

# eToken™

YOUR KEY TO eSECURITY

Digital  
Signature  
Trust Co.

## for Digital Signature Trust (DST)

Digital Signature Trust (DST), Inc. provides organizations with fully integrated Public Key Infrastructure (PKI) managed services designed to secure Intranet, Extranet, Virtual Private Network (VPN), and eCommerce applications. DST solutions can enable a number of security services, including strong authentication and non-repudiation of transactions.

eToken enables users of Digital Signature Trust's PKI systems to generate and store private keys and digital certificates inside the token, creating a secure environment and allowing full portability and maximum ease of use. eToken PRO can also perform sensitive on-chip encryption operations, ensuring that users' keys are never exposed to the PC environment. eToken eliminates the need to store certificates and keys on a hard disk or browser file, or to transmit them across the Internet/Extranet, assuring peace of mind and confidence during online communications.



E-BUSINESS SOLUTIONS  
PORTABLE PKI

### Features

#### eToken

- eToken R2 - DESX 120-bit
- eToken PRO - RSA 1024 / 3-DES / SHA-1
- Secure Storage of Private Credentials
- On-Board Cryptographic Processing
- Strong Authentication & Non-Repudiation Support
- Standard USB Connectivity
- Standard Connectivity to Multiple Business Applications (CAPI, PKCS#11)

#### DST Services

- Certification Authority Services
- Repository Services
- Customized Services
- X.509 v3 Certificate Support
- 1024-bit RSA Key Support
- Multiple Client Application Support

### Benefits

- High-level security for users' private credentials & digital certificates. Users can authenticate, encrypt, sign and decrypt electronic transactions with full confidence.
- Two-factor authentication is enabled for a variety of eCommerce and banking applications, ensuring a high level of security through reliance on a hardware based USB device.
- DST's keys & certificates can be securely created and stored on the eToken, operating transparently with any standard browser or eMail client.

## PKI, Digital Signatures & Certificates

In today's world of electronic business transactions, organizations need a method to authenticate the identity and validity of users accessing information on computer networks. A public key infrastructure (PKI) is a system that provides solutions for secure eCommerce and network services.

A PKI consists of protocols, services, and standards supporting applications of public key cryptography. In a PKI, every user is assigned a cryptographic key pair consisting of a public key and private key that are mathematically related. The public key is published, while the private key is kept secret.

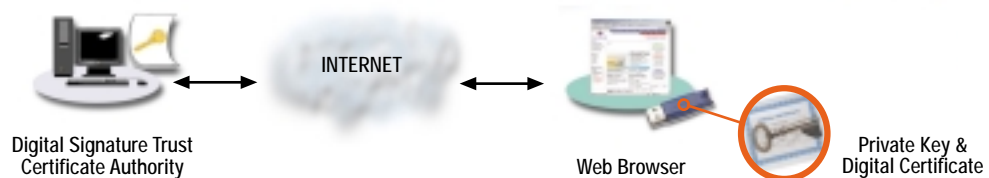
### Digital Signatures

A **digital signature** is created using the private key of an individual to ensure the validity of his request. This technology can be used to guarantee non-repudiation of various transactions. The strength of either the authentication level or the digital signature relies on the level of protection offered to the private key. eToken PRO offers the maximum level of security, since it enables the use of the private key for signing and authenticating, inside the eToken.

### Digital Certificates

**Digital certificates** are electronic credentials that tie a public key to an individual, and help prevent someone from using a phony public key to impersonate someone else. A basic certificate will contain a public key and an individual's name. Common certificates also include an expiration date, the name of the Certificate Authority (CA) that issued the certificate, and a serial number. Most importantly, it contains the digital signature of the CA.

The most secure use of authentication involves enclosing at least one certificate with every signed message. The message recipient verifies the certificate using the CA's public key. If the sender's public key is legitimate, the recipient verifies the message's signature. Digital signatures created with a private key are verified with the digital certificate containing the public key.



## eToken Enterprise & DST Certificates

The eToken Runtime Environment (RTE) contains all the necessary files and components needed for eToken to work with a computer. With eToken, users do not need to remember different passwords for different user accounts and certificates, only the password for their personal eToken. All authorization details can be carried on a key chain or in a pocket, and used securely on any computer set up for use with eToken.

For more information on eToken, visit: [www.eAladdin.com/eToken](http://www.eAladdin.com/eToken)

For more information on Digital Signature Trust, visit: [www.digsigtrust.com](http://www.digsigtrust.com)

**Aladdin**<sup>®</sup>  
SECURING THE GLOBAL VILLAGE

**Microsoft**  
Security Partner

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

