Customer Authentication for Small/Medium Banks

a Sevan White Paper

sevan networks

Small and medium-sized banks successfully compete with large banks by providing a more personalized banking experience. Smaller banks are constantly looking for ways to enhance their offering. Incorporating a Sevan WSA into an on-line banking solution will make the banking experience more personal, increase customer satisfaction, and greatly improve customer retention.

Issue: Passwords

Customer authentication is the foundation of an on-line banking service. The bank must take all reasonable means to prevent unauthorized access to customer information or funds. Today, customer passwords are the way of proving on-line identity.

Passwords raise the following issues:

- customers must keep the password secret
- customers must provide the password to access their services
- customers who forget their passwords lose their banking services

The bottom line is that passwords are an impediment to customers doing business with the bank. Passwords are the antithesis of personalized banking.

Imagine an on-line banking service that is so personalized to the user, it no longer requires passwords. This is the promise of the Sevan WSA. A customer sits down at his computer at home, accesses his on-line services and is authenticated automatically. The customer's computer is an extension of his banking experience: his personal teller.

Solution: Sevan WSA

The Sevan WSA provides the user authentication and access control for the on-line banking services. The Sevan WSA authenticates users with public key cryptography, also known as certificate-base authentication. Financial institutions have been using certificate-based authentication for over a decade. This technology is well studied and standardized in the banking community through ANSI working groups. Financial institutions have invested tens of millions of dollars in public-key products and infrastructures. Sevan has solved the problems of cost and complexity to make certificate-based authentication available to the general banking customer.

How does it work? Suppose a customer sits down at his computer to access his account. The Sevan WSA, which is located at the bank's server, builds an secure connection (using Secure Sockets Layer, SSL) to the customer's computer, during which the customer's browser is asked to produce the customer's certificate. The Sevan WSA uses the certificate to authenticate the customer. If the WSA determines that the customer has the right to access the account, the WSA will allow access. The WSA blocks unauthorized access attempts. During typical operation, the customer is not aware that he has been authenticated. It happens automatically and transparently.

What is a certificate?

A digital or SSL certificate is defined in the X.509 and ANSI standards. It is a digital message of a few thousand bytes. It is cryptographically protected so it cannot be altered or forged.

The certificate contains a dozen different pieces of information. The most important is the value of the customer's cryptographic *public* key. The Sevan WSA uses the cryptographic functions defined in the SSL standard to verify that the customer possesses the corresponding *private* key. In this manner, the customer and only the customer can successfully use the certificate.

What happens the very first time? If this is the first time the customer access his on-line account, the WSA does not know that the customer's certificate allows him to access his account. Therefore, the WSA asks the customer to *enroll* his certificate into the account. This requires the customer to type in his account number and password, which he has received from the bank. If the account and password is valid, the WSA remembers the certificate and will use the certificate to authenticate the customer in the future – no more passwords. Notice that the enrollment process is no more difficult than today's authentication using names and passwords.

Certificate Enrollment & Trust

The Sevan WSA uses a trust model that was developed by the banking community. This is generally known as "account authority". Our trust model reflects the business practices and legal frameworks employed by financial institutions.

The initial trust between the customer and the bank is represented by the name and password. When the customer enrolls his certificate, he transfers the trust from the password to the certificate. In this manner we use passwords to initiate trust and certificates to maintain trust.

What happens if the customer does not have a certificate? The Sevan WSA demands that the customer has a certificate. We offer three ways for a customer to obtain a certificate: the bank can mail a certificate, customer can go to a web site to get a certificate, or the WSA can provide a certificate during the customer's first visit. Notice that a customer must obtain a certificate only once.

Can some applications still require passwords? Absolutely. The customer can be authenticated through his certificate and sensitive transactions can be further protected by passwords. It's up to the bank.

What happens if a thief gains access to the customer's computer? Since the certificate is stored on the computer, it is important to protect it against unauthorized access. Fortunately there are many ways of doing so: password lock on the operating system, PIN lock on the certificate, or passwords in the critical applications. Chances are the customer already has sensitive information on this computer (financial planning or accounting software), which require that his computer be protected by his Windows or Mac password.

Can a thief steal the customer's certificate and load it on another computer? Stealing the certificate does not help the thief. The thief must also steal the customer's private cryptographic key. Certificates that are provided by the Sevan WSA are "non-exportable", so a thief cannot use standard tools to copy the certificate and key. We know of no hacking tools that allow a thief to copy the certificate and key. They are secure as can be in a Windows or Mac operating system.

What about a customer accessing his account from multiple computers. The Sevan WSA allows multiple computers to be enrolled in a single account. We also allow a single computer to be enrolled in multiple accounts.

Can a customer access his account from a computer that does not have his certificate? If the bank administrator allows it, the customer can access his account with a name and password of his choosing.

What about a customer who shares his computer with co-workers or family members? Chances are such a customer is using an operating system that supports multiple users. The customer must log onto his user account (which requires a user name and password) in order to use his certificate. In this manner, each user can have his own certificate, which is not available to other users of the computer.

What happens when a customer loses his certificate? The certificate is lost when the customer deletes it or when the computer's disk drive fails. In either case, the customer must get a new certificate and enroll the new certificate into his account.

What happens if a customer replaces his computer? The customer must obtain a new certificate for his new computer and enroll it. The customer should also disable his old certificate. He can remove the certificate from his old computer, or he can use the Sevan WSA's “self-service” feature to disable the certificate on the Sevan WSA.

Where do I install a WSA? The WSA is an appliance that is typically installed between the firewall and the web server or servers. The WSA is usually up and running in less than an hour. The WSA requires no changes to the network, servers, or applications.

If the WSA does the authentication, how does the banking application identify the customer? The WSA can be configured to pass the customer's account number or any other customer-specific information to the application after the customer is authenticated. Your banking application is accessed by only authenticated customers. Hackers can't get close to the application.

Can I control which applications are available to the customer? Absolutely. The WSA has the ability to partition your on-line web site so the bank administrator can control which web pages or applications each customer can access.

Can a WSA be shared among multiple banks? If you are hosting a web site that is serving multiple banks, one WSA can independently support each bank. The WSA strongly partitions the web site, so each bank can securely manage its customers without affecting the other banks.

Can the Sevan WSA authenticate bank employees? Absolutely. The bank administrator can set up portions of the web site for customers and portions for employees. After an employee enrolls his certificate, he has access to only those resources required by his job. If the WSA is shared by multiple banks, the employees of one bank cannot access (or even see) the resources of another bank. Each bank administrator can securely and independently control the access of his employees.

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