Identity Authentication
A Sevan White Paper

Businesses are increasingly turning to Web technology to distribute sensitive or valuable information. Corporations are basing more of their enterprise systems on the web by allowing employees, customers, and partners access to mission-critical information. Merchants and service providers are also using the Web to reach consumers of services, information or entertainment.

These high-valued Web-based services are underpinned by the concept of a *subscription*: the consumer of the information or service has a subscription relationship with the provider of the service. The subscription has a set of implicit and explicit rules concerning the use of the service and the compensation for the service. These subscription rules are manifested in many ways. Examples include:

- employment agreements,
- user license agreements, and
- consumer subscription agreements.

Any Web-based delivery of subscription services must enforce the subscription rules to protect the value of the service or information.

Subscriber Authentication

By adding Sevan's Identity Authentication to a web site hosting subscription services, the site will allow only subscribers to access a subscription service. Identity Authentication is a multistep process with the following components:

1. Positive identification (also known as *authentication*) of the user attempting to access the subscription service
2. If the user is a legitimate subscriber, he gains access to the service. The subscriber's use of the service is recorded for audit and billing purposes.
3. If the user is not a recognized subscriber, the provider can invite the user to enroll for the service. The success of the enrollment depends on the user's ability to satisfy the service's subscription rules. Hence, some enrollments will succeed and others fail.

Identity Authentication identifies each subscriber through the use of the technology shipped with every browser. Therefore, Identity Authentication requires no additional client software. This is an important feature, since the cost of installing and maintaining client software is prohibitive for many businesses. Each subscriber is identified though a unique Digital Certificate. This Certificate is stored in browser or stored in a smart card or smart token (more on these later). When the user attempts to access the subscription service, the web site performs the following:

1. reads the SSL Certificate from the browser,
2. challenges the browser to make sure that the Certificate truly belongs to this user (more on this later),
3. determines if the owner of the Certificate is a legitimate subscriber.

This is automatically performed by the browser and usually requires no user intervention: Identity Authentication is transparent to the subscriber.

How does a user become an subscriber? If the user already has a Sevan Certificate or any other SSL Digital Certificate, the web site will simply ask the user to enroll as a subscriber. The enrollment process can take one of two forms, depending on the requirements of the subscription service:

1. Enrollment through an account name and password, which the services' administrator gave to the user. If the user has a valid account and password, the user is immediately enrolled as a subscriber.
2. Enrollment through an application, which the user fills out and submits to the web site. After

the application is reviewed and approved, the user is enrolled as a subscriber. Note the application enrollment is not incorporated in the current release of the WSA.

It is important to remember, that once the subscriber is enrolled, all subsequent accesses to the subscription services are transparently authorized through Identity Authentication. The enrollment is generally a one-time event.

We noted that user must have a SSL Digital Certificate in order to enroll. In the event the user has neither, the user can obtain a Certificate directly from the web site. The user is simply asked for her name, and her browser receives a certificate with three mouse clicks. After receiving the Certificate, the user can continue with enrollment.

A single Certificate is sufficient for most users. The user can enroll this Certificate in multiple subscription services, which can be offered by different service providers. For example, a single Certificate can be used to access your employer's subscription service(s), on-line banking services, on-line merchants, or any other on-line service. Because of the technology underlying Identity Services, the subscriber can widely use a single Certificate knowing that her identity is secure.

Users with multiple computers (e.g. a laptop and desktop or a work and a home machine) can obtain a unique Certificate for each computer and enroll the computers into common or separate subscription services, if so allowed by the service's administrator. This allows a subscriber to access a service from multiple computers or to make sure that a service can be accessed from only a specific computer.

In a similar fashion, an advanced user might wish to load multiple Certificates on a computer. When this user attempts to access a subscription service, the browser will ask her to select one of her Certificates. This feature allows users to chose and manage their identities, Those users who are sensitive to privacy issues, can use multiple Certificates to protect their privacy.

Smart Cards and Tokens

Sophisticated users might chose to hold their Certificates on small, portable devices that are independent of their computer. A smart card is the size of a credit card. When the subscriber wishes to use her Certificate, she inserts the card into a reader that is attached to her computer. The browser users the Certificate on the smart card to authenticate the subscriber to the subscription services. A smart token is equivalent to a smart card. The smart token is about the size of a house key and is inserted into the computer's USB port. Both smart cards and tokens provide three valuable features. First, the Certificate is portable, so it can follow the user to any computer. Second, the user can remove the Certificate to make sure that no one else can use it. Lastly, the smart card or token is generally protected by a PIN (Personal Identification Number), similar to those protecting ATM cards. The PIN protects the Certificate in the event that the smart card or token is stolen. The thief cannot use the Certificate without the PIN.

Securing Certificates Stored In Browsers

Most subscribers will store their Certificates in the browser. This is the most convenient and inexpensive option. Furthermore, by storing the Certificate in the browser, the user avoids the problem with lost smart cards or tokens. However, this means that the browser contains the information necessary to identify you as a subscriber. If a thief should gain access to the Certificate on your computer then the thief becomes you.

Fortunately, all standard computers and browsers have build-in mechanisms to protect the Certificates. Browsers have an option to protect the Certificates with a PIN (much like the smart cards). Therefore, a thief must know your PIN in order to use your Certificate. Another level of protection is found in the operating system itself. Most computers allow the user to protect the computer with a password. Therefore a thief with your computer can't even start the browser without knowing your password.

Certificates and Public Key Cryptography

In an effort to keep the explanation simple, we have taken a few liberties with the role of the Certificate.

The actual authentication of the subscriber is not really done with the Certificate. If we used the Certificate like a password, then anyone knowing your Certificate can steal your identity. Fortunately, the browsers are more sophisticated than that. The Certificate contains the value of the subscriber's *public key*. This key is a few hundred digits long and has absolutely no meaning to the subscriber or service provider. The service provider uses the subscriber's public key to test if the subscriber's browser has the corresponding *secret key.* The subscriber's public and secret keys have a special mathematical relationship, which allows the service provider to perform this test without knowing the actual value of the subscriber's secret key. With this explanation in mind, we now know that the "key" to the subscriber's identity is the value of the subscriber's secret key. If a thief should discover the secret key, the thief could masquerade as the subscriber.

sevan networks

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