

# White Paper: CA and Microsoft Support for User-Centric Identity and the Identity Metasystem

---

Author: Dave Martinez

Date: April 2008

## **Abstract**

This document discusses the Identity Metasystem, Windows CardSpace™ and CA® SiteMinder® Information Card Authentication Scheme (ICAS). After reviewing the existing problems encountered when managing digital identity, this paper introduces the Identity Metasystem, defines its architectural components, then describes how Microsoft® Windows CardSpace and CA SiteMinder ICAS can be used together in business-to-consumer (B2C) and business-to-business (B2B) scenarios to facilitate secure, consent-driven, privacy-enhanced authentication, authorization and federation.

CA Inc.

*Copyright © 2008 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. Certain information in this presentation may outline CA's general product direction. This document is for your informational purposes only and is not deemed to be incorporated into any contract. Notwithstanding anything in this document to the contrary, this presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this document remain at CA's sole discretion. To the extent permitted by applicable law, CA provides this document "As Is" without warranty of any kind, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of such damages.*

*This document was based on current information and resource allocations as of April 2008, and is subject to change or withdrawal by CA at any time without notice.*

*Microsoft Corporation*

*This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.*

*The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.*

*This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.*

*Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.*

*Microsoft, Active Directory, Windows, Windows CardSpace, Windows Server and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Contents

Overview.....	5
The Digital Identity Dilemma.....	6
The Identity Metasystem and User-Centric Identity .....	7
Identity Metasystem Roles and Components.....	8
The Relying Party (RP).....	8
The Identity Provider (IdP).....	9
The User (a.k.a Subject).....	10
Microsoft's Perspective and Windows CardSpace.....	11
Windows CardSpace .....	11
CA's Perspective and CA SiteMinder .....	12
Information Card Authentication Scheme (ICAS).....	12
User-Centric Identity Workflow: CardSpace and ICAS .....	12
Use Cases .....	14
Case 1: Personal Cards for B2C Authentication Without Passwords .....	14
Case 2: Managed Cards for B2B Identity Federation.....	15
Case 3: Managed Cards for High-Value B2B Transactions .....	16
Summary .....	17
For More Information .....	18
About the Author.....	18



## Overview

Every day, the Internet's importance in business and personal affairs grows. This success has brought with it issues – challenges regarding operational efficiency, security and privacy that only become apparent in a world with Internet-scale connectivity.

These issues revolve around digital identity, and the management of digital identity in the Internet age. Forgotten passwords, phishing attacks, orphaned user accounts – these are all consequences of the fact that the Internet was not constructed with an integrated digital identity management layer.

An ongoing dialogue among constituents in the business, government and consumer advocacy sectors has led to the development of a new architecture, known as the *Identity Metasystem*, which provides that missing digital identity layer for the Internet. Inclusive of existing and future technologies, and supported by a broad coalition of technology vendors, the Identity Metasystem introduces a new model for identity-based Internet transactions. A focus on making the user a central, informed participant in these transactions leads to the frequent description of the Identity Metasystem as enabling *user-centric* identity management.

Understanding the Identity Metasystem architecture requires understanding a number of new organizational roles – identity providers, relying parties – as well as new technology tools – tokens, claims, security token services, identity selectors and information cards. Many vendors are working today to create these tools to enable organizations to perform these roles, thus converting the Identity Metasystem from vision to reality.

For example, Microsoft® is delivering tools for the Microsoft Windows® operating system that plug into the Identity Metasystem. Microsoft's initial contribution, called Windows CardSpace™, is an identity selector application for Windows users. Available in Windows Vista® and as a free download for other Windows operating systems, CardSpace provides an interface in which users work with information cards – managing their Internet identity relationships, better understanding how and when their identity information is shared with outside parties, and authenticating to Web applications and services without typing a username and password.

Similarly, CA® is augmenting its CA SiteMinder® Web Access Manager (WAM) solution to interoperate with the Identity Metasystem. CA's SiteMinder Information Card Authentication Scheme (ICAS) enables organizations running CA SiteMinder to integrate with Windows CardSpace, accepting CardSpace-managed identities to enable access to SiteMinder-protected resources. Available in SiteMinder Release R12 SP1 due in 2008, ICAS brings SiteMinder customers the efficiency and security of information card-based authentication and authorization in business-to-consumer (B2C) and business-to-business (B2B) scenarios.

Microsoft and CA encourage organizations to become more familiar with the Identity Metasystem. Please see the For More Information section at the end of this document for relevant links to more content.

## The Digital Identity Dilemma

The Internet is an essential medium for business and personal interaction. It seems virtually anything can be done on the Web – managing supply chains, buying Christmas presents, managing bank accounts, collaborating with business partners, renewing your vehicle registration...the list is long, and growing.

However, as the Internet grows as a platform for both low-value and increasingly high-value transactions in people's home and work lives, some growing pains are being felt:

- In the business-to-consumer (B2C) context, Web-based social engineering attacks like phishing and pharming, as well as high-profile thefts of millions of customer records from business databases are increasingly common. This reduces public and organizational confidence in the Internet as a place to do business, slowing growth. It's extremely costly – not just financially, but in the goodwill established between customer and vendor. And every day there's more criminal incentive, as more value is made accessible via the Internet.
- In the business-to-business (B2B) context, accelerated service outsourcing (401K, CRM, etc.) coupled with the growth of partner-focused extranets is creating a dynamic business environment – and an explosion of user accounts. The increasing administrative overhead for all parties concerned (user, employer, and partner) keeps eating away IT resources better spent on higher-value projects. Additionally, each new identity represents a potential security risk, as compromised passwords and orphaned accounts become easier to create and harder to spot.

A commonality shared by the above points is that they have to do with identity, specifically the mismanagement of identity information, much of it by end users. Users are being overwhelmed by the process of Internet-scale identity management. The typical user has so many identities in so many different places, with so few management tools at their disposal, that the whole concept of "digital identity management" might seem an oxymoron.

Why is this aspect of the Internet experience so flawed? Because the Internet as it exists today has no integrated digital identity "layer" – a set of holistic, standards-based services for managing identities on the Web. And the solutions that have developed to fill this void have helped in some areas while hurt in others. For example:

**Passwords** – They are easy to guess, not protected well, people have too many of them, and thus they're often reused, and often forgotten. All this makes passwords vulnerable to theft, and administratively burdensome to manage. But they're by far the most popular way to control access to Web applications, regardless of how valuable the content.

- *Privacy and Security* – The Passport Network, now Windows Live ID, reduced the number of passwords people needed on the Internet by providing a general-purpose identity for Internet use. However, Microsoft learned that it wouldn't make sense for any one organization to participate in all of a person's identity transactions – as a customer, a citizen, an employee, and in their various other contexts. Moreover, if the entire Internet is accessible via a single password, a thief who steals that one password has the "keys to the kingdom."

- *Cost effectiveness* – Alternative authentication methods such as smartcards and other “hard” tokens are generally more secure than passwords, but they’re much more expensive, both in upfront hardware cost and downstream replacement cost. “Soft” tokens like client SSL certificates, while cheaper to create, are equally expensive to administer and train users on.

**Server identification** – It’s easy for criminals to create fake Web sites that look just like a person’s bank, or an e-commerce site, and collect users’ personal information through simple forms users are all too willing to fill out. The growing sophistication in phishing tools means most people – including experts – often can’t tell whether the Web site they’re at is “real” or not.

- *Ease of use* – Most B2C Web sites use SSL certificates for protecting inbound data from man-in-the-middle attacks. With recent advances in browser technology, those certificates are now providing users some data regarding the identity of the Web site. However in practice, very few users know or understand how certificates work, how to determine the authenticity of a site by looking at its certificate, or where to find the certificate information.

**Data collection, retention, accuracy, auditing and compliance** – Every Web site collects user information to create identities for access control and service personalization. But sites often collect more data than they need, don’t properly secure the data, and don’t discard the data when appropriate. Ultimately the identity sits there waiting to be misused by identity thieves, or organizations that collude to develop profiles of specific users. In the B2B context, “identity islands” like these are completely disconnected from an employer’s IT systems, which means they can contain outdated information, which may be used without an employer’s knowledge by users (possibly former employees) who should not have access. Moreover, they are often redundant -

- *User consent* – Single sign-on (SSO) solutions are used today by many enterprises to control access to internal applications and these solutions often enable the federation (or sharing) of those identities across the Internet to other trusted parties. This is a good thing, as it reduces the number of passwords users need, the data management requirements for the application provider, and improves security for the employer. However, today’s federation solutions treat the sharing of user identity data like a “back-room” process, where the user often has no role in determining what personal information is shared about them. Sometimes this lack of explicit user consent can undermine user privacy, and leave the user with less control over their identity.

## The Identity Metasystem and User-Centric Identity

Fortunately, efforts are being made in the technology industry to address the digital identity dilemma. An ongoing dialog is taking place by stakeholders in the business, government, and consumer advocacy sectors, with the intention of designing that missing identity layer for the Internet. The fruit of their labors, known as the *Identity Metasystem*, will help mitigate the threat of identity misuse on the Internet.

It’s called a *metasystem* because it’s a system of systems – tying existing technology solutions together through a standard set of communication protocols (for tech vendors) and user interface metaphors (for users). It’s instructive to think of the Identity Metasystem as analogous to the advent of the Internet Protocol (IP), or what could be called the Network Metasystem. Introduced in 1982, the Internet Protocol enables interoperability among a collection of diverse networking

technologies (Token Ring, Ethernet, etc.), making the ubiquitous connectivity of the Internet a reality. Just like the Internet Protocol enables the use of different underlying physical networks on the Internet, the Identity Metasystem enables different underlying identity technologies, such as X.509 Kerberos, and SAML.

This is critical, because many types of identity management solutions are already widely deployed today. A “rip and replace” technology strategy is usually too expensive and disruptive to be accepted. Thus, any new approach must work with (not instead of) this set of current technologies, to ease migration while protecting the return-on-investment (ROI) of existing systems. As a result of the inclusive nature of the Identity Metasystem architecture, numerous technology vendors (including CA and Microsoft) are busy building Identity Metasystem components today.

The set of principles that shaped the development of the Identity Metasystem are published and commonly referred to as the [Laws of Identity](#). Chief among them is that users must be in a position of control of their identity information. Therefore it is said that the Identity Metasystem enables *user-centric identity*.

## Identity Metasystem Roles and Components

Today most Web interactions involve two parties; a user and the service he or she is using – typically a Web site. The Identity Metasystem architecture refers to the service as the **relying party**, adds a new party to the mix – the **identity provider** – and provides these two parties and the user new technologies with which to perform their roles.

### ***The Relying Party (RP)***

It's easy to imagine any Internet-facing Web site or Web service in the relying party (RP) role – it is the site or service the user wants to use.

The most important characteristic of an RP in the Identity Metasystem is that instead of learning the user's identity information through manual entry (during registration, in future password requests, etc.), RPs receive identity data in the form of **tokens**. A token is a computer-generated representation of a user's identity; it can say as little or as much about an identity as is needed for a given scenario; and since its contents can be cryptographically encrypted and signed, it can be used to securely package identity information for transit on the Internet, and to prove a user's identity without typing a password.

Tokens contain **claims**, or statements regarding attributes of the user's identity. The claims included in a token might include a user's name or email address, for example, which would be useful for correlating a token to an account in an application's user directory. Other claims like age, citizenship, title, affiliation to a group, or membership in a corporate directory can be useful for determining what a user should be able to do in an application. Being inherently flexible, there is no limit to what claims can be defined, or what information they can convey. Tokens and claims enable RPs to make decisions about user access and entitlements – and can theoretically replace existing user repositories as a primary means of enabling authentication and authorization in Internet-enabled applications.

Enabling an application to support the RP role can be done with relatively minimal impact on the application architecture, by leveraging solutions that act as a layer between the Identity

Metasystem and the application. Commercial products such as CA SiteMinder WAM are adding this support today.

## ***The Identity Provider (IdP)***

If tokens replace passwords in the Identity Metasystem, then who makes the tokens? The answer is an identity provider, or IdP.

An IdP can be any entity that can create tokens, and knows something about users that could be useful to a relying party. Examples include:

- An employer might issue a user a token to use in a partner's extranet, asserting the user is an employee and a manager;
- A business might issue a user a token to use at affiliated businesses' Web sites, asserting the user is a Gold level loyalty program member;
- A credit card company might issue a user a token to use at e-commerce sites as an alternative to providing a credit card number, asserting the user has a valid credit account with available funds and an authorization code;
- A government might issue a user a token to use at Web sites where age verification is a requirement (such as online wine merchants), asserting the user is over 21 years of age;
- People can also be identity providers for themselves. A user might create a token containing their name and email address, and use it to register at Web sites.

That last scenario is common. People often provide information about themselves to web sites, even information that is managed by other entities (like a credit card number, or a loyalty program account number). In the Identity Metasystem, however, it becomes possible for a third party IdP to generate a token on behalf of a user, upon request – providing data similar to that on a physical credit card or driver's license, but doing it in real-time. This information is more valuable than what users provide themselves since it comes from a place both the RP and the user **trust** to (a) provide accurate information, and (b) provide the information only when requested by the rightful owner.

IdPs use a technology called a **security token service** (STS) to create tokens. An STS typically has the following capabilities:

- Authenticate users, to make sure it creates tokens for the right user.
- Create tokens of various types (SAML 1.1, SAML 2.0, Kerberos, XrML, etc.) depending on the requirements of the RP.
- Create tokens with as little or as much information as is needed by the RP and authorized by the user for a given transaction.
- Cryptographically encrypt tokens for security and sign tokens to demonstrate authenticity and integrity.

## The User (a.k.a Subject)

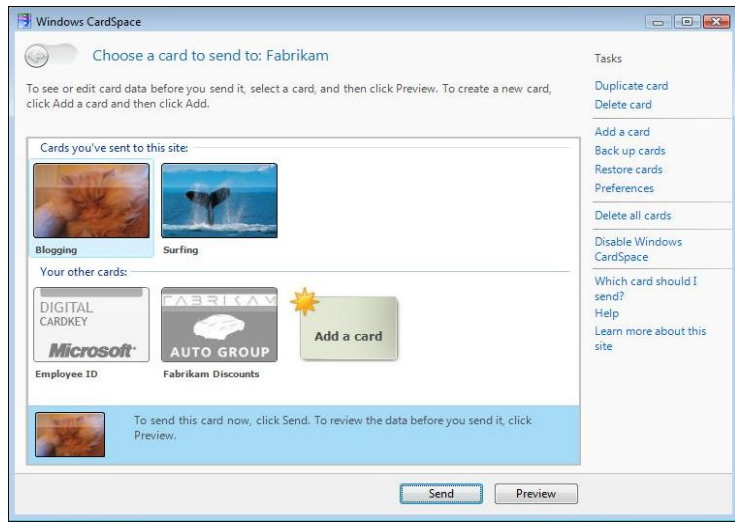
A token's claims are made on behalf of the user. The term "subject" is sometimes used instead of "user" because a single token can represent an individual, a group, an organization or a resource. Since the most familiar case is where a token refers to an individual, the term "user" is used here.

With the large potential number of IdPs a user might interact with, it is important that they have some method to understand and manage these relationships. For that purpose, the Identity Metasystem introduces the concept of an **identity selector**. An identity selector is an application for managing relationships with IdPs, and sharing information with RPs, all under user control. An identity selector:

- Brings a consistent user interface to each identity transaction;
- Provides an environment for users to view and consent to the sharing of identity data pertaining to them;
- Enables the use of various authentication technologies, token types and communication protocols between IdPs and RPs by determining requirements for each and choosing options that work for all parties;
- Assists users in selecting among the relevant identities that could be used in a given situation.

It's useful to think of an identity selector as a personal portfolio of digital identities, containing all of a user's relationships with identity providers. An identity selector manifests these user-IdP relationships as "cards", specifically **information cards**. Information cards look like a digital version of an actual physical card, and users will commonly have a collection of information cards useful for different purposes.

Unlike a physical card, information cards do not actually contain any personal identity data. Each card is, in fact, only a pointer to a security token service (STS) operated by an IdP. The card is used to initiate contact with an IdP, to request tokens for use at RPs. Since the IdP provides the identity data, less information is kept on a user's computer, thus increasing security.



Windows CardSpace identity selector

Information cards come in one of two different types:

- **Personal cards** point to a "personal STS" that is local to the user (on a computer, or possibly in the future in other locations such as on a cell phone or a USB device) for asserting information about himself/herself to RPs. Personal cards are created by users, and can obtain only specific low-sensitivity information from the "personal STS".

- **Managed cards** point to an STS operated by a third party, like an employer or a government. Managed cards are digitally signed by the IdP and given to users – they are not created by the user. They can request any information, even sensitive information if the scenario requires it.

Microsoft has shipped an identity selector called **Windows CardSpace**, enabling Windows users to participate in the Identity Metasystem. Compatible identity selectors have also been released by others for MacOS, Linux and FreeBSD.

## Microsoft's Perspective and Windows CardSpace

Microsoft's long history of tackling identity management issues has informed its thinking on the Identity Metasystem. Those experiences have included:

- Incorporating Kerberos as a robust, reusable identity token service in Windows Server®, and extending the Kerberos identity to provide the value of a centralized identity in a variety of Windows applications,
- Extending Active Directory through technologies such as Active Directory® Federation Services (ADFS), which extends the value of Active Directory accounts for uses outside of a corporate domain infrastructure
- Creating Microsoft Passport, a multi-purpose identity for the Internet, and the educational value of the business, privacy and security concerns that this effort raised.

Microsoft believes the Identity Metasystem brings improved security, privacy and administrative efficiency to people and organizations using the Internet for work or play. As a result, Microsoft is committed to both implementing and promoting an interoperable Identity Metasystem architecture. Microsoft's Kim Cameron, the author of the *Laws of Identity*, hosts [identityblog.com](http://identityblog.com), a primary forum for industry discussion of the Identity Metasystem.

His and others' efforts are profoundly impacting the development plans for Microsoft technologies including Active Directory, ADFS, the Microsoft .NET Framework and Windows Communication Foundation. Most recently, however, they have culminated in Microsoft's first technology contribution to the cause – Windows CardSpace.

### **Windows CardSpace**

Windows CardSpace is Microsoft's identity selector for the Windows platform. CardSpace is a client application integrated into Windows Vista and available for free download for Windows XP SP2 and Windows Server 2003 as part of the .NET Framework (version 3.0 or 3.5). If used with Internet Explorer®, CardSpace requires version 7; note that it also works with non-Microsoft browsers such as Firefox on Windows via plug-ins.

As does any identity selector, CardSpace provides a consistent user environment for the management of digital identities. CardSpace's notable features include:

- An integrated "personal STS" with enhanced cryptographic security, to issue personal cards;
- An intuitive user interface for creating and managing personal and managed cards;
- Security-enhancing integration with Windows client and Server products.

In order for users to get value from CardSpace, potential relying parties have to incorporate support for the Identity Metasystem into their infrastructures. CA is one vendor working today to make this easier for its customers.

## **CA's Perspective and CA SiteMinder**

CA has long been a leading provider of Internet-scale access control solutions. CA SiteMinder Web Access Manager (WAM) is one of the most popular commercial WAM products on the market – providing authentication, authorization, federation and session management (SSO) services for Web applications running in heterogeneous technology environments. With time, SiteMinder's scope has expanded to include:

- Support for the broadest array of authentication mechanisms, Web servers, Web application platforms, databases, directories, and operating systems on the market;
- A leadership role in the development of Security Assertion Markup Language (SAML), paving the way for the use of tokens for cross-domain authentication and authorization – an essential underpinning of the Identity Metasystem;
- Extending the value of SiteMinder accounts for use in partner extranet applications through the SiteMinder Federation Security Services (FSS) product;
- Early support of federation protocols including WS-Federation in SiteMinder FSS, and resulting interoperability with Microsoft's ADFS.

CA supports the Identity Metasystem, as it represents another natural extension of the purpose SiteMinder has always played in enterprises, simultaneously securing and easing access to Web applications. The first deliverable in this effort will be called the Information Card Authentication Scheme, or ICAS.

### ***Information Card Authentication Scheme (ICAS)***

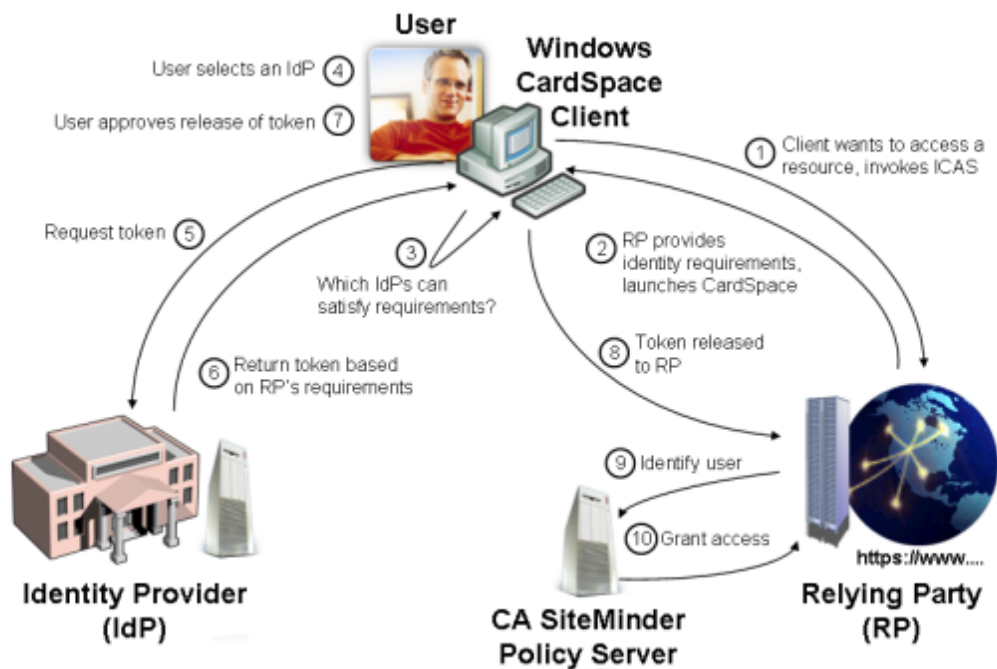
Available soon as a SiteMinder authentication scheme, ICAS will allow relying parties using SiteMinder to accept information cards (from Windows CardSpace or other identity selectors) as an alternative authentication technique to pre-existing accounts in SiteMinder user stores. ICAS is scheduled to be included in SiteMinder Release 12 SP1, with availability planned sometime in 2008.

By enabling SiteMinder to consume and understand the tokens used in the Identity Metasystem, SiteMinder customers can:

- Accept personal cards for simple authentication to B2C Internet sites;
- Accept managed cards issued by IdPs as a method of authentication, identity federation, and claims-based authorization.

## **User-Centric Identity Workflow: CardSpace and ICAS**

One feature of the Identity Metasystem architecture is that the basic process flow between components remains the same, regardless of the particular scenario (personal card, managed card, B2B, B2C, etc.), making it easier to understand for IT professionals and users alike. Any identity transaction using Windows CardSpace and SiteMinder ICAS would flow as follows.



At setup, RPs and IdPs establish policies regarding what security token types and claims they will supply (at the IdP) and consume (at the RP). Additionally, an IdP establishes policy for what authentication methods it will support. The user creates personal cards or imports managed cards (which include the IdP policy information) into the CardSpace identity selector.

1. A user visits a SiteMinder-protected Web application. The SiteMinder Web agent intercepts the request and invokes the ICAS authentication scheme.
2. The SiteMinder credential collector instructs the user's browser to launch the identity selector (in this case CardSpace) on the user's computer, and sends along RP policy information.
3. CardSpace reads the RP policy and compares it with the IdP policies for each installed information card, highlighting cards in the user's collection that can create valid tokens for the RP. Cards that cannot meet the RP's requirements are "grayed out."
4. The user selects a highlighted card from the collection. Before requesting a token, CardSpace collects credentials for authentication to the IdP; Support for Kerberos, X.509 client certificates and even personal information cards as authentication techniques means this process is usually seamless to the user.
5. CardSpace sends the IdP a Web service message requesting a token. The IdP authenticates the user and processes the RP requirements.
6. The IdP generates and sends back a digitally signed and encrypted token carrying the required claims.
7. Before sending the token to the RP, CardSpace gives the user the opportunity to preview the claims, informing the user what data about them is being shared.

8. By clicking Send, the user approves release of the token to the RP. There SiteMinder's ICAS decrypts the token, making the claim data accessible.
9. Using the token's contents, ICAS associates the inbound token to the user's identity in the SiteMinder user store, while using cryptography to verify the token's authenticity and integrity.
10. SiteMinder now performs its standard policy-based authorization processes, giving the user access if policy allows.

## Use Cases

Some examples might help illustrate how Windows CardSpace and SiteMinder ICAS together can improve the organizational security, user privacy and IT administrative efficiency in real-world B2B and B2C identity management scenarios.

Contoso Limited sells home, auto and life insurance products to consumers in various markets. Contoso's sales channel is comprised of a network of independent agencies of varying size in local markets across the country.

Employees for the local agencies interact with Contoso through an extranet application (<https://www.contoso.com/agent>) where they can research products, generate quotes, and register new policyholders. Additionally, at <https://www.contoso.com/consumer>, Contoso policyholders can access a customer-facing Web application, where they can change their policies, initiate a claim, pay policy premiums, etc.

Contoso uses CA SiteMinder to provide access control for these two Internet-facing Web applications. By adding information card support through ICAS to their environment, Contoso enables user-centric identity management – giving the company, its partners and its customers the improved privacy, security and efficiency benefits discussed above.

### ***Case 1: Personal Cards for B2C Authentication Without Passwords***

Users	Contoso Limited customers
IdP	User's own CardSpace "personal STS"
RP	<a href="https://www.contoso.com/consumer">https://www.contoso.com/consumer</a>

In this case a Contoso customer running Windows at home can use CardSpace and their personal card, instead of a username and password, to perform secure authentication to the SiteMinder-protected Contoso consumer application. Some key takeaways in this example:

- When using personal cards and the "personal STS", no IdP configuration is required. For ease of use, and to protect users from inadvertently disclosing identity data, the "personal STS" in CardSpace has limited data and configuration options. It publishes claims containing subsets of a fixed set of low-sensitivity information via SAML 1.1 tokens.
- CardSpace is integrated into Windows, appearing in a private desktop similar to what's seen when a user presses CTRL-ALT-DEL to bring up the Windows logon screen. This is part of the consistent user experience for identity interactions that CardSpace enables.

- When a consumer first uses a personal card, CardSpace's presentation of Contoso's RP identity data (including company name, privacy policy, certificate issuer, etc.) helps ward off phishing attacks. Extended Validation (EV) certificates, which put RPs through more thorough security checks, are highlighted by CardSpace to provide visual cues that engender increased consumer confidence.
- The same personal card can be used securely with multiple Web sites. For each place a personal card is used, CardSpace generates and transmits data uniquely identifying the user – including a Private Personal Identifier (PPID) and an RSA public/private key pair – corresponding to a specific card used at a specific site.

This (a) disables rogue RPs from using correlating attributes to spy on user behavior across sites, and (b) enables the use of digital signatures, thus providing the secure cryptographic replacement for a username and password. Also, if someone is tricked into using their personal card with a rogue Web site, the resulting token cannot be used to impersonate the user anywhere else, since it is usable only at the requesting site – in this case the rogue RP.

- ICAS is implemented as a SiteMinder custom authentication scheme, making it simple to add to existing SiteMinder deployments and integrate with existing SiteMinder features.

For example, if ICAS fails to map an incoming token to an existing user, it can send a standard SiteMinder authentication response to the SiteMinder policy server, which can redirect users to a forms-based authentication page. Upon identifying the user, ICAS can then write a unique value to the user's attribute collection to facilitate mapping in the future.

- If users need the ability to access the Contoso consumer application from locations besides their primary PC, they can export personal cards into a .crds file, and import it into CardSpace or another compatible identity selector on another machine.

## ***Case 2: Managed Cards for B2B Identity Federation***

Users	Fabrikam Insurance agents
IdP	Fabrikam STS
RP	<a href="https://www.contoso.com/agent">https://www.contoso.com/agent</a>

Fabrikam Insurance is an insurance agency with multiple locations. Fabrikam agents sell Contoso Limited insurance policies, and access the Contoso extranet application at <http://www.contoso.com/agent>. Fabrikam uses Windows Server and Active Directory to manage network accounts for internal access.

In this case a Fabrikam agent running Windows at work can use CardSpace and their Fabrikam managed card (issued either by a future Microsoft STS product, or another compatible commercial or open-source STS) to perform secure authentication to the SiteMinder-protected Contoso agent application. Some key takeaways in this example:

- Fabrikam employees choosing their Fabrikam card for access to Contoso's application are leveraging their company-based identity to link to an application operated outside their home network, without needing a password. RPs like Contoso no longer need to incur the cost of administering passwords for partner employees.

- A managed card STS product from Microsoft will accept various authentication methods, including Kerberos – meaning that the user is automatically authenticated to the STS by virtue of his Windows Kerberos session when on the corporate network.
- While Fabrikam’s Active Directory might include many user attributes, and its managed card might be able to deliver many of them as claims, only the few required by the Contoso application are actually released, to maximize privacy.

In addition, these claims can be transformed to further reduce outside exposure of user attribute data. For example, Fabrikam can send the claim “ApprovedUser=Yes” for agents that are members of the Managers group, without ever disclosing to Contoso the existence of a Managers group.

- ICAS can convert inbound claim data into SiteMinder “active responses” – user attribute data provided directly to applications by SiteMinder via HTTP headers or cookies – eliminating the need for LDAP lookups to the user’s identity.

Fabrikam, for example, could provide a “Gold Level” claim for agents who are authorized to sell specialized products – and Contoso’s application could use the resulting active response to expose the Gold Level products. When RPs use claims to drive application behavior, IT personnel at the IdP are freed from spending time updating user identities in external directories.

- During token processing, SiteMinder and ICAS provide flexibility – allowing other processes to be added to the ICAS processing chain. For example, Contoso could get additional claim values from internal sources to complement the initial Fabrikam claims, and deliver the aggregate claims via the same “active responses” process described above, to further personalize the user experience.
- Fabrikam agents must successfully authenticate to the Fabrikam STS in order to receive the token required by the Contoso application. If an agent’s user account is disabled in Active Directory, then no tokens are generated and access to external applications is immediately blocked. This reduces the threat of ex-employees using orphaned accounts to improperly access data.
- Since this experience is the same as the experience consumers have using personal cards, the consistency allows for greater user comfort and understanding as they learn to use multiple identities in different contexts.

### ***Case 3: Managed Cards for High-Value B2B Transactions***

Users	Fabrikam Insurance managers
IdP	Fabrikam STS
RP	<a href="https://www.contoso.com/agent/pricing">https://www.contoso.com/agent/pricing</a>

The Contoso application allows agencies to modify their pricing to account for local market conditions. At Fabrikam, this right is granted to a small group of managers.

In this case, Fabrikam managers with these privileges have access to a “Pricing Change” claim via their managed cards, which grants them access to more sensitive areas of the SiteMinder-protected Contoso application. Some key takeaways in this example:

- Because ICAS is deployed as any other SiteMinder authentication scheme, one can deploy multiple instances of ICAS in different areas of the same site, each with its own policies. For example, a higher SiteMinder protection level (which invokes reauthentication) might be used to protect the pricing adjustment pages, invoking an ICAS instance requiring the “Pricing Change” claim. This could re-invoke the CardSpace interface, and re-generate a token – this time with the additional “Pricing Change” claim.
- An alternative approach would be for Fabrikam to issue “Pricing Change” managed cards to the privileged managers, which provide only the one additional “pricing change” claim. In this case, the IdP could integrate strong authentication systems like smartcards into the managers’ CardSpace workflow, to more strongly control access to specific areas of the RP’s application – keeping the basic interface for identity interactions the same, while changing the technologies employed underneath.
- Since pricing changes are important events to Fabrikam executives, the use of a “Pricing Change” card can also be used to trigger reporting and auditing events, email notifications, etc. Tying external access events to issuance of tokens on internal servers results in better security compliance through easier auditing.

## Summary

While the problems of Internet identity are not new, they are becoming more pressing. The desire to address phishing, move to a better form of authentication than passwords, give partners secure and appropriate access to organizational resources, and other inspirations have led to the development of the Identity Metasystem architecture and user-centric identity management.

Microsoft Windows CardSpace and the CA SiteMinder Information Card Authentication Scheme make it possible for organizations running B2C or B2B-focused Web applications and their constituents to experience the benefits of user-centric identity management, which include:

- Better security – Threat vectors like passwords stolen through phishing attacks are mitigated, while user-centric federation gives organizations more visibility and control over constituent use of managed identities.
- Better privacy – User consent to data sharing is explicit, and only shared among entities on a “need to know” basis.
- Better efficiency – Organizations reduce password reset costs, while eliminating identity management redundancies by leveraging claims-based authorization as an alternative to multiple directories for multiple applications.

Organizations, particularly those with identity management solutions in place today, should begin examining how to evolve their current infrastructure in a way that best takes advantage of the opportunities made available by the Identity Metasystem.

## For More Information

### *Identity Metasystem*

- The Laws of Identity  
<http://msdn2.microsoft.com/en-us/library/ms996456.aspx>
- Microsoft's Vision for an Identity Metasystem  
<http://msdn2.microsoft.com/en-us/library/ms996422.aspx>

### *Microsoft Sites*

- CardSpace page on the .NET Framework 3.0 Community site  
<http://netfx3.com/content/WindowsCardSpaceHome.aspx>
- CardSpace page on Microsoft Developer Network (MSDN)  
<http://msdn.microsoft.com/CardSpace>

### *CA Sites*

- CA SiteMinder Home Page  
<http://ca.com/products/product.aspx?ID=5262>

### *Open Source Sites*

- Open Source Identity Systems (OSIS) Working Group  
[http://osis.idcommons.net/wiki/Main\\_Page](http://osis.idcommons.net/wiki/Main_Page)
- Eclipse Higgins Project  
<http://www.eclipse.org/higgins>

### *Blogs*

- Kim Cameron's Identity Weblog  
<http://www.identityblog.com/>
- Windows CardSpace Team  
<http://blogs.msdn.com/card/>
- Mike Jones (Identity Metasystem, Information Cards)  
<http://self-issued.info/>

## About the Author

David Martinez is a technology consultant based in Redmond, Washington. A graduate of the Wharton School of the University of Pennsylvania, he has 15 years experience in the technology industry, including product marketing and management positions at Microsoft and Netegrity (now CA).