

Federated Identity

Seizing Business Opportunities by Sharing Trusted Electronic Identities

In the networked economy, strategic partnerships are an important way to reduce product development and marketing costs, increase sales figures and seize new business opportunities. In order to achieve the required agility to capitalize on such opportunities—and combine the efficiency of web-based collaboration with strong security to protect proprietary information on other network resources—companies need to be able to trust the electronic identities that access their web sites from external entities. In this paper, RSA Security discusses how federated identity, a key component of a comprehensive identity and access management (I&AM) solution, enables organizations to share trusted identities through strong authentication and single sign-on (SSO) functionality.

TABLE OF CONTENTS

I. INTRODUCTION	1
II. MARKET OVERVIEW	1
Business Drivers	1
Technical Drivers	2
Regulatory Drivers	3
Key Federated Identity Concepts	3
III. TECHNOLOGY ISSUES	4
Standards and Approaches	6
IV. NON-TECHNICAL ISSUES	7
Deployment Timeline	7
V. CONCLUSION: RSA SECURITY LEADS THE WAY	8
ABOUT RSA SECURITY INC.	8

I. INTRODUCTION

From the advent of the Internet, its primary benefit was the easy and efficient sharing of information to users worldwide. The users, for the most part, were anonymous, their identities hidden in impersonal cyberspace. As more and more information got pushed to the web—much of it sensitive and confidential—it became more and more important for the publishers of this information to know who was accessing it. Thus, electronic identities emerged, with some form of authentication method, such as a password, attached to them.

An enterprise enabling employees to access its own applications is one thing; enabling them to then just as easily access the electronic resources of remote offices, autonomous business units and business partners is far more complex. When businesses begin to join together in more consumer-facing online ventures, the complexity will grow exponentially. And yet that is where numerous industries are going, because just as the Internet made it easier to share information, today's collaborative and interconnected e-business landscape requires a secure and effective way to share trusted user identities.

This is the concept behind federated identity, which the Burton Group defines as "The agreements, standards and technologies that make identity and entitlements portable across autonomous domains." It is analogous to a driver's license: one state provides a credential to an individual that is trusted and accepted as proof of identity by other states. This trust requires—and is a result of—the combination of powerful, reliable technology and the business and legal agreements that enterprises enter into to establish mutual responsibility and commitment.

Federated identity is a key part of an enterprise identity and access management (I&AM) strategy, and provides the following benefits to organizations and end-users:

- Organizations—enhanced ability to collaborate with business partners, manage supply chain, offer new revenue-generating services to customers and protect enterprise resources while reducing costs
- End-users—increased convenience, ease-of-use and productivity; broader access to information and services; protection of personal information from companies that don't require that information (e.g., social security number can be read by healthcare provider, but not by retail partner)

As a leading provider of federated identity solutions and a leader and/or active participant in numerous standards bodies and solution development groups, RSA Security is qualified to address the business, technology and legal issues of federated identity systems.

II. MARKET OVERVIEW

It is important to note at the outset that federated identity is not an engineer's dream on a white board waiting for technology and market demand to catch up—it is real, in demand and currently in use in major enterprises worldwide. While some of the underlying standards and protocols are still being reviewed by appropriate bodies, this is a technology that works and is delivering the benefits it has promised.

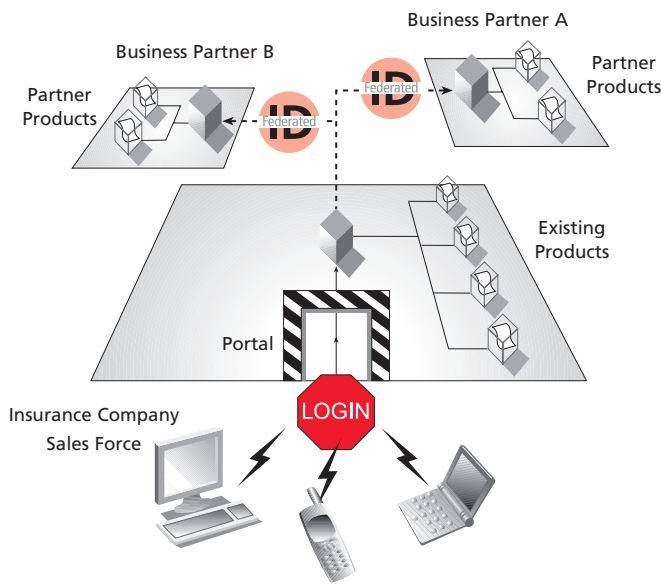
This section will explore some of the key concepts of a federated identity solution and the business, technology and regulatory drivers that have made federated identity a reality. These drivers span a broad range of industries—including financial services, healthcare, government, manufacturing, telecommunications and retail—and represent some of the myriad challenges and opportunities facing organizations in the global, highly networked economy.

Business Drivers

Among the business drivers that have given rise to federated identity are user convenience, risk management, business enablement and cost reduction. Each of these drivers is critically important to business growth; taken together, they represent the incalculable value of federated identity.

User convenience. In the past, companies had to balance convenience with security. Each application required a password, but it was difficult for users to memorize multiple passwords (sometimes upwards of 10 or even 20!). Solutions like writing them down or using obvious passwords created security holes and ultimately defeated the purpose. At the same time, user productivity was negatively affected by the need to login multiple times in a single session. With single sign-on (SSO)—which, as we'll see, is a key concept behind federated identity—users get the convenience they want and organizations get the security they need.

Risk management. Risk management is obvious—every organization needs to know who is accessing their systems. In a collaborative environment, however, where external users as well as internal users are logging on, a secure, trusted identity authentication solution is even more critical. Risks can include exposure of confidential information, liability due to lack of compliance or privacy lawsuits, hackers and denial-of-service attacks, and theft of identity or intellectual property. Federated identity balances user convenience with the strong security required to reduce risk.



FEDERATION IN ACTION I: INSURANCE COMPANY

This company's sales force sells its products through a portal. The company identified three critical goals: to increase revenues and introduce new products, to increase sales of existing products by expanding the sales force and to accomplish both cost-effectively. The key to achieving these goals involved linking the company's sales force with the products and sales personnel of its business partners. The technical challenge was to deliver the same user experience to end-users and provide seamless access to new applications in both company and partner domains—and to do this securely and by leveraging standards.

The solution was federated identity. In the first scenario, when the company's salespeople login to the portal, they can click on links that lead to new products hosted on partner sites without having to re-authenticate at the partner sites. The business partners trust the assertion and provide access authorization based on the attribute (such as "Company A salesperson") attached to the identity.

The second scenario works the same but in reverse. Partners can seamlessly access the company's portal, enabling them to sell the company's products from their own domains. This solution minimizes costs by leveraging existing resources and negating the need to hire additional salespeople. Company salespeople, as well as those of its business partners, have federated identities that are accepted throughout the circle of trust; these identities include authentication information, as well as the attributes required to gain access to the other sites.

Business enablement. With federated identity, it is also much more efficient to conduct supply chain transactions, collaborate with partners and provide services to a broader customer base. Keeping vendors and distributors informed and up-to-date on orders, inventory levels and projected needs requires two-way communication and input up and down the supply chain. Federated identity enables partners to safely share sensitive information on a timely basis. With co-design, co-marketing or joint sales activities, federated identity makes it easier and more cost-effective for organizations to work together on revenue-generating projects. Federated identity also makes it safe and simple for business partners to provide customers with click-through services on their web sites.

Lower costs. Managing this capability from a centralized location—while also reducing help desk calls from users who have forgotten their passwords—significantly trims administrative costs and contributes to ROI. Specifically, organizations can reduce user administration and directory management costs in addition to the savings that will be realized as fewer and fewer employees need to call the help desk when they've forgotten their passwords. In addition to cost savings, organizations can benefit from cost avoidance due to reduced risks and liabilities and by avoiding the need to develop separate access rights profiles for each user and each application.

Technical Drivers

As businesses seek to consolidate or collaborate more efficiently, the need has arisen for a simpler, faster and more cost-effective way to integrate or connect to heterogeneous systems. The emergence of standards such as XML and SOAP provides the foundation of a common language that enables heterogeneous applications to understand each other.

Additionally, the rise of web services—which perform application-to-application transactions—presents a unique identity "crisis." In this context, applications require trusted identities just as human users do. Combining the reach and flexibility of XML and SOAP with the mechanical efficiency of web services requires a secure federated identity solution that enables a web service to do its job.

Also, while a number of IT professionals have spent many hours assembling a complex maze of homegrown point-to-point access solutions—in which individual users are linked to any number of applications on a 1:1 basis—many have found the task to be more challenging than expected. Without widely accepted standards, businesses are forced to build non-repeatable solutions from scratch. Now federated identity enables efficient SSO implementations at a fraction of the ramp up time and cost.

Regulatory Drivers

In recent years, there have been numerous government regulations worldwide that focus on privacy and security issues related to the electronic storage, access and transmission of personal information. Some are industry-specific, some are country- or region-specific, but all require that companies employ security technologies such as authentication and web access management solutions in order meet compliance. Federated identity combines strong authentication with access control capabilities and is a sure route to compliance with these regulations, a sampling of which follows.

- Health Information Portability and Accountability Act (HIPAA) — This broad legislation applies to healthcare providers and payers operating in the U.S.; the elements of interest to this discussion are the privacy and security standards designed to protect patient identities and sensitive health and treatment information.
- Gramm-Leach-Bliley — This legislation applies to financial services firms operating in the U.S. and is designed to protect consumers’ financial information from unauthorized access.
- Sarbanes-Oxley Act — This legislation applies to all public companies in the U.S.; the Act sets forth auditing standards designed to ensure the integrity of the IT systems of publicly traded companies.
- US Patriot Act Customer Identification Program — This program requires financial services firms operating in the U.S. to obtain, verify and record information that identifies each individual or entity that opens an account.
- European Data Protection Directive — This legislation, which applies to firms operating in the European Union, prohibits an individual’s personal information from being accessed and redeployed for other uses.

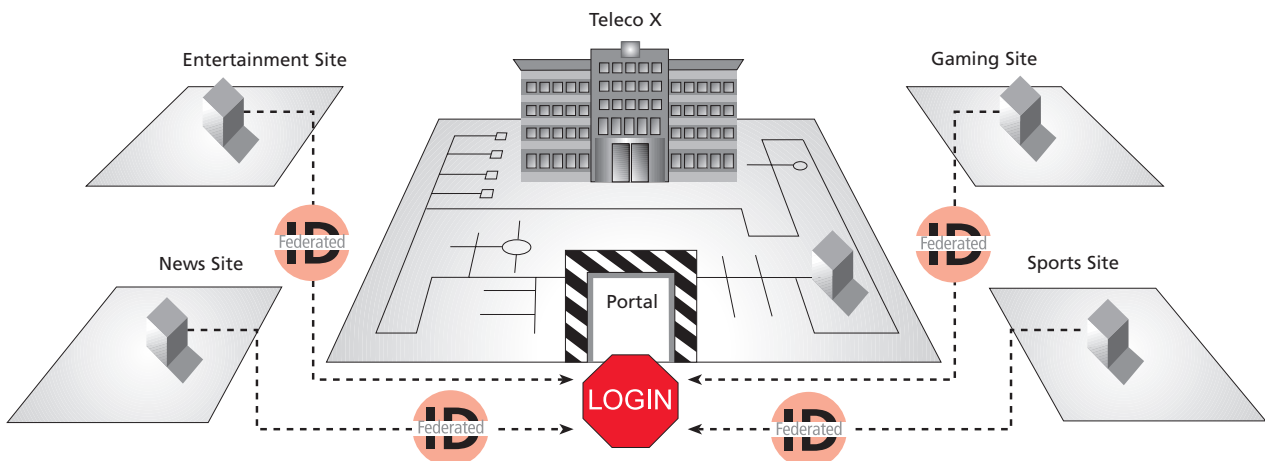
- Canadian Personal Information Protection and Electronic Documents Act — This legislation, which applies to firms operating in Canada, governs the collection, use and disclosure of personal information by organizations.

Key Federated Identity Concepts

There are four key concepts inherent to any federated identity solution: single sign-on (SSO), identity mapping, identity attributes and management. The value of a federated identity solution will correspond to its ability to efficiently provide and easily handle these elements.

**FEDERATION IN ACTION II:
TELECOMMUNICATIONS COMPANY**

This company intends to build brand loyalty by offering its customers access to a number of value-add services provided by business partners. These services would span retail, banking, entertainment, content and more. Customers would login to the company’s web site and click on partner links to access information and services. Customers would be able to click from one service to the next to the next, as if all were resident on the company web site. The company would serve as the identity authority, responsible for authenticating users at login; all business partners would agree to trust the identities of users entering their domains from the company’s web site. Authentication information would pass in the background, invisible to customers and business partners. The company would offer this capability to its partners, who would be able to easily opt in or out according to their needs and preferences.



Single sign-on — While SSO is becoming well understood among users and IT professionals as a means of enabling users to quickly and conveniently access multiple web-based applications, federated identity takes it further by providing single login access to multiple web and non-web applications and network resources (e.g., VPNs) across heterogeneous domains both internal and external to an organization.

Identity mapping — Applications and networks—particularly across different organizations—all employ varying naming conventions; salesperson John Doe, for example, could have a range of different usernames, including Johnd, John_Doe, Jdoe and salesrole. In order to enable disparate systems and applications to accept a previously authenticated user, they must be able to correlate the different conventions. Identity mapping tells an application that Johnd is the same user as Jdoe—and that Jdoe is John Doe and not Jane Doe.

Identity attributes — The more attributes (i.e., information about the user) attached to an identity, the more valuable that identity is to business partners. Attributes can include social security and account numbers, organizational role, account balances, license plate and blood type. Specific examples include the following: Johnd is certified for licensing; employee #245; location = New York City. All user attributes travel with the identity, but some can be blocked to specific organizations by embedded rules and contractual policies designed to protect user privacy.

Management — This refers to the myriad business policies and system tools required to create, provision, manage, maintain and monitor a federated identity solution. It includes the creation, modification and termination of user identities; the agreements forged among business partners concerning acceptance and use of federated identities; and logging and reporting on user activity.

III. TECHNOLOGY ISSUES

Federated identity is a key component of a comprehensive identity and access management (I&AM) solution and, as such, must interoperate with two key I&AM technologies: authentication software and web access management. These are areas in which RSA Security has a demonstrated expertise and leadership position.

Authentication is the process by which the identity of a user is proven. This is often accomplished with a password. However, a password alone is usually insufficient—especially when systems containing sensitive information are involved. The problems with using passwords alone include:

- Passwords can easily be lost, forgotten or shared/overheard,
- Passwords can be guessed or hacked,
- Some applications automatically “remember” passwords,
- Using the same password for multiple resources gives the keys to the kingdom to unauthorized users and
- Password policies tend to be inadequate (i.e., they do not require regular password changes and mandate use of both numerals and letters).

Strong authentication combines a password with at least one other authentication method, such as a time-synchronous token, smart card, digital certificate, Kerberos ticket or biometrics. For example, RSA SecurID® authentication software works with a token to provide two-factor authentication. Users are prompted for their password (something they know) and the random digital “tokencode”—which changes automatically every 60 seconds—that appears on their token (something they have). That way, someone could learn a colleague’s password but not be able to steal his or her identity without also gaining possession of the token. And if someone were to find or steal a person’s token, it would be useless without knowing that person’s password.

Strong authentication is critical to this discussion because the entire concept of federated identity is predicated on the ability of business partners to trust the identities that are shared from domain to domain. That trust is established with the initial login, where a strong authentication solution proves the identity of the user and permits the user to enter the network. [For more information on strong authentication, we invite you to download a white paper on the subject from www.rsasecurity.com.]

Web access management software enables organizations to assign permissions to an identity that authorize a given user to access specific applications and resources. Access control can be implemented in a range of levels, from basic protection (“coarse-grained”) to very granular control (“fine-grained”). With a web access management solution such as RSA Access Manager technology, authorizations can be applied based on rules or roles.

- Rule-based authorization grants or denies access to electronic resources based on whether a user’s privilege profile meets certain criteria. These rules can be yes/no (“grant access if account is valid”) or conditional (“grant access if account is valid, balance is at least \$500 and no payments outstanding”).

- Additionally, transactional authorization can be employed to simplify what could otherwise be a highly complex string of conditions. For example, instead of a rule that states “requested charge is less than \$1,000 if the user has a platinum card, or less than \$500 if the user has a gold card and if the expiration date is prior to January 1, 2006,” transactional authorization removes the actual values and the rule is instead expressed as “requested charge is less than credit limit.”
- Role-based authorization grants rights and permissions to roles rather than to individual users. Users then acquire rights and permissions by being assigned to appropriate roles. By grouping individuals with others having similar access rights, role-based access control (RBAC) streamlines security administration. RBAC specifically addresses part of the HIPAA Privacy standard, which states that covered entities should provide workers with access only to the “minimum necessary information needed to perform their work,” given their particular role in the organization.
- Many organizations possess resources requiring varying levels of access control. For example, a user may be able to view his or her benefits information on the company intranet with just a password, but a sales database may be based on a public-key infrastructure (PKI) solution, requiring the issuance of an additional credential. In order to enable users to work with multiple authentication methods, an organization will want to create an authentication authority or “security token service” capability. The token service will field requests from applications (including those deployed as web services) for a review of the relevant authorization profile, then pass the information to the access management system, which will either issue the appropriate “token” (which could include SAML assertions, X.509 certificates, Kerberos tickets or other)—or challenge or deny the request if a user is not authorized for that credential.

Standards “Stack”

Source: Burton Group, July 2002



Standards and Approaches

In addition to the identity management technologies mentioned above, there are a host of emerging standards that are facilitating the interoperability required to enable a federated identity solution. These standards are providing a critical foundation to some of the leading approaches to federated identity. Those approaches will also be discussed.

First, a couple of key standards from the web services realm that enable connectivity among disparate systems should be briefly discussed.

- **Extensible Markup Language (XML)** is a software- and hardware-independent data format that uses tags to describe—rather than technically format—information. Because it focuses on what data is and not on how it is displayed, data can be shared among heterogeneous applications and systems without the need for translation utilities.
- **Simple Object Access Protocol (SOAP)** is an XML-based messaging protocol that allows web service applications to talk to each other. SOAP provides a uniform way to exchange XML-formatted information across the Internet, using HTTP as a transport.

The key underlying standard for federated identity is Security Assertion Markup Language (SAML). Also XML-based, SAML enables web services to readily exchange information relating to authentication and authorization. This information takes the form of trusted statements—called “assertions”—about end users, web services or any other entity that can be assigned a digital identity. RSA Security was one of the primary creators of SAML and donated royalty-free rights to several of its patents to the effort in order to facilitate industry-wide adoption. Accepted by the Organization for the Advancement of Structured Information Standards (OASIS), SAML has been enthusiastically supported by security vendors to the extent that the Burton Group noted, “SAML’s early success...is clear proof that federation is not only possible, it is a practical identity management solution today.” [For more information, please visit <http://www.oasis-open.org/>.]

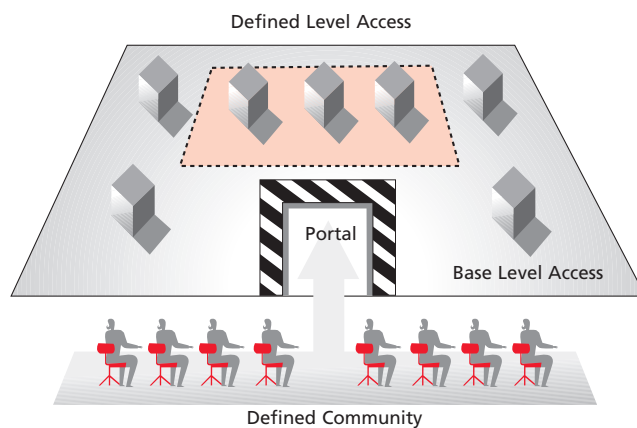
Aside from proprietary, single-vendor domains, which provide a federated SSO solution within a closed community, there are two leading approaches to federated identity that overtly or ostensibly promise to deliver the benefits of such a solution in the open marketplace: Liberty Alliance and WS-Federation.

FEDERATION IN ACTION III:
HEALTHCARE COMPANY

A number of physicians and other healthcare professionals access this company’s web site for information and to participate in clinical trials. This is a highly qualified and targeted audience and acquisition costs are high. To cost-effectively grow the number of doctors and other healthcare providers who come to the site and participate in the trials, the company wanted to link to other online communities of interest worldwide. Because of the nature of the audience base, access must be quick and seamless—the time it would take to re-authenticate at the company’s web site is more time than these people have or are willing to spend. Federated identity is the solution.

Yet there is an additional challenge: individuals with different roles participate in these communities of interest, but certain offerings at the company’s web site are not intended for all. The federated identities would provide for layers of access based on people’s roles. Some would be able to access certain information while others, whose licenses and certifications would be part of the attributes in their identities, would be permitted to go deeper into the web site reserved for the most qualified users.

In order to do this, the company would first have to develop business relationships with these communities, approve legal contracts and then establish a technical relationship to use standards-based tools to federate identities. The identities would assert that the user has this name and comes from this community. The user would have to give consent to become federated and privacy controls would have to be enacted. The federated solution would also have to work in concert with the existing authorization solution.



Liberty Alliance. The Liberty Alliance is a consortium of more than 150 companies—including RSA Security, the only founding security vendor—from a range of industries that are working together on specifications for federated identity, SSO and web access management. Its federated model is the “circle of trust,” in which an organization takes on the role of identity provider, managing a login facility that is shared among its business partners (who may choose to federate or defederate at will). Liberty’s first specification, Identity Federation Framework (ID-FF), is a set of extensions to SAML that enables multiple circles of trust to affiliate, providing greater reach and choice to users, as well as provisions to protect user privacy. ID-FF and Identity Web Services Framework (ID-WSF), another specification in development, are built on open standards, which provides for simpler integration, stronger security, easier management and a higher level of integrity within the system. [For more information, please visit <http://www.projectliberty.org/>.]

WS-Federation. Microsoft®, IBM®, RSA Security and others are also working on standards for federation; currently, 15 of them are planned, including WS-Security (which provides basic security services for SOAP messages), WS-Trust (which defines the means for establishing trust relationships among web services) and WS-Federation (which supports federated identity using a range of authentication methods). The WS-* specifications enable web services to enforce security policies by requiring other web services to authenticate themselves with any of a range of security tokens (such as passwords, digital certificates, SAML or Kerberos tickets). [For more information, please visit <http://msdn.microsoft.com/>.]

IV. NON-TECHNICAL ISSUES

Federated identity is much more than simply a technology solution and there are numerous non-technical issues that must be considered and resolved by any organizations participating in a federated business scenario. These issues revolve around a mutually accepted trust model backed up by appropriate business policies and legal agreements.

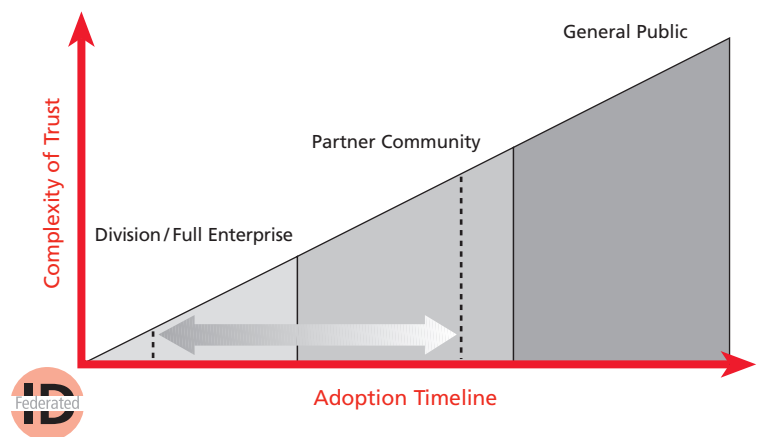
Some important questions for partners to ask themselves as they plan for a federated arrangement include:

- How will identities be vetted? How do partners trust each other to assign credentials responsibly?
- Who is liable in the event that a rogue individual is successfully authenticated within a federated network?
- How do we ensure the integrity of the identity throughout the system?

In a “circle of trust” scenario, the company proposing the arrangement to its business partners will likely assign itself to serve as the identity provider. Yet all partners need to assess whether varying levels of access control are required for specific content areas of their sites. Employees will need to be notified and organizations should decide whether or not to enable them to opt in or out. The negotiations and the legal agreements will be as important to the success of the venture as the architecture and technologies, so they should be carried out thoughtfully and strategically with the help of trusted business, IT and legal advisors. RSA Security, for example, has a great deal of experience helping clients to address these kinds of trust-related business issues.

Deployment Timeline

The extent to which federated identity will be adopted in the marketplace is a factor of the complexity of the trust model involved and the complexity of the technology required to support that trust model. In the deployment scenarios of today’s early adopters [see diagram], it is primarily occurring within large, extended enterprises. For these organizations, gaining the immediate benefits of federated identity—such as enabling efficient two-way access between London-based users and applications and Los Angeles-based users and applications—outweigh the fact that some of the underlying technologies have yet to be officially blessed by the standards authorities.



Federated Identities—Deployment Sequencing

The next stage of adoption is B2B, either bilateral agreements among established business partners or multilateral relationships such as in a B2B exchange. An example of the latter, an automotive exchange, is able to securely manage and share more than 100,000 identities among more than 25,000 companies. The exchange serves as the identity provider and all participating business partners agree to trust those identities. The area of greatest complexity—and therefore the longest to adopt—will be services targeting the general public. These include government-to-citizen (G2C) services, as well as consumer-facing scenarios (B2C), the most popular example being an airline portal that offers customers the ability to book hotel rooms and rental cars from its site by clicking links to its partners.

V. CONCLUSION: RSA SECURITY LEADS THE WAY

Federated identity is a key element of identity and access management (IAM), one of the most powerful and comprehensive security frameworks available for the 21st-century enterprise. The technologies on which these solutions are built have long been part of RSA Security's portfolio of innovative and effective e-security products. The company's two decades of experience and proven expertise position RSA Security as the most highly qualified and trusted architects and vendors of federated identity solutions.

In fact, RSA Security products and technologies are already providing federated identity capabilities—and the business benefits they bring—to enterprises throughout the world. They include:

Authentication. RSA Security authentication solutions continue to set an industry standard for protecting data assets and enabling e-business applications. RSA Security offers organizations a wide range of authentication options including RSA SecurID® tokens and smart cards, RSA® Mobile one-time use access codes, RSA digital certificates and RSA Access Manager password management. These solutions help to positively identify users and devices before they interact with mission-critical data and applications through VPNs, mobile networks, intranets, extranets, web servers and other network resources.

Web Access Management. RSA Security's standards-based approach to web access management is designed to enable organizations to generate revenue and reduce costs by providing secure access to multiple web-based applications and services. The solution helps to map access privileges to end-users, allowing them to move seamlessly and efficiently between the applications and domains they are authorized to access, providing a single sign-on experience.

RSA Access Manager technology is a scalable web access management solution that is engineered to offer seamless integration within heterogeneous and ever-expanding e-business infrastructures.

The RSA Federated Identity Manager (FIM) is a powerful, web services-based solution (XML, SOAP and SAML) that is designed to enable organizations to manage federated identities with their business partners. The Federated Identity Management Module offers a complete solution that includes support for digital signatures and for the three most widely requested and prominent SAML use cases as defined by the industry and OASIS: web SSO profile, attribute service profile and authentication service profile.

Developer Solutions. RSA Security developer solutions help programmers to create secure web services that leverage an identity management infrastructure. These solutions—in the form of RSA BSAFE® and RSA® e-Sign software—are engineered to enable companies to quickly and cost-effectively build privacy, authentication and digital signing technology into virtually any business application. Based on nearly two decades of extensive engineering and cutting-edge cryptographic advancements, these solutions are designed to empower developers to secure data in any format on any network.

ABOUT RSA SECURITY INC.

RSA Security Inc. helps organizations protect private information and manage the identities of people and applications accessing and exchanging that information. RSA Security's portfolio of solutions—including identity & access management, secure mobile & remote access, secure enterprise access, secure transactions and consumer identity protection—are all designed to provide the most seamless e-security experience in the market. Our strong reputation is built on our history of ingenuity, leadership, proven technologies and our more than 15,000 customers around the globe. Together with more than 1,000 technology and integration partners, RSA Security inspires confidence in everyone to experience the power and promise of the Internet. For more information, please visit www.rsasecurity.com.



RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

RSA, RSA Security, the RSA logo, RSA Secured, SecurID and the RSA Secured logo are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners.
©2004 RSA Security Inc. All rights reserved.

FID WP 0504