

The Rise of FEDERATED IDENTITY

Federated Identity is a hot topic.

At the same time, it is one that isn't well understood. For some

it isn't clear exactly what the term means. Others understand it a bit, but ask "is federated identity really deploying anywhere?" Still others see multiple standards and wonder how to avoid picking the wrong one.

There are already hundreds of real-world federated identity projects underway, and the pace of deployment is rapidly accelerating. And as it does so, it is becoming clear that federated identity is destined to transform much more than just technology.

The broader technology marketplace is beginning to become aware that solving many of its IT and compliance problems will require something called identity or identity management. Just as internal enterprise identity management is becoming understood, however, a new thing called federated identity is starting to create buzz and scream up the hype cycle. What is federated identity, and how does it fit into the pantheon of authentication, authorization, identity management and identity based audit products on the market?

What Is Federated Identity?

The earliest and simplest definition of federated identity is the management and use of identities across security domains. Indeed, solving the use case of single sign on across security domains is what drove the creation of SAML, the first federated identity standard (see sidebar.) Linking identity, however, recreates

a pattern that occurs in all networked computing – the need to change your thinking about management, security, and control from hierarchical to networked. Recent deployments of federated identity highlight these implications of creating identity federations.

In this feature section, we highlight federation through real world deployments, stories you probably haven't heard on the history of federated protocol development, and context and perspective articles that deal with its structure, deployment evolution and business and technological implications. To fully appreciate the power of the concepts behind federated identity, you must understand the context of the task it is being called on to do.

The Nature of Federated Identity

Federated identity marks an inflection point in both technology, and the business processes it enables. Businesses are used to having control over all of the identity information



their computing systems use. But in a networked business setting some identity information always exists beyond any single corporation's control. Thus as federated identity allows the use of identity information across boundaries, it must inevitably deal with issues like liability, privacy and trust.

Federated identity is a technology that cannot be viewed in isolation from the business processes that it is enabling. As identity is federated it becomes much more than simply linking existing security and access control systems. It forms the foundation for automating truly networked business processes and making them predictable and manageable.

Separating Identity Management from Identity Use

Federated identity must ultimately develop techniques to address the network demand to break the use of distributed identity data apart from its administration and management. This separation is required to allow identity use to scale along a different axis than identity administration. The management problem that immediately appears (and currently remains unsolved in any generalized way) is how to keep "control" of the identity data once its management is distributed differently from its use. This is usually spoken of as the issue of trust in a federation. Trust is needed so that all of the identity based assertions made in a federated transaction can be "trusted" or insured accurate to the required level of certainty by all parties to the transaction.

A little understood implication of the management of federated identity systems is that once identity is federated, no overarching hierarchical management system can remain to ensure a single point of con-

The Protocols of Federated Identity

SAML 1.0, 1.1 and 2.0 – The Security Assertion Markup Language (SAML – pronounced "Sam –el") standard specifies an extensible language for securely exchanging user information between security domains. Published by the OASIS Security TC, SAML 1.0 defines a security token format (called an assertion), as well as 'profiles' that define methods of using these assertions to provide web single sign-on. SAML 1.1 incorporates feedback and errata from the 1.0 specification, but because of namespace changes it cannot be made backward compatible with SAML 1.0. SAML 2.0 is currently in the solution proposal phase – a state meant to address the requirements outlined in the market requirements document. A primary objective of SAML 2.0 is an incorporation of Liberty ID-FF 1.2 (see below) in hopes of creating some convergence. (for details see <http://oasis-open.org>.)

Liberty Phase 1 (ID-FF 1.0) – The Liberty Alliance Phase 1 specification extends SAML 1.0 by adding its own profiles for how to wield SAML assertions. These additional profiles add support for account linking, identity provider introduction, and global logout. The Liberty Alliance model defines roles within a federation – an Identity Provider (IdP) and a Service Provider (SP). Liberty ID-FF1.1 incorporates feedback and errata from the 1.0 specification. (for details see <http://www.projectliberty.org>.)

Liberty Phase 2 (ID-FF 1.2 & ID-WSF 1.0) – This set of standards extends the ID-FF specification with new functionality, such as one-time assertions of identity (for anonymity), metadata exchange, and affiliate relationships. The

Liberty Phase 2 (ID-WSF 1.0) specification is a set of standards that adds functionality for discovering and offering identity-related services. Profile access mechanisms are specified as an initial service, allowing for access to user attributes. The Liberty Phase 2 specification defines many of its messages and protocol bindings in terms of SAML 1.1, and uses WS-Security for securing SOAP messages.

Liberty Phase 3 – This set of standards are still in the elaboration stage, but it is expected that ID-WSF will be extended with new services built on top of attribute exchange, such as a digital wallet and calendaring/address book services.

WS-Security – This specification, published by the OASIS Web Services Security TC, defines mechanisms for providing security token-based integrity and confidentiality on Web Service (SOAP) messages. Several security tokens are defined, as well as a mechanism for associating them with messages. (for more information: <http://www.oasis-open.org>.)

WS-* (WS-Trust, WS-Policy, WS-Federation, etc.) – This collection of specifications is an evolving set of Web Service-oriented mechanisms being developed by IBM and Microsoft for layering authentication, authorization, and policy across both single and multiple security domains. WS-Federation defines a framework for federation. Profiles will be developed subsequently to specify the details for implementation. Microsoft and IBM have indicated their intention to contribute these specifications to a standards committee once they are largely developed, as they did with WS-Security.

trol. Thus administration, management and control must become a networked proposition, and the governance issues, liability, etc. must be distributed using methods that can be shown to maintain trust despite the fact that the people involved don't coordinate their management efforts very much at all.

A brief look at how identity wants to be administered reveals that its axis of distribution is quite different from the axis that the identities themselves will be used on. Administration must ultimately distribute through extreme delegation along line-of-business management and must reliably network administrative workflows across business boundaries. Identity use, on the other hand, needs to follow applications, data and users around the network.

We've Been Here Before – And Failed

Federated identity isn't the first attempt to integrate identity across boundaries. Public Key Infrastructure (PKI) was one high-profile attempt to deal with this problem. By providing authorities to certify identity, and a means for authenticating and verifying identity PKI was supposed to allow "trust" across boundaries. In practice, however, PKI has failed to produce a scalable, cross-boundary, identity management capability. For federated identity to create the environment of trust the problems it is working to solve require, it must find ways to address the use of digital certificates – or something equivalent – in a fashion that is reasonable to administer, and which provides the require levels of trust.

The Liberty Alliance ID-WSF model addresses this through the use of techniques such as discovery, opaque identifiers, distributed identity attributes, etc. Doing so opens the way to applications that have long been contemplated but not been possible. We examine one such federated identity deployment in the article "eRX Takes Federated Identity Beyond

Real World Deployments

Federated identity is in an explosive phase of real world deployment. Burton Group Analyst Dan Blum has identified nearly 200 corporate federated identity projects in the process of deployment. Several companies are using federated identity to integrate outsourced business process provider services (such as employee benefit plans) into their employee portals. Companies such as Boeing are using federated identity to integrate access to services by airlines that use their products. Beyond linking services into web portals, the Liberty ID-WSF specification is being deployed by several in the mobile services to allow the delivery of several new products through a variety of channels.

Vodafone has collaborated with Trustgenix and GameFederation to build a Liberty-enabled multiplayer mobile gaming proof-of-concept. Liberty is used to federated authentication, and through Liberty's discovery mechanism, a user can discover a game site over Vodafone's network, access it, and then personalize his or her experience while playing that game.

Radio@AOL has combined with D-Link to create a service that uses fed-

erated identity to allow digital radio and digital photography access through a wireless player connected to a home entertainment center and managed through a TV interface and remote control. They also deployed a prototype with Nokia that used federated identity to allow users to subscribe and listen to radio services through Nokia cell phones. This prototype demonstrated using the ID-WSF specifications — particularly the authentication, discovery, and permission-based attribute sharing and security features — to enable any cell phone user to access and personalize the Radio@AOL service using their Nokia mobile handset.

From financial services to pharmaceuticals, to mobile services, federated identity is already enabling new services to be deployed. This year will see many prototype, pilot, and early production deployments. In 2005 federated identity production deployments should ramp significantly. According to a recently released Radicati Group report, sales of federated identity products will reach \$738 million in 2004 in worldwide revenues, and grow to over \$10.2 billion by 2008. Federated identity is real, and it is moving into production.

SSO" which illustrates trust federation with digital certificates.

By not requiring a single global, hierarchical, trust model, but allowing the organic development of networked trust models, federated identity opens the door to successfully solving the network identity trust problem. It acknowledges the needs of real world networking, and allows for each federation to develop its management, trust, and liability apportionment

techniques. The protocols may need to be updated as lessons are learned, but one of the strengths of federated identity is that it is a model that can adjust.

The Current State of Federated Identity

Today we have reached the point where federated identity technology has learned pretty well how to decouple, distribute, and execute using federated identities if it

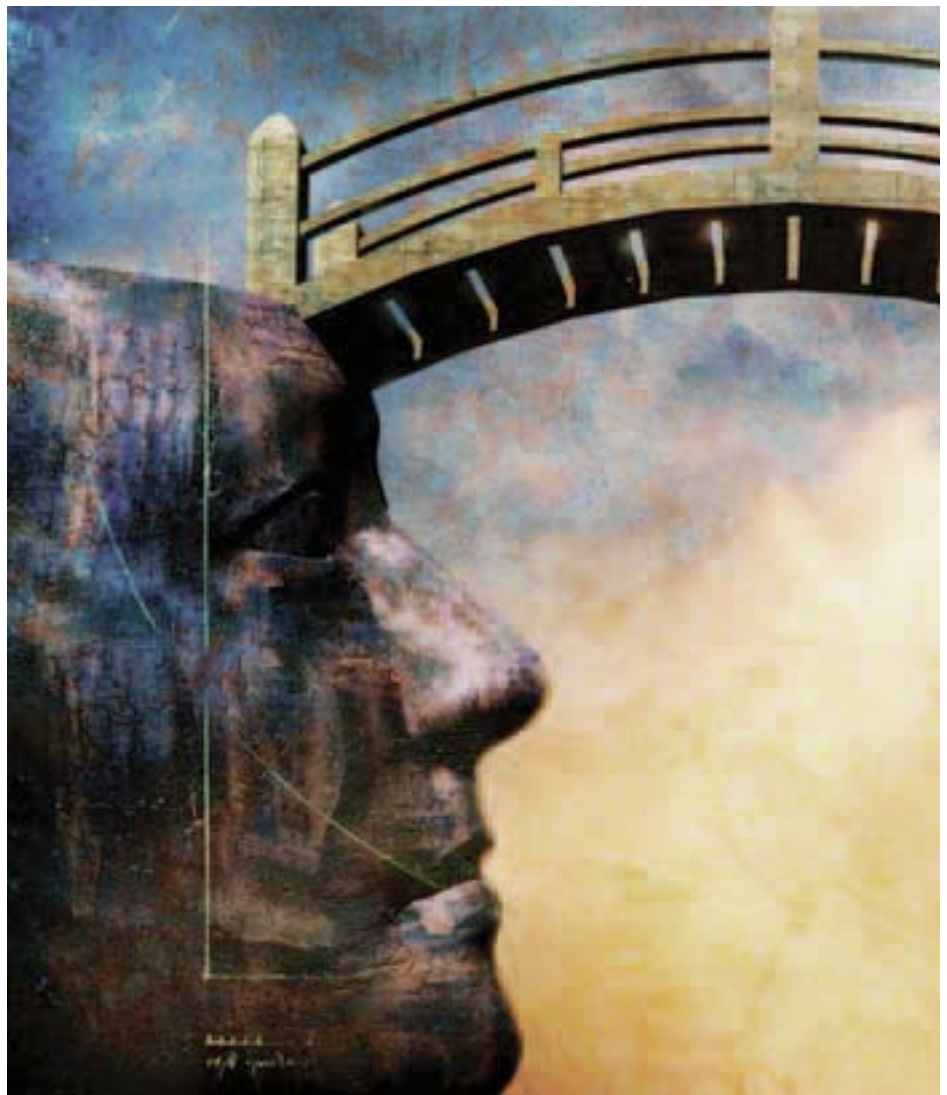
“assumes” they have been properly managed “out of band” and can be trusted. We are just at the beginning, however, of understanding the real needs of the federated administration of identities. Archie Reed examines the continuum of federated trust models and their missions and looks at the implications for administration and management in “Federation – The Final Frontier.” In the process, he shows that it is possible to get from where we are to where we need to be using federated identity.

Federated identity allows a staged approach that can begin with using existing enterprise authentication systems and grow incrementally as “circles of trust” take on differing requirements for different networked applications. Linda Elliott examines how this trend is already playing out in real world federated deployments in “The Evolution of Federated Identity Deployments.”

Real World Deployments

In this feature section we examine two real world deployments in detail. First, in “GM Deploys Federated Identity and Learns,” we look at one of the use cases that has been an example of why federated identity is needed – the integration of an outsourced benefit provider’s services into a company’s enterprise portal. GM candidly shares what it has learned from going through this process, and the effect the experience has had on the company’s identity management initiatives.

In “eRX takes Federated Identity Beyond SSO” we investigate how federated identity combines with web services to provide capabilities beyond single sign on. The real estate industry has tried to automate the mortgage and land title recording process unsuccessfully for years and this real-world production



application shows how the discovery services of Liberty ID-WSF federated identity created the ability to network PKI-based digital certificate usage in ways that were previously impossible.

What’s Going on With Protocols?

A major concern of those looking at federated identity today, is the proliferation of protocols, and fear of a “protocol war” that leaves them with the wrong choice of technology. We examine the history that created each protocol and then look at what that means for where things might go in the future in “The Future of Federated Identity: Ivory Tower or In the Trenches.” This article gives you the background to understand how and why each protocol arose, and the motivations behind them as well as where each is headed.

Summary

Federated identity marks the step at which identity based computing can truly create business value. Federated deployments are now beginning in the hundreds, and much more will be learned about the business impacts and technology of federated identity in the next year or so. Many trends in computing create buzz and excitement, but ultimately fail to become what they once appeared they would. But federated identity is a trend that will not be denied, because it is rooted in the intrinsic nature of networked computing. Ultimately federated identity will return the manageability and security that was lost when applications began becoming distributed on the internet, enabling truly networked business processes that release tremendous business value and productivity. ■