Federated Identity Management
A Sevan White Paper

Federated Identity Management is a term widely used to refer to authentication and authorization of people or systems across independent organizations. The most commonly used example is that of an employee of one company accessing information belonging to and controlled by an independent, partner company. The two companies are "federated" in the sense that they allow specific employees of one company rights within the other company. Other examples can be found in consumer-merchant relationships, business outsourcing scenarios, and supply chain management. Federated relationships are becoming increasingly common.

Many commonly used identity management products have evolved from centralized, "closed" security models. These products assume that all users are under the control of a single authority. This model is awkward in federated environments. The Sevan WSA's identity management is designed to support federated organizations. This paper shows how Federated Identity Management is supported by today's WSA as well as the WSA's ability to support enhanced Federated Identity Management in the future.

Federated Identity Arrangements

There are many ways for federated organizations to interact. The most commonly mentioned are shown in Illustration 1 and Illustration 2 on page 2. In Illustration 1 the *user* is attempting to access resources in the *destination site*. The user has a trust relationship with the *source site*, which means that the source site can authenticate and authorize the user. The destination site has a trust relationship with the source site, but the destination site does not trust the user. This is a federated arrangement because the destination site authorizes the user based on the source site's authentication and authorization. In other words, the destination site relies on the source site to vouch for the user.

The user sends his request for the destination site resource to the source site. The source site authenticates the user, and if the user is authorized, the source site passes the request plus authorization information to the destination site.

This arrangement mimics the action of an employee making business travel arrangements through an external travel agency: the travel agency is the destination site, the employee is the user, and the employer is the source site. The employer has a contract (trust) with the travel agency. The employee has a trust relationship with the employer, but there is no relationship between the employee and the travel agency. The employee can book travel that is charged to the employer because the employer vouched for the employee. The authorization information might include the employee's department, spending limits, and airline class restriction.

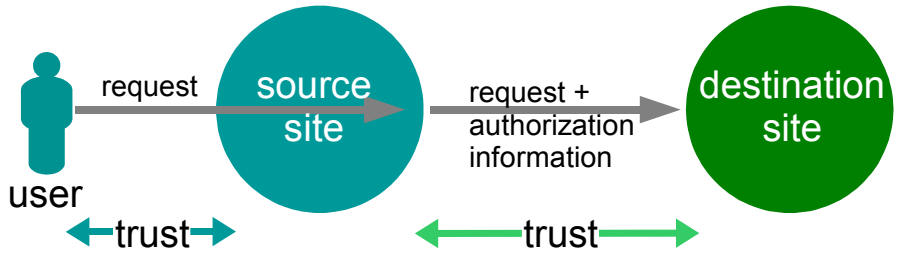

Illustration 1-- Federated access through the trusted site

Illustration 2 shows an alternate federation arrangement. As before trust is between the user and the source site. There is also trust between the source site and the destination site, but there is no trust between the user and the destination site. The difference between this and the previous example is that the user directly accesses the destination site. Before the destination site grants the user access, it must ask the source site to vouch for the user. This is suggested by the authentication and authorization arrow between the sites.

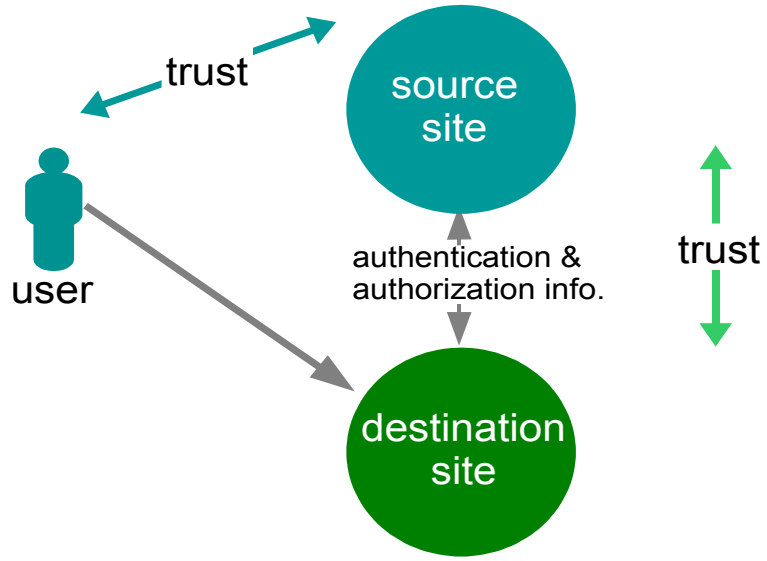

Illustration 2-- Federated direct access

WSA's Support of Federated Arrangements

This section shows how the WSA supports the common arrangements of federated identity management. Illustration 3 demonstrates how the WSA supports the federated arrangement shown in Illustration 1. There are two WSAs, one administered by the source site (e.g. employer) and one independently administered by destination site (e.g. travel agent). The user accesses the destination site though the source site's WSA. After the user is authenticated and authorized, the WSA at the source site forwards the request to the destination site.

In order to prevent unauthorized requests from arriving at the destination site, the WSAs establish an authenticated SSL session between them. The administrator at the destination site determines which parts of his site can be accessed through the source site's WSA. This allows the destination site to open up a portion of itself to users who are authenticated and authorized by the source site. The source site administrators determine which users are authorized to access the destination site. The destination site administrators unilaterally control which resources in the destination site are available to the source site users.

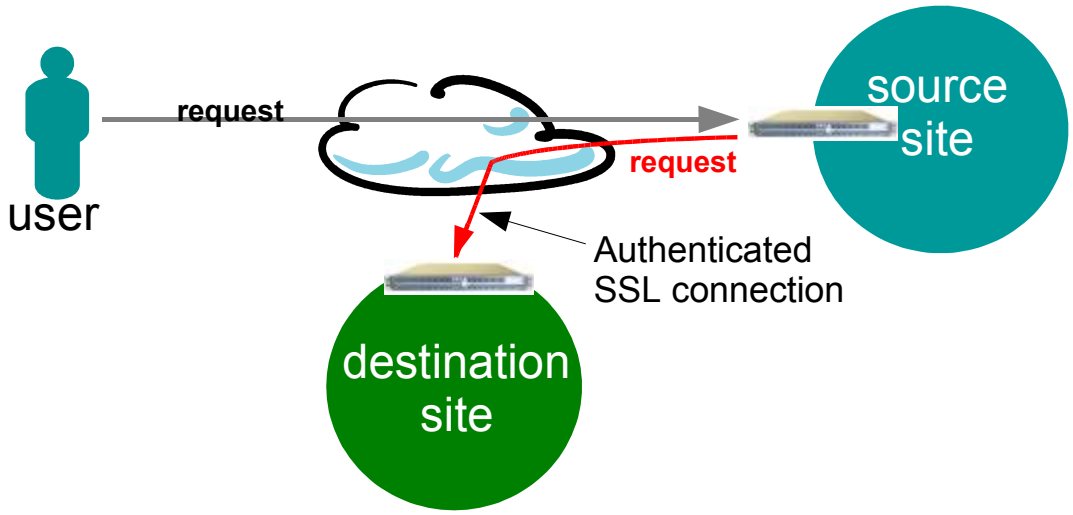

Illustration 3-- WSA Configuration

Illustration 3 is the simplest example. The WSA can support more complex federated arrangements such as:

- a source site may be associated with multiple destination sites
- a destination site may serve multiple source sites
- a site can serve the role as a source site and destination site.

It is also possible to implement the federated arrangement without the WSA at the destination site. Because there is no destination WSA, the destination site must implement alternative methods for controlling access to its federated resources, such as:

- Install a firewall at the destination site that allows requests only from the source site's WSA
- Configure the destination site web server to require basic authentication for the federated resources. The source site's WSA administrator must configure the WSA with the basic authentication name and password.
- Configure the web server to require SSL client authentication for the federated resources. The source site's WSA has the SSL certificate that allows access to the federated resources.

Illustration 4 shows how the WSA supports the federated arrangement of Illustration 2. Since the destination site trusts the source site, it can delegate the administration of a portion of itself to a source site administrator. This allows the source site administrator to independently determine the authentication and authorization of the users accessing resources that were delegated by the destination site.

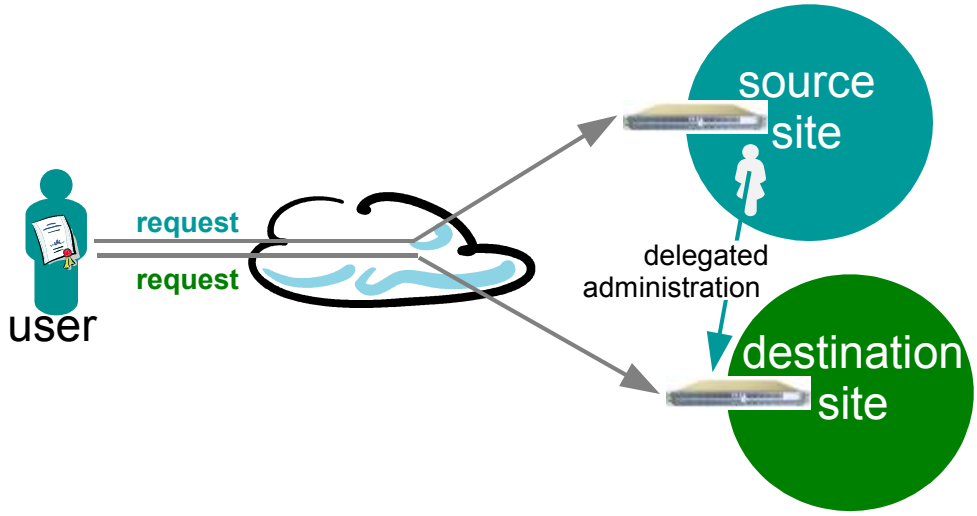

Illustration 4 -- WSA federated configuration

The destination site administrators can change which resources are available to the users. The source site administrators determine which users are allowed to access the resources. Notice that both sites authenticate the user through his SSL certificate. As such, the user has a common authentication credential for both sites.

Notice that the WSA uses a slightly different authorization paradigm than that suggested by Illustration 2. Rather than the destination site querying the source site for the user's authentication and authorization, the destination WSA maintains the authorization information locally. As a consequence, the destination site can operate independently of the source site: the user can access the destination site even when the source site is down.

In situations where the source site does not require access control, it is possible to forego the WSA at the source site. In this case the administrators from the source site determines who can access the federated resources at the destination site.

We've seen that the WSA supports the most common arrangements of federation. The rest of this paper discusses additional characteristics of the WSA that make it ideal for Federated Identity Management.

Federated Authentication Issues

User authentication is the foundation of Federated Identity Management. Each federated party must be able to authenticate users within its federation. When users are authenticated through passwords, federated user authentication is complicated by the fact that the source organization cannot simply share the user's password with destination organization. Rather, the destination organization must ask the source organization to authenticate the user on its behalf. The problem with passwords is that they are “secrets”; only the user should know his password. Anyone else knowing the user's password can masquerade as the user. If the source organization were to send a user's password to a destination organization, a dishonest administrator within the destination organization could compromise the user's identity.

The Sevan WSA does not use passwords, which allows it to share user authentication credentials. The WSA authenticates users through public key cryptography. Public key systems use two keys. One is “public” and is used by the authenticating party to verify that a user is indeed who he claims to be. The public key is a field in the user's certificate. The other key is “private” and is used by the user to prove his identity. The private key is known only by the user: it is never shared.

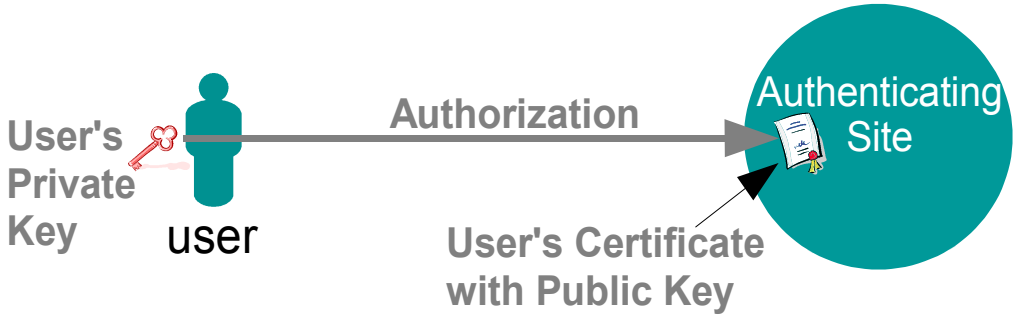

Illustration 5-- Authentication through public key cryptography

Any party needing to authenticate the user can do so if it has the user's certificate. Federated organizations can share authentication information by exchanging user certificates. The source organization (the organization with a trust relationship with the user) can readily share the user's certificate with any federated organization with complete confidence that the user's identity is safe. Once a federated organization is given the user's certificate, the federated organization can directly and independently authenticate the user. In this manner, certificates provide a common credential, which can be used by all organizations to authenticate the users.

There are some situations where a common credential might be considered a liability. The problem is that a common credential allows the authenticating parties to track the user's activities. Some people believe that this could result in a invasion of user privacy. In situations where a user wishes to maintain multiple identities, the user can have multiple certificates. Certificates can be used for different activities. For example one certificate can be used for work and a different certificate could be used for shopping on the Net. The WSA can be configured to accept one or multiple certificates from a user.

Identity Source Issues

As mentioned previously, most security products presuppose a centralized repository for user information. These “Authoritative Identity Sources” contain information such as user names, passwords, roles, and permissions. In federated organizations there is no single Authoritative Identity Source; typically each organization has its own. This means that each organization must augment his Authoritative Identity Source with users from federated organizations. Messaging technology has been proposed in an attempt to solve this problem, however the technology cannot solve the hard problems of cross-organization policy and trust.

The WSA natively supports federated organizations, because it does not rely on a pre-existing Authoritative Identity Source. The WSA allows an administrator to establish permissions for a user before the administrator knows the user's identity or authentication mechanisms. Before a user can actually use the permissions, he must go through a WSA enrollment procedure in which he authenticates himself (typically through an enrollment password) and binds his certificate to his identity. In this way, the WSA uses the enrollment process to generate, on demand, an Authoritative Identity Store, which includes only those users who require federated access.

In situations where a user is already in an Authoritative Identity Source, a WSA administrator can pre-enroll the user so the user need not go through an enrollment process. This allows the administrator to manage both classes of user: those within the Authoritative Identity Source and those who are not.

Standards Issues

Today many associate Federated Identity Management with the technology standards proposed to support it. Industry has unanimously agreed on web technology (HTTP, HTTPS, HTML, XML) as the basis of all federated interactions. The Sevan WSA is optimized for web access and identity management, which makes it ideally suited for federated organizations.

SAML (Security Assertion Markup Language) allows federated sites to share information concerning authentication, authorization, and user attributes. The WSA is designed for federated deployments and is SAML-ready. The addition of SAML will allow WSAs to exchange information among themselves as well as other SAML-enabled products. Sevan Networks plans to incorporate SAML technology into the WSA as soon as it will benefit our customers. The WSA's user authentication mechanism makes SAML especially efficient. Since each user is authenticated with a common, shareable credential, the WSA's SAML authentication assertions are far more efficient and more secure than those found in password-based products.

Conclusion

Businesses are becoming collections of federated organizations. The Sevan WSA is designed for federated environments, and it supports federated business today. Some of the features that make the WSA especially appropriate include: a common user authentication credential, flexible delegated administration, ability to control access to partner servers, and independence from Authoritative Identity Sources.

sevan networks

Sevan Networks, Inc
1310 Hollenbeck Ave, Ste F
Sunnyvale, CA 94087
Tel: 408.830.1000
Fax: 408.830.1001
www.sevannetworks.com