

An identity metasystem approach to improve eID interoperability and assure privacy compliance.

Andrea Valboni

Microsoft Italy

Via Rivoltana 13, 20090 Segrate

Milano, Italia

andrea.valboni@microsoft.com

Abstract

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.

INTRODUCTION

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 WSMetadataExchange. 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. 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 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 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.[4] Existing vendor-neutral communication standards based on SOAP and XML will make this possible. These include WS-Security, WS-Trust, WSMetadataExchange, and WS-SecurityPolicy. 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, extensively refined through the Blogosphere, which he has named the “Laws of Identity.”[5] Long experience has proven that these principles are essential to maintaining good online security and privacy.

Systems that breach these laws tend to fail, 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:

1. **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.
2. **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.
3. **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.
4. **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).
5. **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.
6. **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.
7. **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) [6]

- **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.

INFORMATION CARD TECHNOLOGY

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.

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 Cards Model is based on the “Identity Selector Interoperability Profile V 1.0” as described in [8] and it is based on the following design principles:

- **Browser independent:** A goal was to ensure that the protocols developed for using Information Cards on web sites could be implemented by a broad range of web browsers on the platforms of their choice.
- **Web server independent:** A closely-related goal was to ensure that the protocols developed for Information Cards on web sites could be used by web-based applications running on a broad range of web servers on the platforms of their choice.
- **Minimal impact on web sites:** A goal was to facilitate the adoption of Information Cards on existing web sites by requiring as few changes to them as possible.
- **Seamless browser integration:** A goal was that Information Cards should be viewed as a seamless security feature that is a natural extension of the browser(s) being used.

- **Seamless user experience:** A goal was that the Information Card web integration design should permit graceful fall-back when a browser or platform does not have Information Card support available.
- **Work with browser high security settings:** A goal was that the mechanisms chosen should remain enabled even when browser security settings are set to “high”

The resulting implementation available in CardSpace is an attempt to balance among all these sometimes competing goals and to achieve all of them as well as possible.

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).[7]

Scenario One: Basic Protocol

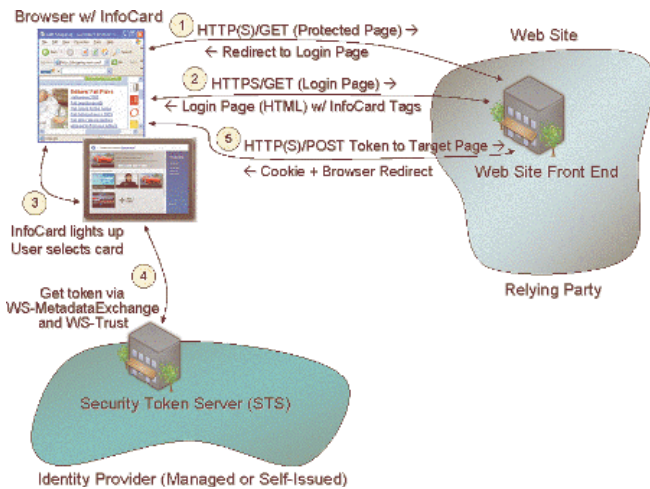


Figure 1. Basic Protocol Flow when using Information Card for authentication at a web site.

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.

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.

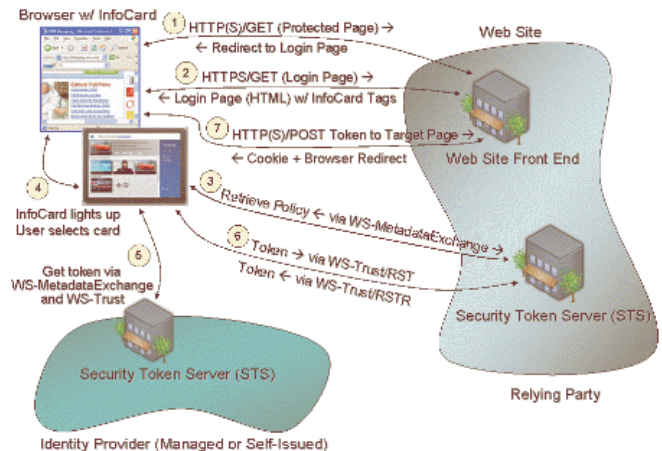


Figure 2. Information Card flow to authenticate at a Web site that employs a relying party STS

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.

Information Cards Implementations

Since its first announcement, Information Cards technology drove the attention of many players in the IT space. Thanks to the Interoperability Profile, it is actually possible to implement the Information Cards protocol on different platforms and with different languages. Here follows a list of third party implementations of the technology described in the previous sections:

- PingIdentity (www.pingidentity.com) developed InformationCard-C, a low level library available on multiple platform for the processing of submitted identity information based on the Information Card Profile. A PHP extension exist which allows the single sign on into Drupal CMS, and open source CMS product.
- JinformationCard is a project aimed at developing a Java library which allows a single sign on capability using Information Cards technology to support Apache Tomcat, JBoss and SUN Application Server platforms running on Windows or Linux. The project was developed by the Fraunhofer Institute FOKUS in Germany[9].
- InformationCard-PHP is build on top of the Zend Framework (<http://framework.zend.com/manual/en/zend.infocard.html>) and allow consumption of Information Cards by a relaying party.
- Information Card Ruby provides a rail plugin and supporting library for integrating personal information cards

to the Ruby on Rails (<http://www.rubyonrails.org/>) relying party web application.

- ICSynergy has extended OpenSSO from SUN to include CardSpace as a simple authentication module [10]

Moreover, in June 2008 a non-profit foundation, The Information Card Foundation (www.informationcard.net), has been started by Equifax, Google, Microsoft, Novell, Oracle, and PayPal, plus nine leaders in the technology community to promote the rapid build-out and adoption of Internet-enabled digital identities using Information Cards.

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.

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 Directive¹.

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 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

¹ 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.

of the Identity Metasystem can have similarly beneficial consequences for user privacy. The Information Card model is only one of many potential approaches.

ACKNOWLEDGMENTS

The principal contributors 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.

REFERENCES

- [1] London School of Economics, June 2005, *The Identity Project: An Assessment of the UK Identity Cards Bill and Its Implications*, available at (<http://is2.lse.ac.uk/idcard/identityreport.pdf>)
- [2] National Academies Press, 2003, *Who Goes There?: Authentication Through the Lens of Privacy* 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).
- [4] 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)
- [5] Kim Cameron, "Laws of Identity," <http://msdn.microsoft.com/en-us/library/ms996456.aspx>
- [6] 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.
- [7] For an exhaustive discussion on how to use the Information Card protocol within applications and browsers see Michael B. Jones, Microsoft Corporation, "A guide to supporting Information Cards within web applications and browsers as of Windows CardSpace 1.0" at <http://msdn.microsoft.com/en-us/library/aa480726.aspx>
- [8] Arun Nanda, Microsoft Corporation, "Identity Selector Interoperability Profile V 1.0", [http://msdn.microsoft.com/it-it/netframework/aa663320\(en-us\).aspx](http://msdn.microsoft.com/it-it/netframework/aa663320(en-us).aspx)
- [9] <https://zeno.fokus.fraunhofer.de/MiniShop/home.jsp>
- [10] Martin Gee, ICSynergy International, "Securing Site Access with CardSpace and OpenSSO: an overview", <http://developers.sun.com/identity/reference/techart/cardspace.html>