Resource-Centric Access Management
A Sevan White Paper

Most identity management systems are user-centric: administrators manage users. An administrator can directly entitle a user to access selected resources or the administrator can indirectly entitle the user by assigning him to groups or roles. The Sevan WSA employs a resource-centric model: administrators manage web resources. In this model, an administrator configures a resource to allow access by a specific set of users. The WSA's resource-centric model also supports user groups or roles.

User-Centric Access Management

In the user-centric model, the administrators start with a list of all users. An administrator selects a particular user and assigns him rights to access resources, or assigns him to a "role", which has predefined rights.

Illustration 1 shows a simple example of user-centric access management. In this example, "John Smith" is represented by a single row in the table. In this example, John Smith is allowed to access "page 1" (a specific resource) as well as all of the resources allowed by the "sales" role.

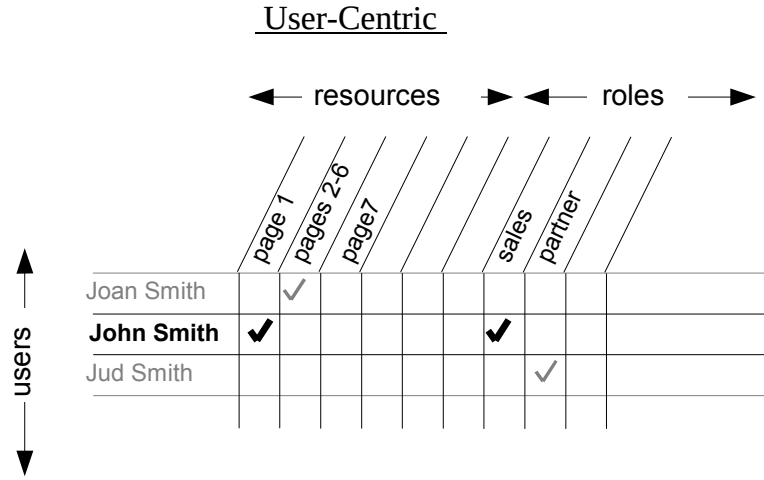

Illustration 1-- Typical user-centric access management

User-centric management requires that the organization maintains an "Authoritative Identity Source". This is a list of all users. It includes the identity (typically a unique name) and the means of authenticating the user (typically one or more passwords). The Authoritative Identity Source is usually held in a directory or a meta-directory.

As businesses become "extended enterprises", an Authoritative Identity Source become more illusive. Think about the problems of maintaining an Authoritative Identity Source for:

- employees of partners; e.g. distribution channels
- employees of companies that recently merged
- employees of customers; e.g. customers of an Application Service Provider, ASP.
- infrequent consumers

Today's common business practices conflict with the traditional concept of an Authoritative Identity Source. Consequently the extended enterprise is poorly served by user-centric management. The following questions are not easily resolved in extended enterprises:

- "Who is John Smith?";
- "Is your John Smith the same as my John Smith?";
- "What is the relationship between John Smith and J Smith?"; and
- "How do I authenticate John Smith?"

As business relationships become more open, the user-centric model becomes less appropriate. Mergers, acquisitions, partnerships, and the heightened demand for individual privacy make an Authoritative Identity Source more expensive and less dependable. The Sevan WSA uses a "resource-centric" model to conform to the realities of modern business.

Resource-Centric Access Management

In the resource-centric model, the administrator manages resources rather than users. The resource-centric model does not require an Authoritative Identity Source. As a consequence, the users of one resource are, in general, completely independent of the users of other resources. A resource administrator is aware of only those users who are able to use his resource. This means that the administrators of different resources can have different views of users and can even use different identifiers ("names") for the same user.

Illustration 2 shows an example of a resource-centric model. The administrator selects a resource (e.g. "pages 2-6") and assigns users to it. The users of "page 2-6" are independent of the users of the other resources. For example, the user "John Smith" may or may not be the same person as user "J Smith". Since they are using different resources it makes no difference whether or not they are the same person. Conversely, naming ambiguities in the user-centric model can result in the wrong user gaining access to a resource – a series security breach.

Since the naming of users is local to the resource, user names need not identify a specific person. For example, "ACME Partner" is an acceptable name for a user within the context of "page 1". This WSA feature gives the resource administrators a great deal of flexibility in naming and referring to users.

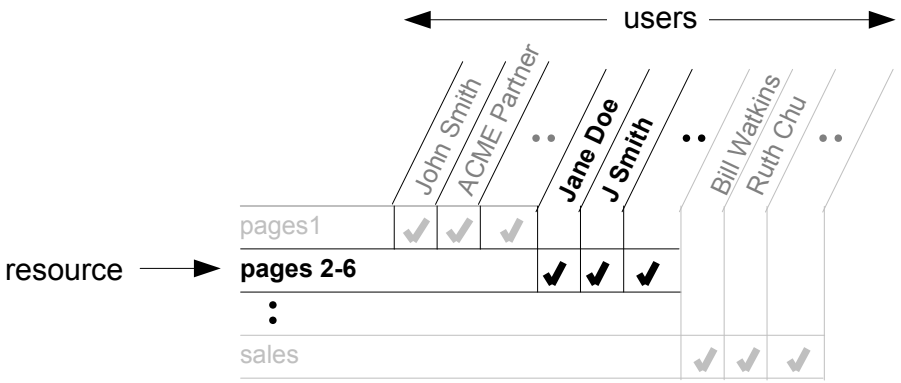

Illustration 2-- Example of Resource-Centric

Since the WSA does not depend on an Authoritative Identity Source, it does not have a predefined authentication mechanism (e.g. password) for new users. Each new user must establish his authentication mechanism before being allowed to access his resources. The WSA does this through an ***enrollment***

process. Since the WSA uses certificate-based authentication, a successful enrollment results in a binding between the user's certificate and his name[1]. Through the user enrollment process, the WSA essentially constructs an Authoritative Identity Source for each resource. The resulting Authoritative Identity Source is securely stored within the WSA.

In many situations a person might access multiple resources. In these cases, it is desirable to manage the person rather than a set of independent users. Fortunately, the WSA is capable of creating an Authoritative Identity Source that spans multiple resources. The WSA traces a person though multiple resources by searching for a common enrolled certificate. Consider the example shown in Illustration 3, which shows the enrollment of four users. There are three certificates, shown as red, green, and blue. Since "John Smith" and "J Smith" enrolled the same certificate, these users are actually one person. The WSA will show an administrator who can manage "page 1" and "pages 2-6" that "John Smith" and "J Smith" are the same person. This feature allows an administrator to quickly identify the resources for which a person has enrolled. This is useful when the administrator must manage a specific person (e.g. the person is leaves the company and is no longer permitted to access company resources).

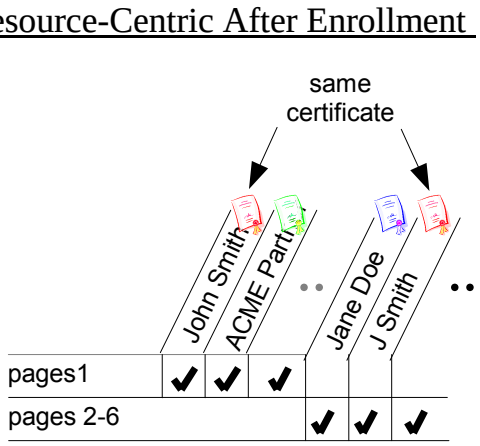

Illustration 3-- Resource-Centric after certificate enrollments

Role-Based Capabilities of Resource-Centric Access Management

It is common for a person to access to many resources. It is cumbersome to enroll in each resource. Fortunately, the Sevan WSA supports role-based access management, which allows a single enrollment to grant access to many resources.

Role-based management is built on a WSA feature that allows administrators to define a resource and *link* other resources to it. After a user enrolls in the first resource, he gains access to all of its linked resources. In this manner, a single enrollment provides the user access to the enrolled resource as well as all of its linked resources.

Illustration 4 on page 4 shows this capability. The top two resources (*employee* and *partner*) define user roles. *Employee* has *resource1* and *resource2* linked to it, as suggested by the quote marks in the table. A user enrolling in *employee* gains access to *resource1* and *resource2*. Similarly *partner* has *resources2* and

1 Those of you familiar with the "X.509" or "PKI" model will note that the binding between the certificate and user is achieved when the certificate is issued. This is equivalent to establishing an Authoritative Identity Source. The Sevan WSA does not presuppose a trusted binding between a certificate and a user, so it must establish the binding through the enrollment process.

resource3 linked to it. Users enrolled in *partner* are automatically given access to *resource2* and *resource3*. Note that a linked resource can also have its own set of users, which is suggested by the user "Alice Bob" in *resource1*.This user can access only those resources in *resource1*.

An administrator can modify the resources available to a role by adding or removing linked resources. This does not require the users to reenroll. When a user changes roles, the administrator simply removes him from his current role. The administrator invites the user to enroll in his new role, or the administrator can perform the enrollment on the user's behalf.

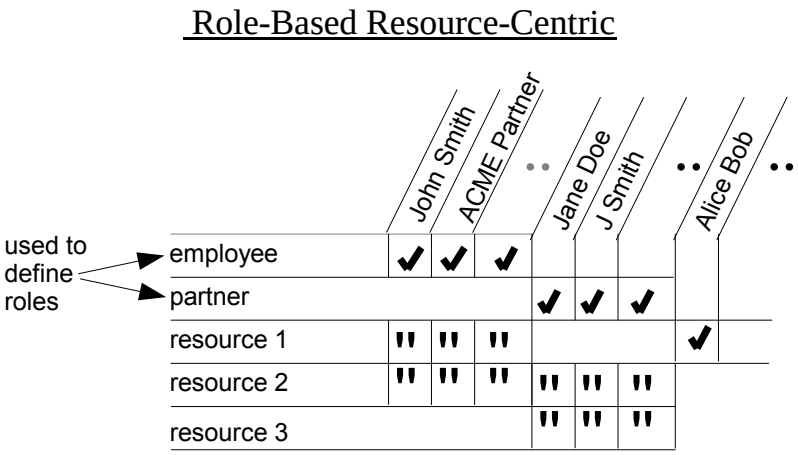

Illustration 4-- Role-based access management

Conclusion

The Sevan WSA's resource-centric model is designed for situations where an "Authoritative Identity Source" is difficult, expensive, or unreliable. As business becomes increasingly decentralized it is less likely that an Authoritative Identity Source exists. With the resource-centric model, the resource administrators have independent control of users and need not rely on a common identity source.

In situations where an Authoritative Identity Source is available for some or all of the users, the WSA's resource-centric access management is an attractive alternative to user-centric schemes. Anything that can be done though a user-centric model can be achieved through a resource-centric model. A WSA administrator can pre-enroll users who are included in an Authoritative Identity Source (these users need not enroll), while requiring users who are outside the Authoritative Identity Source to enroll.

The Sevan WSA's identity model supports the realities of your business. Our resource-centric approach is optimized for situations where user identities are as diversified as your business.

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