Federated Identity Management
Corporate strategies for managing security, liability, scalability and the risk of fraud as identity moves towards federation.

Abstract
As a consequence of globalization and increased pervasiveness of outsourcing, the emergence of federated identity will require enterprises to re-examine their approach towards inter-company information exchange, especially as it pertains to digital identity -- establishing quality control and managing liability and risk within the context of required interdependence.

Enterprises are faced with an increasingly complex set of challenges as they balance the need for security and the growing requirements for seamless access to information from a diverse set of users. While existing identity management solutions can help reduce the inefficiencies associated with managing users, roles, permissions and access to information, there are a growing number of applications that require the inter-company (federated) exchange of identity-based information (e.g. single sign-on, web services etc.). This document explores the complexity, requirements and merits associated with wide-scale deployment of identity federation, including strategies for pooling resources and the creation of standardized business frameworks for assuring quality, maintaining security, managing liability, reducing risk and resolving disputes.

Eric Norlin and Andre Durand
PingID Network, Inc. | 1899 Wynkoop Street, Suite 600 | Denver, CO 80202
Table of Contents

The IT Dilemma ......................................................................................................................... 3
The Advent of Digital Identity .................................................................................................... 4
From Enterprise to Federated Identity Management ............................................................... 5
Identity Federation .................................................................................................................... 6
Challenges of Wide-Scale Identity Federation ......................................................................... 8
Defining a Solution: The ATM Network Analogy ..................................................................... 13
Enter the PingID Network – An Identity Network Operator .................................................. 14
Conclusion ................................................................................................................................ 15
The IT Dilemma

The 1990’s witnessed the adoption of an increasing number of enterprise information systems, each designed to streamline business processes through electronic automation. With the introduction of new systems for managing customers, supply chains, content and corporate knowledge, enterprises have been challenged with how to cost-effectively integrate and maintain an increasing number of information systems across a growing number of networks and platforms. Simultaneously, enterprises have also been challenged by the need to provide increased access to a larger and more dynamic group of end-users.

The challenge of managing these systems has resulted in a complex IT dilemma – namely, how to control costs and maintain security while increasing access to information.

As a consequence of globalization and to add to the growing list of corporate pressures, IT departments are now being forced to increase access to information for both employees (e.g. intranets) and partners and customers (e.g. extranets, supply chain management etc.). These and other pressures are driving corporations to re-evaluate their security and information architectures to accommodate the increasingly dynamic and transparent ways in which a growing number of parties wish to interact.

© Copyright 2002, PingID Network, Inc. All Rights Reserved
The Advent of Digital Identity

New distributed computing models such as those provided by web services create a fresh set of challenges which in turn give rise to a requirement to establish stronger and more granular methods of electronic identification.

To meet these new challenges, emerging technologies such as ‘Digital Identity’ are now being recognized as a key ingredient in the re-architecting of systems to accommodate the secure adoption of more distributed and transparent computing models.

**Definition: Digital Identity**

A Digital Identity is a virtual representation of a real identity that can be used in electronic interactions with other machines or people. The value of Digital Identity is that it allows us to transpose the ease and security human interactions once had when we knew each other or did business face-to-face, to a machine environment where we are often meeting one another (virtually) for the first time in transactions which might span vast distances.

A digital identity is typically accessed or managed through an ‘authentication’ process which is normally comprised of a username, a password and or some additional form of verification such as biometric or smart-card. Generally speaking, a digital identity is made up of several components, which include information related to the identity (profile or attribute data), the credentials which have been assigned to that identity (certificates or signatures) and in some cases, an electronic reputation.

Unlike a physical identity, digital identities are typically distributed, with pieces of information located at different places throughout the network. As individuals living in a progressively more digital world, we have a growing number of digital identities which are used to identify us in our relationships with other entities (e.g. drivers license, social security number, United Mileage Plus number, credit cards, phone numbers etc.). The issue is not how these identities are created, but how to manage the linking or sharing of the ones that already exist.

The broad adoption of XML Web services as a computing model means that solutions no longer reside just within the four walls of an organization—while this brings new capabilities, it also forces one to consider how to manage trust and identity, not just across internal applications that are tightly controlled by corporate IT, but also to manage identity information across applications and services that span organizations, platforms, security approaches, and programming models.

Microsoft Website regarding Federated Security and Identity Roadmap

As corporate IT systems become more distributed and interdependent with partners and affiliates, new Digital Identity-based information architectures are
helping to readily “identify” each component (application, web service, device, user etc.), thereby allowing IT departments to maintain security while allowing increased access to sensitive information. By answering the questions: a) Who are you? B) What are you allowed to do? and c) Where are you allowed to go? in a cost efficient way, IT departments are able to respond to the pressures of globalization by safely allowing their boundaries to become more transparent and permeable without sacrificing security.

To manage the transparent access to information, companies are integrating identity management solutions to automate the procedures for user and role provisioning, password management and access control to information. To date however, the bulk of these solutions have focused on the internal use and management of identity, and not the interdependent management of identity information between companies -- what is now referred to as ‘Federated Identity Management’.

**Evolution of Identity Management**

![Evolution of Identity Management Diagram](image)

While current identity management solutions provide distinct cost-saving benefits, they do not specifically address the issues which surround the emergence of identity federation, namely, how to safely exchange identity information between companies, without incurring liability.

**From Enterprise to Federated Identity Management**

The true nature of the identity challenge is just now beginning to unfold, and stems not from how corporations manage identities within their control, but how they handle identities that are at least partially beyond their control.
Federated Identity Management (FIM), or the management of identities between corporate boundaries, has recently emerged in response to the desires to simplify the way in which individuals (consumers) are able to move between companies. Applications such as shared sign-on (SSO) and the emergence of web services architectures are driving the need for companies to understand and manage inter-company dependencies. Unlike Enterprise Identity Management (EIM), where technology resolves a good portion of the corporate IT dilemma, FIM raises issues which are far more complex and extensive, and require new approaches. To truly appreciate the FIM challenge, one must recognize that some identity information fundamentally exists beyond the corporate firewall, and is therefore at least partially beyond any one corporation’s individual control.

The adoption of new distributed computing models (e.g. federated identity and web services) are requiring enterprises to recast their view of themselves as a component of a larger interdependent construct. Furthermore, the hard boundaries of today’s corporate firewalls are dissolving, or at least becoming semi-transparent -- allowing for more transparent movement of the individual between control boundaries.

**Identity Federation**

Federated Identity is just one of several new distributed computing constructs that recognizes the fact that individuals move between corporate boundaries at an increasingly frequent rate. Driving the requirement to understand the implications of identity federation is the rise in popularity of Shared Sign-On (SSO), an application which reduces redundant logons by allowing applications, systems and companies to share a user (identity) authentication. As a consequence of inter-company SSO, and the interdependency which is assumed in such
interactions, companies are now forced to deal with new issues such as liability, risk and the costs associated with establishing trust and security in a quality conscious manner. As one would expect, these new challenges give rise to new costs, including: (i) the cost of negotiating and establishing formal agreements with electronic trading partners, (specifying the rules which will govern the exchange of identity information—including provisions for legal liability, dispute resolution and ensuring compliance with privacy requirements), (ii) the cost of implementing new technologies and (iii) the cost of maintaining security.

“Over the next few years we have to deal with some very messy problems – namely, what it takes to deploy federated technology along with what it takes to bash out contracts between partners…”

Michael Barrett, Vice President of Internet Strategy at American Express & President of Liberty Alliance
Challenges of Wide-Scale Identity Federation

While it’s entirely possible to control the costs and complexity of identity federation on a limited scale, within small circles of trust, wide-scale federation introduces new costs, complexity and challenges which exist on an entirely new scale.

The reality is, trust will only take you so far in terms of managing quality and maintaining security in a new world of inter-company computing dependencies. It’s inevitable that if companies are to realize the full potential of the Internet as a medium for automated electronic interaction, they must holistically approach the challenges which allow for one another to engage on the largest of scales -- everyone talking to everyone.

To efficiently enable wide-scale identity federation, without incurring incremental costs which are proportional to the number of relationships which are established, both technology and business standards must be established and new frameworks for creating these relationships explored.

<table>
<thead>
<tr>
<th>Wide-Scale Identity Federation Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Standards</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual Confidence</td>
</tr>
</tbody>
</table>

| Business Standards | Defined Liability | Pooled Knowledge | Privacy Legislation |
| Minimum Requirements | Dispute Resolution | Revocation Procedures | Fraud Protection |

Figure: Four major areas which must be addressed to enable wide-scale identity federation.
In analyzing the complete spectrum of technical and business issues surrounding wide-scale federation, the following challenges must be addressed:

**Interoperability Standards**

Technical interoperability is the cornerstone of efficient wide-scale federation. Without interoperability, the full potential of identity federation will never be achieved. Addressing interoperability requires cross-industry cooperation to ensure that the resulting solutions address the wide range of systems with which it must integrate. The Liberty Alliance Project is one such consortium which understands the need for open standards surrounding interoperable federated identity.

*The mission of the Liberty Alliance Project is to establish an open standard for federated network identity through open technical specifications.*

*Liberty Alliance Project Website*

**Managing the Needs of All Constituents**

Unlike the management of identity within an enterprise, where user data is deemed proprietary and an asset of the corporation, federated identity requires that the privacy requirements of any of the individual be satisfied and that the exchange of data does not violate government legislation such as the Health Insurance Portability and Accountability Act (HIPPA) or Gramm Leach Bliley Act (GLB).

*Figure: Successful identity federation requires that the needs of three different constituents be met: 1) individual, 2) government and 3) business.*
The challenge of federated identity lies in managing – and indeed aligning – the needs of all three constituents. Without a structure for doing so, constituents might soon find themselves at odds with government legislation, privacy concerns of consumers or the needs of business to better serve its customers.

**Ever Expanding ‘Circles of Trust’ - Peering to the Nth Degree**

Establishing legal agreements will become even more important as companies engage ever larger concentric circles of trust, moving from known and trusted trading partners to first time interactions with a growing number of entities. Practically speaking, while it is possible to establish agreements with a few dozen entities through bilateral negotiation, it is entirely cost prohibitive and impractical to do so with hundreds or potentially thousands of companies.

To overcome this challenge, new models of peering must be explored -- models which do not introduce proportional costs, or introduce an inconsistency in the handling of identity relationships.

**Dispute Resolution**

Just as the necessary business agreements must be established for the federation of identity, so too the necessary measures for handling and resolving disputes and intrusions must be addressed. Imagine a customer of an online brokerage firm who uses a shared identity to access their account to perform a critical trade but is unable to do so as a result of a problem stemming from the shared authentication. Who’s at fault? Who’s financially liable? What’s the individual’s recourse? And most importantly, what are the efficient and timely procedures for resolving the incident? Without a defined resolution process to the issues which will arise as a result of inter-company dependencies such as this, the legal ramifications alone would prohibit voluntary interaction.

**Liability**

In today’s legal environment, liability is big issue and most parties who engage one another electronically specifically limit or explicitly refuse to incur any liability which results from representations they make to others. With a movement towards web services and identity federation, inter-company dependencies become fundamentally more substantial and the potential ramifications which may result from assertions which are inaccurate more damaging.
Example: An individual who signs into My Yahoo clicks through to their brokerage account (and is automatically signed-in via Single Sign-On) to sell a stock that has performed well and is an unrealized gain. Perhaps the stock has recently become active and the trade is time-sensitive but the individual is unable to complete the transaction because of a technical problem associated with the SSO. *Who’s at fault?*

Initially at least, it is unlikely that any additional liability will be tolerated as companies begin to engage one another in federated identity interactions. While this may be satisfactory (because the risk is known) when dealing with known and trusted trading partners, it becomes less tolerable when engaging or relying upon an unknown company’s assertions. Long term, the future of web services and identity federation depends on the industry at large to define acceptable methods of addressing quality in identity assertions, thereby reducing the risk of financial liability. Furthermore, accountability must be established as companies engage one another in asserting identity or other forms of information within the larger context of federation.

**Quality Assurance**

Overall, addressing the issue of quality identity interaction is a major challenge in the context of wide-scale federation. *Who will stand behind a given digital identity when fraud occurs? How can companies limit their exposure to the propagation of a fraudulent authentication throughout the network? How can one validate that a particular digital identity pertains to a particular individual?* Without an ability to assure or affect quality in the assertions which are made between companies, the cost of misplaced trust outweighs the rewards of relying upon others.

A foundation for enabling quality begins with an ability to define (and enforce) minimum standards and requirements. Each party must assert that they can and will adhere to these minimum requirements, and each party must have an ability to confirm that standards are being adhered to.

Furthermore, legally binding recourse must be defined in a context which motivates (if not rewards) each party for continual improvement in the quality of the assertions which they represent to other relying parties.

**Revocation**

One of the risks of identity federation is that security becomes interdependent, a notion which is viewed negatively or in some cases unacceptable by IT.

Example: If Company B relies upon the authentication of Company A to allow a given identity to complete a financial interaction or access sensitive information,
these transactions are dependent upon the quality of the initial authentication performed by Company A.

Furthermore, as an identity-owner, the possibility that linked accounts (within an identity federation) can result in additional damage to one’s reputation if compromised by identity fraud is potentially terrifying.

Therefore, in an environment where security breaches will inevitably occur, solutions that allow companies to minimize the resulting damage or financial exposure is essential. Defining the federated procedures for revoking credentials, suspending an identity or lowering the confidence in a particular interaction must become an integral component of any quality assured identity network.

Risk Management

Every interaction which involves a third party inherently introduces new risks. While every company’s risk tolerance is different, each company must evaluate for themselves how much they are willing to invest to reduce risk.

Within the context of wide-scale identity federation, the risks of misplaced trust can easily outweigh the potential return of having the freedom to interact with everyone. On the other hand, the risk of isolationism can result in a loss of marketshare to those companies who better serve the same customer.

In today’s non-federated environment, risk is both assessed and addressed on a company by company basis, a format which is appropriate, but also expensive and inappropriate or perhaps even cost prohibitive in a federated environment. With proper coordination, both group and individual risk can be minimized through pooled efforts. One of the ways to address this collectively is to define for the federation the same minimum quality standards, standardized procedures, certification and credential programs which are used individually, and to track the adherence to these standards as well as the successes and failures of each party. Pooled information on breaches can be invaluable in pin-pointing and correcting weaknesses in the federation constituency and procedures.

Privacy Compliance

As identity authentications and attributes are shared within an identity federation, businesses are compelled through privacy legislation to be cognoscente of the individual’s privacy rights and preferences. Identity federation simply does not work if an individual is subjected to differing privacy policies but is not explicitly made aware of such fact as they move from one company to the next within a SSO interaction.

Recent Federal legislation has required stricter identity verification and authentication for account management, transactions and information transfer.
These include **Gramm-Leach-Bliley Act (GLB)** and the **Health Insurance Portability and Accountability Act (HIPAA)**. GLB provides for closer ties among banks, securities firms and insurance companies as long as they follow specific guidelines for privacy and security of customer information. HIPAA requires that healthcare institutions take reasonable steps to limit the disclosure of an individual's personal health information, including training of employees to follow privacy procedures, designating an individual to oversee the organization's privacy initiatives, and securing access to electronic patient records. Covered institutions generally have until April 2003 to comply. As of October 23, 2002 – the first official compliance deadline – 20%, or 400,000 of the 2 million obliged organizations, filed for extensions including the government organization administering HIPAA regulatory control.

As noted earlier, identity federation MUST accommodate the needs and desires of all three constituents, the individual, the business and the government. Once again, a pooling of resources within an identity federation can reduce redundancy and thereby alleviate or help to solve many of these issues.

**Defining a Solution: The ATM Network Analogy**

One potential framework which can serve as a model to understand how many of the challenges surrounding federated identity can be resolved can be found in the analogous history of the evolution of ATM and other financial networks.

For hundreds of years, the banking industry was characterized as a local or regional business. With the advent of ATM’s, it became possible to extend a bank’s presence to allow cash withdrawal 24/7 from a much greater number of locations. While this enhanced consumer convenience, it also created a problem, namely, how individuals could remove cash from any ATM, even if the ATM was part of another banks network.

To resolve this issue, banks began to regionally establish regional partnerships and to invest in connecting their systems. While this resolved some of the problems, at least within a defined territory, it left the traveling individual to another state or country without a solution.

Once more, it was becoming increasingly cost-prohibitive for banks to negotiate and establish what appeared to be a never ending number of ATM partner relationships and similar issues of quality, risk and liability became a challenge to manage as the number of relationships increased.

In response to this problem, national and international ATM networks were established to respond to this “Peering Nth” degree dilemma. By establishing a set of common operating rules and regulations, these new independent third party ATM networks were able to establish quality control with minimum requirements and standardized procedures, maintain security, control, and mutual confidence,
while at the same time eliminating the requirement for every bank to communicate directly with every other bank (by offering transaction clearinghouse services).

At the core of many of these networks was a member-owned corporation that provided for a fair and equitable governance structure, affording its membership an opportunity to define for themselves the operating rules and minimum requirements which would govern how they would interchange with one another.

**Enter the PingID Network – An Identity Network Operator**

The PingID Network is a member-owned, technology-neutral identity network, the first of its kind designed to provide the necessary business and legal framework for the accelerated development of wide-scale identity federation.

By joining PingID, member companies are afforded an opportunity to instantly engage all other Network members in quality assured identity-based interactions, similar in nature to how financial institutions established national and international ATM networks to control quality, manage risk, limit liability and accelerate the clearing of debit transactions between one another.

**Member Services Include**

- Standardized business / legal agreements for federation
- Standardized interoperability rules and dispute resolution procedures
- Shared services for enhanced interoperability and identity interchange

**Member Benefits Include**

**Reduced cost of federation** – standardized agreements, shared resources and pooled knowledge make widespread FIM affordable across all market segments.

**Reduced complexity** – as peering becomes standardized, it reduces a requirement to maintain one-off relationships.

**Increased interoperability** – a standardized business framework combined with enhanced identity interchange services improves interoperability.
Improved ability to comply with privacy legislation – by providing services which help individuals manage their privacy preferences, enterprises are better equipped to deal with existing and new privacy legislation.

Improved trust – by providing enhanced services which enable distributed trust, companies can engage one another with increased confidence.

Improved framework for resolving new issues – by providing defined procedures for resolving emerging issues, companies can spend less time focusing on identity and more time focusing on their business.

Conclusion

Businesses are challenged with two seemingly opposed trends, the need to increase access to information and the need to maintain security. As firewalls become increasingly semi-permeable, companies are forced to re-examine their approach towards security. New digital identity constructs are serving to help solve this dilemma, allowing known entities to access information with confidence, but new infrastructures are required to manage these identities. Corporations are now beginning to invest in identity management solutions to administer users, roles and permissions but these solutions do not address the issues that arise as a result of inter-company identity services (identity federation) such as shared sign-on.

The rapid adoption of identity services in the absence of formalized inter-company business processes, procedures and standards will result in a patchwork of isolated solutions and a growing and inefficient replication of unmanageable legal agreements. An organized effort is required to represent the best interests of the business community and the end-user at-large. This is accomplished by establishing the business process standards which are required to ensure security, reliability and interoperability.

Through common business frameworks (e.g the ATM network model), pooled resources and shared services, companies can efficiently and with confidence engage one another in wide-scale identity federation.

Please send questions or comments to eric@pingid.com or andre@pingid.com.