifying information they contain. In other words, users will be able to "carry" in their digital "wallets" "cards" ranging from those containing no personal information but perhaps proof of an attribute such as age or gender, to cards for interacting with sites on an ongoing and more private basis, to cards for collaborating with an employer or public agency, thus additionally satisfying the Laws of Minimal Disclosure and Justifiable Parties. The capability to create and use multiple self-issued cards guards users against profiling, consistent with the Law of Directed Identity. Microsoft has no plans to allow users to include or store sensitive identifying information (such as government identifiers or credit card numbers) on a self-issued Information Card, though third-party identity providers could offer cards containing such information. In these and other ways, the Information Card model conforms to the demands imposed by the Identity Metasystem and its Laws.

Protection of Users Against Identity Attacks

Further, Information Card technology helps protect users against the significant and growing threat of identity attacks. Many identity attacks succeed because the user was fooled by something presented on screen, not because of insecure communication technologies. Consider two particularly noxious examples, spoofing and phishing. Spoofing uses a fake sending address to disguise the origin of a message. This might be done legitimately to redirect responses to an account other than the one actually sending the message. However, it can also be done to impersonate another sender for the purposes of obtaining a user's e-mail address for sending out spam or to gain illegal entry into a secure system. Phishing is a scam whereby the sender sends out legitimate-looking e-mails that appear to come from a well-known and trustworthy site, in an effort to "fish" for personal or financial information from the

recipient. Neither type of attack requires sophisticated technical knowledge or tools—they simply rely on tricks to fool users into disclosing critical information.

Information Cards help address the unique challenge of these and other types of identity attacks by making it easier for users to stay in control when accessing resources on the Internet. Specifically, the following features position Information Card technology as a leading solution for addressing these rapidly evolving threats:

- **Secure identity creation.** The identity creation process is arguably the most important step in any digital identity solution. That is why the Information Card creation process is designed to be both intuitive and highly secure. For example, the dialog box for creating a card will run on a separate, secure desktop. The background will be frozen and grayed out, and users will not be able to access their normal desktops—including Task Manager—until they close the dialog box. This user interface will also be very difficult for a criminal hacker to reproduce, especially from within a browser.

- **Authenticating sites to users: Extended Validation certificates.** To prevent users from being fooled by counterfeit sites, a reliable mechanism is needed that helps distinguish between genuine sites and imposters. The Information Card solution uses a new class of higher-value X.509 site certificates that Microsoft is jointly developing with VeriSign and other leading certificate authorities and browser companies.[11] These Extended Validation (EV) certificates will differ from existing SSL certificates in several respects. First, they will be issued according to authentication criteria that will be standard across Certificate Authorities (CAs) and subject to audit for accuracy. (There are currently no standard criteria, so SSL certificates might be issued shortly after a credit card clears without regard for who requests it or whether all the information in the certificate is valid.) With EV certificates, the CA will be responsible for confirming any information related to the certificate, including the legal identity of the corresponding organization and the authority of the person requesting it. Second, Microsoft Internet Explorer 7 and other browsers (including Opera, KDE, and Mozilla) will display an EV SSL certificate in a green-colored browser bar as a visual cue to the user that the certificate was issued against EV criteria. These new EV certificates will be used to identify e-commerce and other Web sites that support Information Cards, as well as to identify vendors that are signing their code for distribution on the Microsoft Windows platform. EV certificates might be extended in future browser releases to display a digitally signed bitmap of a company's logo.

- **Reduced use of passwords and reduced need to store personal data.** The Information Card technology will reduce the use of passwords and other similarly insecure logon information. Indeed, Information Card offers some key advantages over username/password credentials:

    - No password is typed or sent, so no password can be stolen or forgotten.
    - Because authentication is based on unique keys generated for every Information Card/site pair (unless the user is using a card explicitly designed to enable cross-site collaboration), the keys known by one site are useless for authentication at another, even for the same Information Card.
    - Because Information Cards supply claim values (such as name, address, and e-mail address) to relying parties on demand, relying parties do not need to store this data between sessions. In this way, the Information Card technology reduces the need for Web sites to request and retain personal data and thereby narrows a classic attack vector for identity theft.

[11] The CA and browser communities are completing the Extended Validation certificate issuance criteria in the fall of 2006. Microsoft will support final or interim criteria in its Windows Root CA Program, and it will enable pilot deployments of Extended Validation SSL certificates for major Web sites before the final release of Internet Explorer and Windows Vista.

- **Standard interfaces.** The Information Card technology uses a standard user interface for working with digital identities, which helps prevent users from being fooled by some of the tricks and con games employed by identity attackers.

Information Card Technology and EU Data Privacy

The Identity Metasystem does not mandate any specific identity system; rather, it presupposes many systems and many different technologies. Microsoft is already building software that will take part in the Identity Metasystem—namely, the Information Card technology. We expect other companies will develop separate technologies and components to meet the various needs of identifying parties, relying parties, and digital subjects. This final section of the paper will examine ID card schemes within the framework of EU privacy, and then it will address how Information Cards specifically address the problem of managing digital identities in a way that conforms to the EU's data privacy laws.

Overview of EU Data Privacy Law

The EU's data privacy regime arises out of two directives: the framework Data Protection Directive 95/46/EC (Directive) and, more recently, the Electronic Communications Data Protection Directive 02/58/EC (ECDP Directive). The first directive sets forth the EU's principal rules regarding the processing of personal data by organizations that were established in an EU member state or that use equipment in an EU member state to process that data. The second directive offers additional data privacy rules for organizations that are public electronic communications network providers or public electronic communications service providers. In line with general EU legislative principles, the two directives do not have direct effect, but require local implementation by individual EU member states.

The jurisdictional provisions of the framework Directive establish that the EU's data privacy rules apply to organizations—called "data controllers"—that were established in the EU (in a bricks-and-mortar sense) or make use of equipment in the EU to process personal data. Papers published by the Article 29 Working Party, which is made up of data privacy regulators from each of the EU member states, make clear that an organization can be subject to EU jurisdiction even if it does not own or necessarily control the equipment used to process the personal data.[12] With respect to ID card schemes, these rules establish that when the identity provider (usually the organization responsible for devising and issuing the ID card, such as a government agency, a business, or an employer) and/or the relying party (the entity accepting the card as proof of identity or for some other purpose) is situated in an EU member state, EU data privacy laws apply. Note, however, that EU data privacy laws do not apply to most state-run ID card schemes because these schemes typically involve the processing of personal information for purposes of national security, defense, or activities of the state connected to the enforcement of criminal laws. This places them outside the scope of the Directive per Article 3, or they are otherwise considered "identifiers of general application" regulated by national data privacy law or national regulation concerning state ID cards.

Where the jurisdictional requirements of the law are met, the EU's data privacy regime regulates the processing of "personal data"—defined broadly by the framework Directive to mean any information relating to an "identified" or "identifiable" natural person (the "data subject"). Member states that have implemented the laws have largely been faithful to the Directive's formulation of the term "personal data," ensuring that their laws apply not only where information *on its face* identifies an individual (e.g., John Smith living at *x* address), but also where the information can be used *indirectly* to identify an individual in combination with other information held or easily procured by the organization. Significantly, a number of European privacy regulators even take the position that information is "identifiable" to a person, and is hence personal data, as long as someone, somewhere (and not necessarily the organization that holds the information), can attribute it to a particular individual. So, for instance, many Data Protection Commissioners have developed the view that an IP address can be considered protected personal data because it might be possible for an Internet service provider (although

[12] See Article 29, "Data Protection Working Party, Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Web Sites," WP 56, 5035/01/EN/FINAL (May 30, 2002).

not necessarily the organization processing the IP address) to attribute it to a living individual. This sharpening of interpretation has understandably coincided with the growth of mandatory data retention for the purposes of identification for law enforcement.

It is clear that ID card schemes almost inevitably entail some degree of collection and processing of "personal data" as defined under EU privacy laws. Certainly, any ID card meant to have broad utility and function across a range of identity relationships can be expected to involve some initial collection and processing by the card issuer of personal data on the prospective card holder. For example, a customer will be asked to complete and submit a registration form requiring the submission of personal data in order to obtain a credit card or a citizen will be asked to submit a detailed application form in order to receive a government-issued ID, such as a passport. Of course, it is possible to imagine a scheme that involves no processing of personal data from individuals, but then it also appears obvious that any resulting card (an "Anonymity Card") will have no "value" for expressing identity claims within a broader set of relationships. Surprisingly, this intuition is false, and by employing advanced techniques in cryptography, useful "private credentials" can be engineered with interesting properties. Stefan Brands[13] and Jan Camenisch,[14] among others, are currently investigating the viability of such solutions. For example, it should be possible to perform successive strong authentications without the Relying Party being able to link transactions to the same Subject, and the Subject may withhold different attributes from different parties using the same credential, and these properties have very useful application to e-government.[15]

Relying parties that accept the ID card as a valid form of identity are also considered to process personal data, potentially as "co-controllers" with the identity provider, although neither the relying party nor the identity provider are under any obligation to retain particular kinds of data (transaction logs, for example). Relying parties might not be involved in the initial collection and processing of personal data that precede the production of the card, but they will acquire whatever information is within or on the face of the ID card. Most widely deployed ID cards convey the holder's name, address, and other contact details, so relying parties might receive personal data in this direct fashion. But even when a card does not directly identify the holder, the relying party might be deemed to process personal data if the identity of the card holder can be ascertained from information available from the card and from other information that the relying party receives about the card holder in the course of dealing with the card holder.

Data Controllers and Their Legal Obligations

The substantive obligations arising under EU data privacy laws apply to data controllers, which determine "the purposes and means of" processing personal data. Data controllers can be contrasted with "data processors," which are organizations that act on behalf of or under the instructions of the data controller and are not directly liable under EU data privacy laws. It is clear that the principal entities in ID card schemes will generally qualify as data controllers. But it is possible to imagine that an identity provider might act purely as an agent on behalf of relying parties, in effect providing an identification service for clients. Some of this work might entail production of some form of ID (for example, if a firm screens job applicants and then issues security badges for those that are hired). Such organizations arguably are not controllers, but function as processors on behalf of the actual controller.[16]

---

[13] See generally Stefan A. Brands, Rethinking Public Key Infrastructures and Digital Certificates, MIT Press (2000); see also http://www.credentica.com/faq.php.

[14] For a list of relevant publications by IBM Researcher Jan Camenisch, see http://www.zurich.ibm.com/security/privacy

[15] See generally, Dr. Niklas Auerbach, Anonymous Digital Identity in e-Government, http://www.ifi.unizh.ch/ifiadmin/staff/rofrei/Dissertationen/Jahr_2004/thesis_auerbach.pdf

[16] Even under these circumstances, where the purpose for the processing is determined by the organization's client, it might yet be deemed a data controller purely on the basis of its control over the means of the processing.

By virtue of their status as data controllers, both identity providers and relying parties in the ID card context are required to comply with the substantive obligations arising under the Directive, as those have been implemented by individual EU member states. Although a comprehensive discussion of all the applicable data privacy rules and their national implementation is outside the scope of this paper, we will note the following EU data privacy rules, many of which find expression and support within the Information Card technology:

- The manner in which a data controller collects and processes data must be "fair and lawful." This requirement includes providing appropriate disclosures to individuals regarding how their personal data will be processed.[17]

- A data controller must ensure that its processing of personal data is legitimate—that is, it must fall within one of permissible grounds set forth in the Directive. The processing of both ordinary and "special category" (sensitive) data, which the Directive defines as data revealing an individual's racial or ethnic group, political opinions, religious or philosophical beliefs, trade-union membership, health, or sex life, is legitimate where it takes place with the explicit consent of the relevant individual.[18]

- A data controller can collect and process only personal data that is "relevant" and "adequate" to achieve its given purposes or aims, and it must refrain from "excessive" collection of personal data. Moreover, the data controller must ensure that the data it holds is accurate and up-to-date.[19]

- A data controller must be responsive to requests made by individuals to access their data, see any identifiable records of data usage (known as a "subject access" request), and correct any inaccurate data referring to them.[20]

- A data controller must ensure that the personal data it possesses or controls remains subject to suitable security protections, including appropriate technical and organizational measures.[21]

- A data controller is prohibited from transferring personal data to any country outside the EU unless that country ensures an "adequate" level of protection for the rights and freedoms of individuals with respect to the processing of their data.[22]

EU Data Privacy Laws and Information Cards

The Information Card technology, by operating in accordance with the Laws of Identity, will materially assist the principal online parties—identity providers and relying parties—in satisfying key requirement set forth arising under EU data privacy laws. Compliance also depends on responsible implementation and use of the technology, however. The technology itself cannot ensure that the relevant parties fully or even substantially comply with EU, or any other, privacy laws. That said, we believe that the Information Card technology, by conforming to the Laws of Identity, is hardwired to comply with data privacy laws and protects privacy in four primary respects: legitimate processing, proportionate processing, security, and restraints on secondary use.

---

[17] See Data Protection Directive 95/46/EC, *Arts,* 10-11.

[18] *Id.* at Arts, 7-9.

[19] *Id.* at Arts, 6-7.

[20] *Id.* at Arts, 12.

[21] *Id.* at Arts, 16-17.

[22] *Id.* at Arts, 25-26.

Legitimate Processing

The Information Card technology will help to ensure that any processing of personal data by the relevant identity providers and relying parties is legitimate, and therefore legal, by virtue of taking place only with the user's unambiguous consent (Article 7 of the Directive). In the Information Card model, users have control over whether and when to acquire and use an Information Card to access any online services. Use of a particular card in a given context reflects the user's informed choice of what personal data to share, first with the identity provider (to obtain a satisfactory card) and then with the relying party (to access services).

Information Cards are also designed so that before a user acquires a particular card, he will see a link to the privacy policy of the identity provider describing how any personal data submitted will be used. This is particularly important when the identity provider intends to use any submitted data for purposes other than issuing the card. Similarly, before a particular card is deployed to a relying party, the user will see a link to the relying party's privacy policy and can learn whether the relying party intends to use the data for purposes beyond identity verification. The Information Card model thus allows the user to make not merely a choice, but an informed choice as called for by the Directive.[23]

Proportionate Processing

Information Cards also foster adherence to the requirement that organizations process only the minimum amount of personal data needed to accomplish desired aims. This principle of proportionate processing finds expression in Article 6 of the Directive. Delivering suitable identity claims (and associated personal data) that match a relying party's specific needs—rather than data that bears no relevance to the contemplated interaction—is one of the defining features of the Information Card model.

As we have seen, traditional wide-scale ID card schemes involve the creation of a single card containing personal data that is used to identify the card holder in a wide array of identity relationships, including those where some or much of the information on the card is excessive in light of the relying party's actual needs. So, while one Relying Party may legitimately need to know the card holder's home address and have access to a photo of the holder, another may just need to know that the individual is over the age of 18. Information Cards allow users to tailor the submission of their personal data to meet the particular needs of an online service provider by selecting the appropriate Information Card containing the necessary identity claims. For service providers that require more extensive personal data, users will be shown Information Cards that transmit a security token containing the appropriate identity claims. For service providers requiring less information, other Information Cards will be shown. If the user considers the information excessive, he or she can simply withhold use of the identified Information Cards. In this way, Information Cards help to ensure that service providers only receive personal data that are "adequate, relevant and not excessive."

Security

The Information Card model is designed so that the relevant disclosures of personal data among users, identity providers, and relying parties takes place under secure conditions, as required by EU laws. Article 17 of the Directive states that an organization must implement "appropriate technical and organizational measures" to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. As noted earlier, inadequate security is a failing common to many ID card schemes, particularly those involving the accumulation of card holder data in a single repository or database. Information Cards, however, contain a number of features that will enhance

[23] While consistent with current privacy law and practices, this approach should be considered only a first step. There is evidence that many users fail to review the terms of privacy policies or act on them in an informed manner. Far better would be a system enabling web sites to represent privacy policies in a simple, iconic fashion analogous to food labels. This would allow consumers to see at a glance how a site's practices compared to those of other Web sites using a small number of universally accepted visual icons that were both secure against spoofing and verified by a trusted third party. This more refined approach is a long-term objective of many privacy advocates and one that Microsoft strongly supports.

the security of the user's personal data when used for purposes of online identification. The Information Cards that appear to users on their computer screen will not contain any personal data and thus cannot become a target for hackers and others. The cards are simply tokens that enable the flow of encoded identity claims from identity providers to relying parties. Further, unlike most wide-scale ID card schemes, the Information Card model does not entail the creation of a dedicated data repository or database for the storage of users' personal data. Identity providers and relying parties will still receive personal data, of course, and be responsible for ensuring that it is kept secure.

Further, in the Information Card model the request for and issuance of a security token containing identity claims requires strong two-way authentication. Security tokens returned by the user's identity selector to a service provider are encrypted by Windows CardSpace (if they have not already been encrypted by the identity provider) to guarantee that only the relying party approved by the user can examine the contents of the security token. Information Cards also help prevent the tracking of the user's online behavior by identity providers. Windows CardSpace, by default, will not disclose the relying party's identity to the identity provider when requesting security tokens from it. Also, the initial request and receipt of an Information Card token from any given identity provider will be subject to its own authentication process.

Limits on Secondary Use

Finally, Information Cards will serve to deter identity providers and relying parties from engaging in impermissible, secondary processing of user personal data. This "finality" principle finds expression in Article 7 of the Directive, which states that personal data cannot be further processed by a data controller in a way that is incompatible with the original, identified purposes. As noted earlier, the default setting in Windows CardSpace is that identity providers will not learn the identity of the relying party, which could enable them to construct a detailed user profile. The Information Card technology also makes sure that the privacy policies of both relying parties and identity providers are communicated to users in an intelligible form, which would reveal to the user any intended secondary uses of the personal data. Of course, organizations can ignore their own policies, but not without violating EU data privacy laws.

Thus, in at least four respects—legitimate processing, proportionate processing, security, and limits on secondary use—the Information Card model directly promotes compliance with EU data privacy laws. These privacy-enabling features of Information Cards are simply a byproduct of adherence to the Identity Metasystem and its governing principles. Microsoft believes that other identity management systems built according to the precepts of the Identity Metasystem can have similarly beneficial consequences for user privacy. The Information Card model is only one of many potential approaches.

Conclusion

Experience has shown that identity management systems, and notably systems involving the production and use of ID cards, can operate in ways that prove directly harmful to our privacy and other fundamental values. But, as this paper reveals, that need not always be the case. Indeed, it is possible for an identity management system to promote adherence to data privacy laws, and to do so in a meaningful way. Microsoft believes that its Information Card model of identity management is just one example of the requirements for an effective identity management system converging with the demands imposed by data privacy norms. What is more, it can foster compliance with EU data privacy laws—generally regarded as among the most robust data privacy laws in the world—because it conforms to the rules and principles of the Identity Metasystem. However, precisely because the Identity Metasystem offers only standards and protocols and does not replace or compete with existing identity systems, the path remains open for others to develop identity systems that promote greater privacy and security.

The fields of computer security and privacy have changed beyond recognition in little more than a decade, co-evolving with new threats and innovative technologies. Identity systems will become the critical fabric interconnecting us ever more closely in business, government, and cultural and private life. We must be prepared to continue the innovation that the Identity Metasystem enables so that new possibilities are explored, new privacy and security threats are neutralized, and human dignity is respected in the next phase of the Internet—the Identity-Enabled Internet.

Acknowledgments

The principal authors of this white paper are Thomas Daemen and Ira Rubinstein of Microsoft Corporation's Legal and Corporate Affairs department. Special thanks are also owed to Caspar Bowden, Kim Cameron, Chuck Cosson, Peter Cullen and Mike Jones of Microsoft for reviewing earlier drafts of the paper, to Dean Katz for his help with editing and to Urs Gassner and Mary Rundle of the Berkman Center for Internet & Society at Harvard Law School, who were kind enough to provide comments on a draft distributed at Berkman's ID Mashup Conference, June 19-21, 2006.