



Introducing eToken


eToken™

YOUR KEY TO eSECURITY




Nirit Bear
September
2002

eToken
FROM KEY TO eSECURITY



What is eToken?

- Small & portable reader-less Smartcard
- Standard USB connectivity
- Logical and physical protection
- Tamper evident (vs. tamper proof)
- Water resistant container



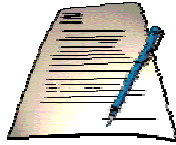
Smartcard
Chip inside

eToken
FROM KEY TO eSECURITY



eToken Is Used For:

- Strong 2-factor user authentication
- Digital signing (non repudiation) of business transactions
- Secure storage of PKI private keys, digital certificates, passwords, files etc.
- Single Sign-On applications



What Can eToken Do ?

- Secure eBusiness Services
- Secure Network Logon
- Secure VPN authentication
- Portable PKI authentication & signing device
- Secured email (Encrypt & Sign)
- Secure online Extranet & Website access
- PC Security





eToken Enterprise

- **Generic application support**
 - Win2000/XP SC logon, win logon (GINA), aladdin SSO
 - Check point VPN-1 client (SAA, NG)
 - Various CA's certificates
 - SSL v3
 - Secure email – MS outlook, Netscape messenger
- **eToken administrative Utilities**
 - Application viewer – application level view of the token content
 - Certificate converter
 - eToken format
- **Token management system (TMS) –**
 - Token profile
 - User profile
 - Supported applications

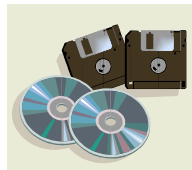


5



eToken SDK

- The eToken Software Developer's kit is mainly intended for use by developers.
- The SDK contains everything a developer needs to evaluate and use eToken, and develop his own eToken application.
- The SDK includes a number of programming interfaces, utilities, tools, sample applications and documentation files.



6



Multiple Applications Support in one eToken

Multiple Access Profiles On One eToken

- MS2K PKI Keys & Certificates
- NT Domain Access Profile
- SSL v3 PKI Keys & Certificates
- VPN authentication PKI certificates
- CheckPoint SAA Access Profiles
- MS Exchange PKI Keys & Certificates



Remember !!!
Only one password needed for all profiles



eToken Hardware

eToken™

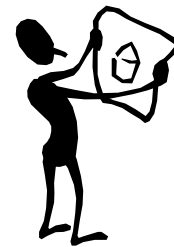
YOUR KEY TO eSECURITY



Nirit Bear
August 2002

Major Points -

- A USB key with a small chip...
- With on-board memory...
- Designed in a secure way...



eToken
FROM KEY TO SECURITY

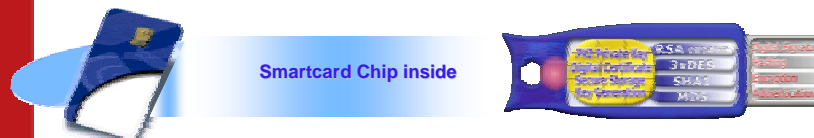
Aladdin
SECURED THROUGHOUT YOUR LIFE

9

eToken Device Options

eToken PRO

- Advanced Smartcard Technology



eToken R2

- Secure EEPROM



eToken
FROM KEY TO SECURITY

Aladdin
SECURED THROUGHOUT YOUR LIFE

10



eToken R2 - Hardware

- Micro controller based
- External EEPROM memory
- 8, 16 & 32 KB memory models. 64K in the future.
- Protected chip serial ID (32-bit length).
- Access via smartcard APDU commands



11



eToken R2 – Cryptographic Features

- Secure & encrypted EEPROM for PKI keys, certificates, profiles and passwords
- On-board 120-bit DES-X encryption/decryption
- Compatible implementation with Smartcards
- Variable key length - 2048
- Strong 2-factor authentication.
- Security API's- CAPI, PKCS#11.



12

What makes eToken R2 Secure

- EEPROM is readable by standard devices **But:**
 - All private data is written to the EEPROM encrypted by the DesX Engine
 - Encrypted Communications with the PC
 - eToken password is transmitted using a challenge-response protocol
 - DESX Engine is used as a tool for pseudo-randomness and MAC's
- Tamper - evident design
- Designed and reviewed by Cryptography experts

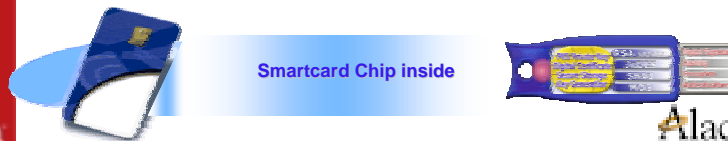
eToken
FROM KEY TO ACCESS

Aladdin
SECURED BY THE GLOBAL VILLAGE

13

eToken PRO - Hardware

- Infineon smartcard chip - SLE66CX
- Siemens CardOS 4
- 16 & 32 KB memory models (storage). 64K in the future.
- Protected chip serial ID (32-bit length)



eToken
FROM KEY TO ACCESS

Aladdin
SECURED BY THE GLOBAL VILLAGE

14



eToken PRO – Cryptographic Features

- On-chip crypto processing of RSA1024bit, 3xDES,SHA-1.
- Secure on-board PKI key generation and storage.
- PKI certificates storage.
- 2-factor authentication and digital signatures.
- Cryptographic API's - CAPI, PKCS#11.



15




What makes eToken PRO secure ?

- Security of CardOS/M4 – ITSEC E4 Certified
- Tamper - Evident mechanisms
- Physical security – data is physically distributed in a way that it is hard to locate
- Logical Security – data is encrypted on the memory chip
- Encrypted communications with the PC




16



eToken OS

- Software that uses the eToken hardware to provide:
 - A Smartcard file system
 - Access to cryptographic capabilities
 - Access to administrative capabilities
- eToken PRO
 - OS on-token
CardOS/M4 by Siemens
- eToken R2
 - OS included in software

Aladdin
17



eToken PRO CardOS/M4 Features

General Features:

- Runs on Infineon SLE 66 chip family. (True RNG, asymmetric cryptography, ITSEC E4)
- All commands compliant with ISO 7816 standards
- PC/SC compliancy and CT-API
- Extendibility of the OS using loadable software components
- All functions can be parameterized.
- Secure messaging – Encrypting data between host and card using predefined symmetric keys.

Aladdin
18



eToken PRO CardOS/M4 Features

File System:

Flexible file system, protected by chip cryptographic mechanisms:

- Arbitrary number of files
- File system tree supporting 8 levels
- Protection against EEPROM defects and power failure

eToken
FROM KEY TO SECURITY

Aladdin
SECURITY TECHNOLOGIES

19



eToken PRO CardOS/M4 Features

Access control:

- 32 distinct programmer definable access rights
- Every command and data object can be protected by unique access condition scheme.
- Security tests and keys are stored as key-objects in DF bodies
- Security structure can be refined incrementally after file/object creation without data loss.
- Formatting and personalization are enabled

eToken
FROM KEY TO SECURITY

Aladdin
SECURITY TECHNOLOGIES

20



eToken PRO CardOS/M4 Features

Cryptographic services:

- Implemented algorithms: RSA 1024 bit, SHA-1, Triple-DES, DES, MAC.
- Support of command chaining.
- Asymmetric key generation "on chip", using the onboard Random Numbers Generator
- Digital signature functions "on chip"
- Connectivity to external Public key certification services



21



On-Token Algorithm Processing

- Processing is performed on-token



- Protected keys cannot be accessed by Viruses/Malicious code
- Enables true 2-factor authentication



22



Additional Security Mechanisms

- Time-Delay mechanism after wrong password entry – eToken R2.
- Password Retry counter – eToken PRO
- eToken Password
 - Minimum length 4 bytes
 - No maximum length limit
 - Password quality check
- Access to sensitive data on memory and functions executed on the eToken require password based authentication to the eToken.



23



eToken PKI Client (the Run Time Environment)

eToken™
YOUR KEY TO eSECURITY



Nirit Bear
January 2002



What is the PKI client?

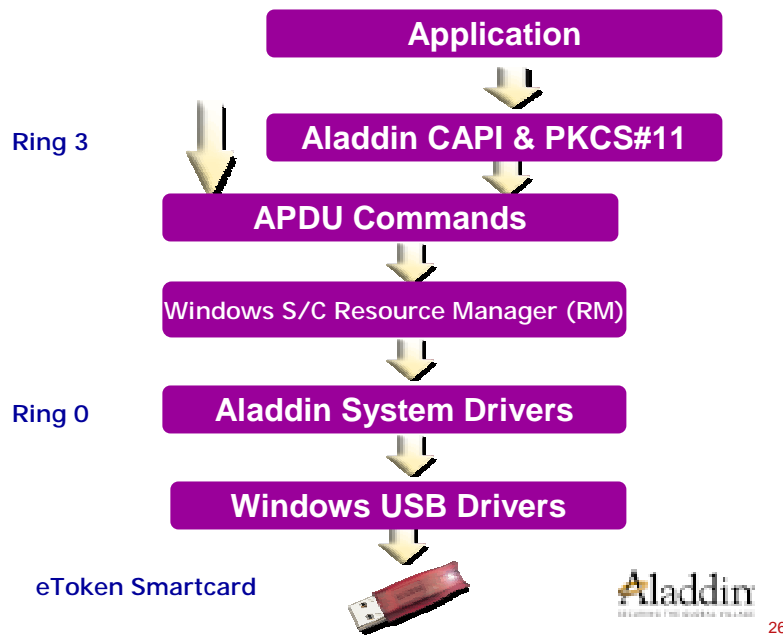
- Software layer for enabling eTokens on a host, including eToken drivers and the cryptographic libraries.
- Minimal end-user eToken management tools.
- eToken **PKI Client** Enables any Windows OS to access the eToken.
- Standard interface provides similar functional behavior of the two tokens



25

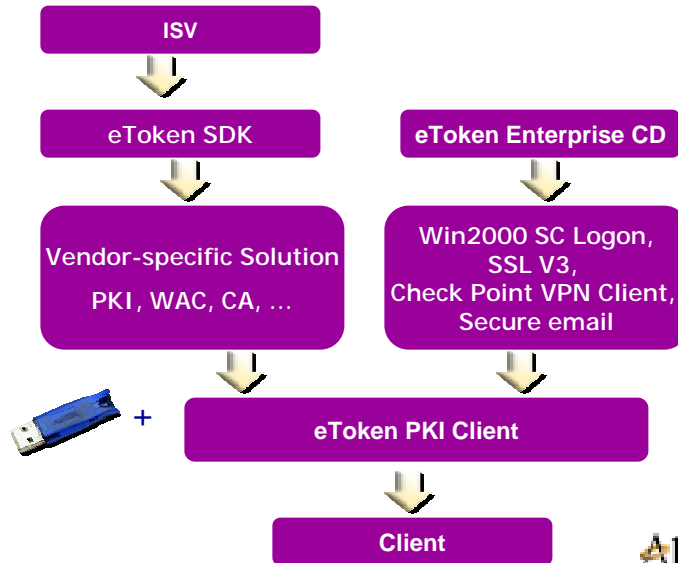


Low-Level Software Layers



26

High-Level Software Layers



27

Standards

The goal:

- obtaining interoperability of several manufacturers in the same environment.
- Portability.

The Solution:

eToken had been developed to support Industry open standards: USB, PC/SC, APDU, CAPI, PKCS#11.

eToken
FROM KEY TO ACCESS

Aladdin
SECURED THROUGHOUT YOUR LIFE

28



Hardware Standards in use by eToken

- **Universal Serial Bus** – A universal standard for bus system and port communication.
- **ISO 7816** part 3,4 – specifies logical requirement for a smartcard device (file system, etc.)



29



Open Standards in use by eToken

- **PC/SC** – The industry standard for smartcards in a PC environment.
- **APDU** - **A**pplication **P**rotocol **D**ata **U**nits
- **CAPI** – **M**icrosoft **C**ryptographic **A**pplication **P**rogramming **I**nterface.
- **PKCS#11** – **P**ublic **K**ey **C**ryptographic **S**tandard **#11** (Cryptoki)



30

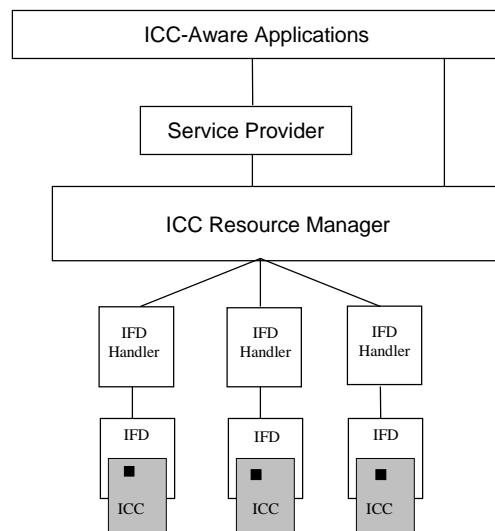


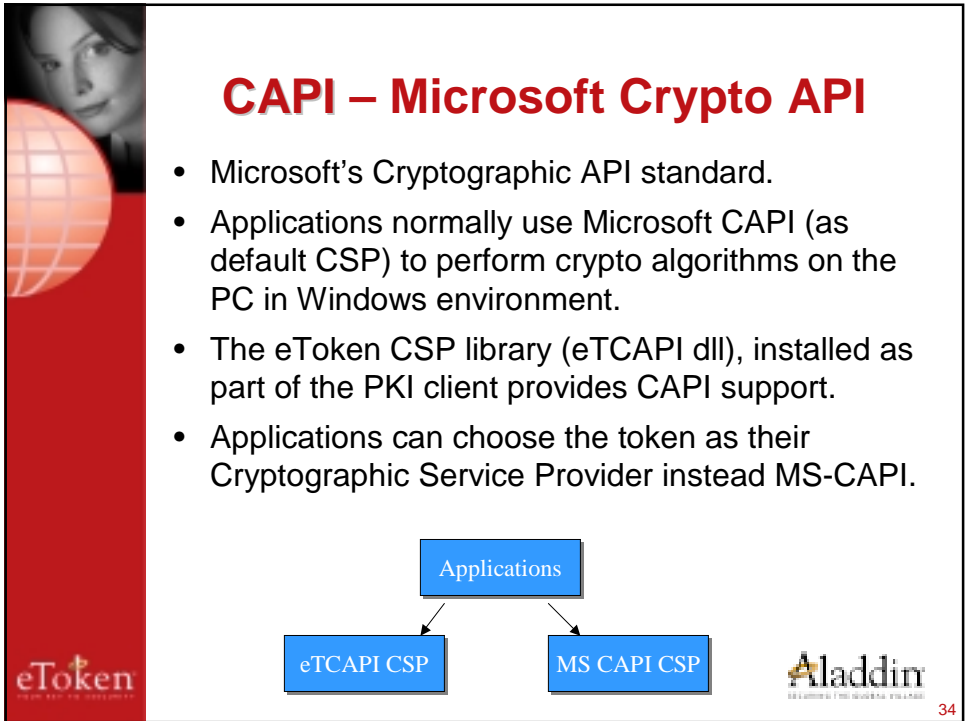
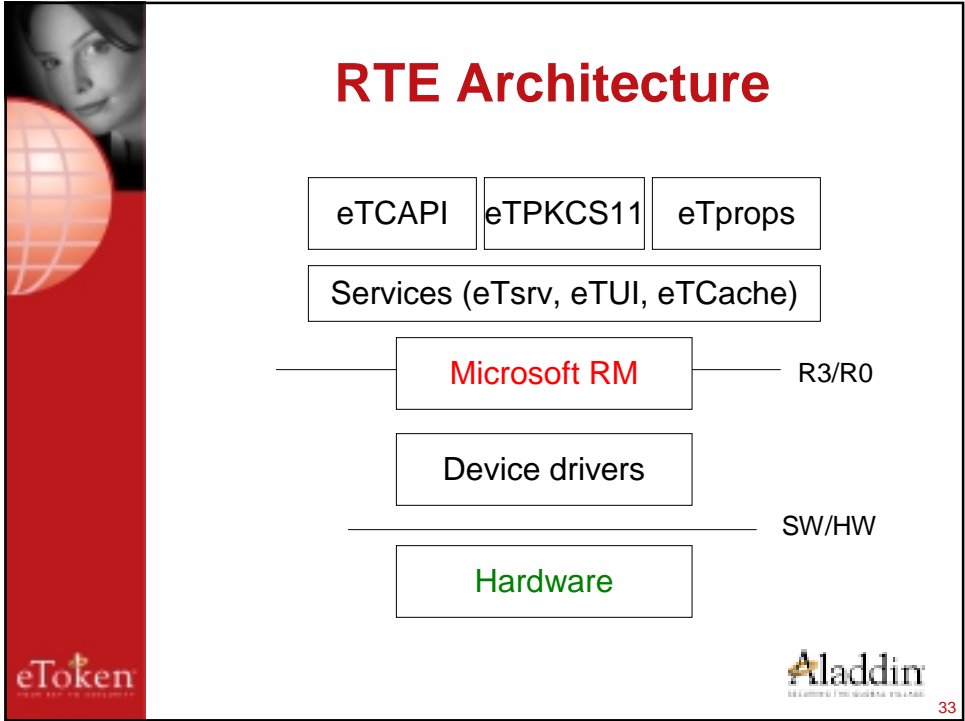
eToken and PC/SC

- eToken RTE installs a software component called eToken IFD Handler
- The IFDH simulates a smart card reader device
 - Can interface with one token
 - When token inserted, reports “card in” to the RM
- Number of installed IFDH devices determines how many tokens can be used simultaneously



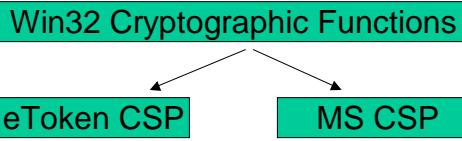
PC/SC Architecture - Components







Microsoft CAPI vs. eTCAPI



- MS CSP uses the processor for algorithms and the Registry for storing keys
- eTCAPI CSP, enables integration with all Microsoft software that supports CAPI
- The eToken Smartcard chip is used for processing algorithms + on board key generation and storage
- eTCAPI enables support for eToken certificate store



PKCS#11

- An open standard API proposed by RSA Laboratories.
- Presents a “virtual token” for applications.
- Enabling applications to access smartcard devices.
- Provides management functions to locate and manipulate cryptographic tokens.
- Allows easy integration into existing smartcard enabled applications.



eToken PKCS#11

- Module provided by the eToken PKI client, implementing PKCS#11 v 2.01
- Installed in the %System% directory
- Uses the token for object storage, and on PRO – on board Decryption and Digital Signature
- Installed in applications by setting the path to the cryptographic module (eTPKCS#11.dll)



37



CAPI, PKCS#11 and Certificates

- Both eTCAPI and eTPKCS#11 provide functionality to write certificates to the token.
- eToken PKI client implements full interoperability between eTCAPI and eTPKCS#11.
- Certificates and keys created by eTCAPI are visible by eTPKCS#11 and vice versa.



38

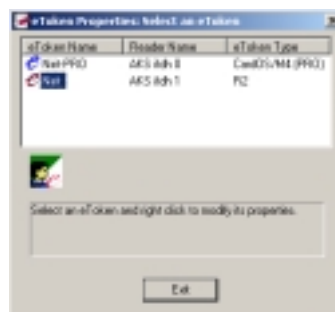
APDU Library

- APDU – **A**pplication **P**rotocol **D**ata **U**nits
- Allows access to low-level commands of the token
- Unique commands to each type of eToken or smartcard
- PRO is compatible with Siemens-Infineon smart card
- Mostly used for custom application

Personalizing the eToken

A user can personalize his eToken using the **eToken Properties** Utility.

- ✓ **Rename eToken**
- ✓ **View eToken information**
- ✓ **Change the eToken personal password**





Aladdin
SECURITY THROUGH INTELLIGENCE

eToken SDK

eToken™

YOUR KEY TO eSECURITY

Developing for eToken

eToken
FROM KEY TO INTELLIGENCE



eToken SDK Overview

SDK (Software Developer's Kit) enables integrating eToken functionality into any customized applications.

- **Authentication**
- **Digital signatures**
- **Encryption and decryption**
- **Secure storage**

The SDK offers robust API's

- eTPKCS#11
- eTCAPI
- **Card APDU commands**


OS support:

- Microsoft Win 9x, Me, NT, 2000, XP
- Real mode 16bit driver
- Linux drivers and smartcard support (APDU)

eToken
FROM KEY TO INTELLIGENCE

Aladdin
SECURITY THROUGH INTELLIGENCE


42




Examples of eToken Applications

- PC boot protection (laptop theft protection)
- File and Desktop access control
- Single sign-on applications
- Personal credential holder (e-Wallet)
- Extranet and web access
- E -Banking

Digitally Sign




eToken
FROM KEY TO DIGITALITY




Examples of eToken Applications

- User identification and authentication to a PC
- User identification and authentication to a LAN, including Windows logon.
- Remote access security clients
- Web authentication (subscription services)
- VPN applications



Authenticate



Aladdin
THE GLOBAL POLARIS

44



Special Development kits

eToken SDK for Linux

- Components: Drivers, Linux CT-API, PC/SC, Samples, Documentation
- Can be used for:
 - PC Logon, Thin client

eToken SDK for 16 bit

- 16 bit Static Library (Borland and Microsoft) that enables the communication with the USB device in real mode.
- Can be used for:
 - Boot protection



eToken for specific Vendors

eToken Vendor ID – Provides a utility enabling a vendor to restrict the application to use only its related tokens.

- Utilization of the Vendor ID option requires:
 - Developer utility
 - Production facility





eToken Utilities Set Overview

- **The eToken Certificate Converter –**
Enables the transfer of digital certificates and keys from a computer to an eToken.
- **The eToken PRO Format –**
Restores an eToken PRO to its initial state, while retaining all essential support libraries and data.
Resets the eToken default password.
Determines the eToken administrator password.
- **The eToken Application Viewer –**
Enables viewing the certificates and application profiles which are stored on the eToken.

eToken
FROM KEY TO ACCESS

Aladdin
SECURITY SOLUTIONS

47



eToken in the Future

- Additional PIN entry systems like Biometric fingerprint and Voice signature.
- Flash memory on card.
- Different proximity coils for extra physical access control functionality.
- Java cards
- Additional applications (like the WSO, SSO, TMS) to our eToken platform.

eToken
FROM KEY TO ACCESS

Aladdin
SECURITY SOLUTIONS

48



Aladdin
SECURITY THROUGH POLICY

Thank you

eToken™
YOUR KEY TO eSECURITY

Nirit Bear
September 2002