



Securing Online Web Services

Modern browsers allow organizations to expand their business model securely to include online commerce and security-related services. Organizations can now rely on the existing browser security infrastructure to provide both authentication and digital signature functionality, without the need to install additional dedicated software clients.

By implementing strong user authentication and access control systems, organizations can ensure that only authorized users access their online information. Practical examples of secure web services include:

- Online banking
- eCommerce
- Online access to medical records and information
- Remote access to network resources

- Online student registration
- Database access
- Business-to-business portals
- Customized reseller websites
- Stock trading

Features

eToken	Online Web Services
● eToken R2 - DESX 120-bit	● SSL v3 PKI
● eToken PRO - RSA 1024 / 3-DES / SHA-1	● Active-X control (symmetric key eToken module)
● Secure Storage of Private Credentials	● Secure web logon
● On-board Cryptographic Processing	● LDAP connectivity
● Strong Authentication & Non-Repudiation Support	● Server/client two-way authentication
● Standard USB Connectivity	● PKI challenge-response
● Standard Connectivity to Multiple Business Applications (CAPI, PKCS#11)	● Digital signatures
	● PKI server support

Benefits

- Highly complementary integration between eToken and online web services.
- Powerful DES-X 120-bit encrypted challenge-response authentication, with eToken Active-X control.
- Maximum security and interoperability for PKI transactions, using SSL v3.
- Two-factor authentication for stronger user authentication security.
- Enhanced Web site access security, protection and authentication assures peace of mind.
- Maximum security for electronic transactions, such as online shopping or banking.

E-BUSINESS SOLUTIONS
ONLINE WEB SERVICES

eToken Ensures Two-way Authentication

Server Authentication

Verifies that the website you are accessing is who and what it purports to be. For example, when giving your credit card details to an online shopping service, you need to be sure that the operators of the site will supply the goods that you are ordering and will not use your credit card details for fraudulent purposes.

User Authentication

Controls who has access to which website and to what data. For example, as an online bank customer, you are allowed access only to your own account data, and not to other customers' accounts. No other customer, web surfer or hacker should be able to enter your account site and access your confidential data.

eToken Web Security Solutions

Secure Sockets Layer (SSL)

SSL Transactions are conducted through a private session between client and server, using the Secure Sockets Layer (SSL) v3 protocol. SSL is built into all major browsers and web servers. After SSL server certificate installation, administrators can then specify server access by certificates and/or users. A client may request and install an SSL browser certificate, granting authentication and the establishment of secure SSL sessions.

eToken utilizes two-factor authentication. For authorized access to the Web site specified in the SSL certificate stored on the eToken, the user must both connect the eToken and enter its individual eToken password. This ensures strong protection for user credentials. Browsers such as Internet Explorer and Netscape can be easily configured to store a user's SSL browser certificate directly on an eToken. Both the eToken R2 and the eToken PRO are compatible with SSL v3. Digital signatures use the private key on the eToken to guarantee non-repudiation.

Active-X

Web browsers incorporating an Active-X control can implement a secure challenge-response mechanism. Incorporating an Active-X control into a server is a relatively simple way to implement predefined functionality with a minimum of programming. The eToken Web Access Control Active-X allows developers to add strong 120-bit DESX challenge-response authentication to their applications. Specifically, applications can:

- Request and validate the user's eToken
- Validate the personalized eToken password
- Store an authentication secret on the user's eToken
- Use the stored secret with a received challenge and the DESX encryption algorithm to produce a secure response for authentication by the server

For more information about eToken, visit: www.eAladdin.com/eToken

International T: +972 3-6362222, F: +972 3-5375796, etoken@eAladdin.com **North America**: T: 1 800-562-2543, 1 847-808-0300, F: 1 847-808-0313, etoken.us@eAladdin.com **UK** T: +44 1753-622-266, F: +44 1753-622-262, etoken.uk@eAladdin.com
Germany T: +49 89-89-4221-0, F: +49 89-89-4221-40, etoken.de@eAladdin.com **Benelux** T: +31 30-688-0800 F: +31 30-688-0700, etoken.nl@eAladdin.com **France** T: +33 1 41 37 70 30, F: +33 1 41 37 70 39, etoken.fr@eAladdin.com **Israel** T: +972 3-6362313, F: +972 3-6362318, etoken.il@eAladdin.com **Brazil** T: +55 21-235-2499, F: +55 21-236-0768, etoken.br@eAladdin.com
Japan T: +81 426-607-191, F: +81 426-607-194, etoken.jp@eAladdin.com **Russia** T: +7 095-923-0588 F: +7 095-928-6781, etoken.ru@aladdin.com **Spain** T: +34 91-375-99-00 F: +34 91-754-26-71, etoken.es@eAladdin.com



www.eAladdin.com

ALADDIN
Securing the Global Village



0 0 8 7 1