Enabling Federated Identity for E-Government

Tanya Candia
Enosis Group, USA

Paul Madsen
NTT, USA

INTRODUCTION

Today's administrative and business environment calls for information sharing on an unprecedented scale, from government to business to citizen. Sharing and interoperating among agencies, businesses, and governments around the world create opportunities to simplify processes and unify work, as well as improve the overall performance of government. Secure interoperability, based on identity management solutions, enables substantial cost savings, streamlined processes and faster communication of vital information to the benefit of governments and citizens of all nations.

At the core of this revolution is the concept of federated identity management and the need for standards that are open, interoperable and decentralized. In addition, such standards must allow for privacy safeguard across all sectors. The Liberty Alliance Project (Liberty Alliance, n.d.) was established to address this need and tackle the twin issues of standards and trust.

BACKGROUND

Today's administrative and business environment has created an unprecedented need to securely share sensitive information among national, regional and local governments, agencies and organizations, as well as with citizens and business entities. The true distributed computing platform created by the Internet brings into sharp relief the importance of adhering to emerging privacy standards and data security regulations.

Identity is at the core of any information-sharing transaction: government to citizen, government to business or government to government. Individuals' identities not only prove that they are who they say they are, it also indicates what they can do and what resources they can access. Governments are often the source of core documents that relate to one's identity: birth certificates, drivers' licenses, employment and tax records, marriage and death certificates, and the like. Identity credentials are perhaps more relevant in today's digital society in their electronic form than on paper.

Identity Management Issues

Effectively managing one's identity means retaining control over the information relative to who one is, who has access to it and how it is used. While simple in the abstract, the task is enormously complex in reality. Even within a single organization, an individual may rely on multiple identities: an employee may need to authenticate to a database, an application or a service using completely different mechanisms. Once outside the organization, the problem is compounded. Multiple organizations will hold multiple instances of identity and attribute information. The problem of effectively managing all these instances is enormously complex, resulting in ineffective identity management and complexity.

Furthermore, as governments, citizens and businesses extend their services, they are challenged to grant access to resources and applications to the right people at the right time without sacrificing privacy, security or scalability. Since today's communities of interest are built and modified on a dynamically changing basis, trust must be able to be created or eliminated quickly. The old ways of managing identity dramatically reduce the organization's ability to move quickly enough to respond to changing relationships.

The Ideal Solution

Ideally, government would like to have the ability (whether through technology, business practices, policies, education or a combination thereof) to meet the following seemingly conflicting requirements:

- Simplify access to services and applications both inside and outside the organization
- Reduce the need to maintain and manage multiple sets of identity credentials
- Reduce the cost and complexity of managing identities

- Enable dynamic creation and management of trusted relationships
- Preserve privacy and ensure data security.

FEDERATED IDENTITY MANAGEMENT

Fortunately, there is a solution that approaches the above ideal: *federated identity management*. Federated identity management makes it possible for an authenticated identity to be recognized and take part in personalized services across multiple domains. Federated identity avoids the pitfalls of centralized storage of personal information while allowing users to link identity information among accounts. Since users can control when and how their accounts and attributes are linked and shared, they retain greater control over their personal information. In practice, this means that users can be authenticated by one organization or Web site and be recognized and receive delivered personalized content and services in other domains without having to re-authenticate.

Increasingly, governments are looking at federated identity as the preferred underlying identity architecture for interacting with their various constituencies and partners. Federated identity provides governments with an open and standards-based approach for enabling access to sensitive internal resources to external parties.

The advantages of federated identity include:

- A standards-based mechanism of both sharing and managing identity information as it moves between discrete legal, policy and organizational domains
- A cost-efficient means of establishing single sign-on to cross-domain resources
- A simpler way to grant and revoke user access to information
- A reduction in the number of sign-ons and passwords an individual must work with to access multiple systems and databases
- Greater security when it comes to user access to information.

PUBLIC SECTOR BENEFITS

Within a single government organization, a federated identity management infrastructure can bring substantial cost savings, operational efficiencies and increased security. These benefits come in the form of more effective employee provisioning and password management, focused development efforts on a single standard that will be supported by a variety of technology providers, and the ability to more easily outsource certain employee applications in a secure and flexible manner. Also, since employee identities can be managed internally and brought online and off-line quickly, deployment of a federated identity infrastructure limits an organization's vulnerability to security attacks by current or former employees and contractors.

The real benefits of federated identity management can be seen when communication takes place between and among various organizations. Below, we briefly discuss several situations that call for federated identity.

Government to Government

Many types of vital information must be shared across government and organizational boundaries. Interoperability is a requirement within agencies, among organizations and even between nations. Indeed, the dynamically changing nature of national coalitions calls for dynamic circles of trust (a group of organizations that have established trusted relationships with one another and have pertinent agreements in place regarding federations). A federated architecture now allows systems to interoperate while maintaining their autonomy. The circle of trust provides participating organizations the framework to ensure that this interoperability is trusted and secure.

The compelling need for sharing sensitive information, and thus for federated identity management, can be clearly seen in times of disaster. A regional incident, such as an earthquake or avalanche, brings together myriad organizations that must freely share disasterresponse information among all relevant agencies and governments, often spanning multiple countries. When information about victims, rescue and response actions, and law enforcement activities are at stake, it is vitally important to ensure that individuals are properly authenticated prior to exchanging such sensitive information.

Government information sharing is a requirement not only in times of crisis; in fact, it permeates all aspects of government. For example, the European Commission's eEurope (eEurope, n.d.) activity covers a number of initiatives, including e-government, e-health, e-learning, and e-business, all designed to foster the development of new and better services. Examples include initiatives related to the health sector in Spain and Finland, the management of relations between administrations and companies in Belgium, the indexing of public files in Italy, e-voting in some local consultations in France, and much more. In each, the need for interchange of information requires a federated identity management framework to enable free flow of information while preserving security and privacy.