
Datakey, Inc.

Hardware-based Public Key Encryption
for
Secure Applications

Presentation Outline

- Datakey Inc. --- Smart-Token Products
- Smartcard and Smartkey Applications
- SignaSURE[™] Product Set
 - cryptographic tokens
 - API's and device drivers
 - initialization and key escrow station
 - electronic document security
- Secure Enterprise Services
 - web browser, email client, file access control

Datakey Product History

Evolution of Smart Tokens

1986: Cytrol utilizes 1400 bit serial EAROM for access control to IBM PC.

1987: NSA adopts Datakey's parallel memory as the token of choice for the Secure Telephone Unit Version 3 (STUIII)

1989: NIST contracts Datakey to produce a Token-based Access Control device using Hybrid DES Module

Datakey Product History

1990: Datakey moves TBACS to smart card/key format (Smart Card Access Control System)

1991: Datakey adds RSA and DSA algorithms to SCACS making it an Advanced Smart Card Access Control System (ASACS)

1993: Datakey adopts the Siemens SLE200 chip with proprietary code to generate public key-pairs on chip. Begins to market SignaSURE™ brand smart tokens

Smartcards and Smartkeys

- More secure than storing your private keys in a file or database on your PC's hard drive !
 - private keys stored in non-volatile memory on the smart token
 - private keys cannot be read by host computer
 - all private key operations are performed on the card by the embedded crypto processor
 - > generate digital signature
 - > unwrap dynamic session (secret) key
 - a secure application user must first “login” to the token by providing correct “PIN” or “passphrase”

Smartcards and Smartkeys

- An intruder needs more than just physical access to your personal computer --- they would have to obtain both your Smart token and your current “passphrase” in order to use the private keys protected within the Smartcard to:
 - forge your digital signature, or
 - decrypt and read your confidential information

Datakey SignaSUREtm Product Set

- Smartcard Cryptographic Token
- Smartkey Cryptographic Token
- Security Officer Station
- User Smartcard/Smartkey Manager
- Windowstm APIs and Device Drivers
 - PKCS#11 (Cryptoki) DLL
 - Crypto Service Provider (CSP)

Datakey SignaSUREtm Product Set

- Enterprise Security Services (ESS)
 - Token-enabled Web Browser
 - > secure web browser and secure e-mail client
 - Directory Server
 - > publish user info., e-mail addresses, ID certificates, etc.
 - Certificate Server
 - > issue and manage ID certificates
 - Secure File Service
 - > manage, exchange sensitive business information

SignaSUREtm Smartkey



January 1997

Datakey, Inc.

SignaSURE™ Smartcard



SignaSURE™ Smartcard

- Model 10XC Reader and model 360 Smartcard
 - ISO 7816 compatible device
 - configured with 2 or 3 public/private keys
 - > RSA signature key (512 or 1024)
 - > DSA signature key (512)
 - > RSA exchange key (512 or 1024)
 - inject keys on token (RSA exchange key)
 - generate keys on token (signature keys)
 - generate random numbers/dynamic session keys
 - private key operations require: PIN/Passphrase

SignaSURE™ Smartcard

- performs private key operations “on the card”
 - > digital signature - sign
 - > key exchange - unwrap session key
- non-volatile EEPROM storage
 - > multi-level directory tree w/access control
 - > public/private keypairs
 - > organization’s security policies/options
 - > security officer PIN/passphrase
 - > user PIN/passphrase(s)
 - > secure application options, user profile, other

Security Officer Station

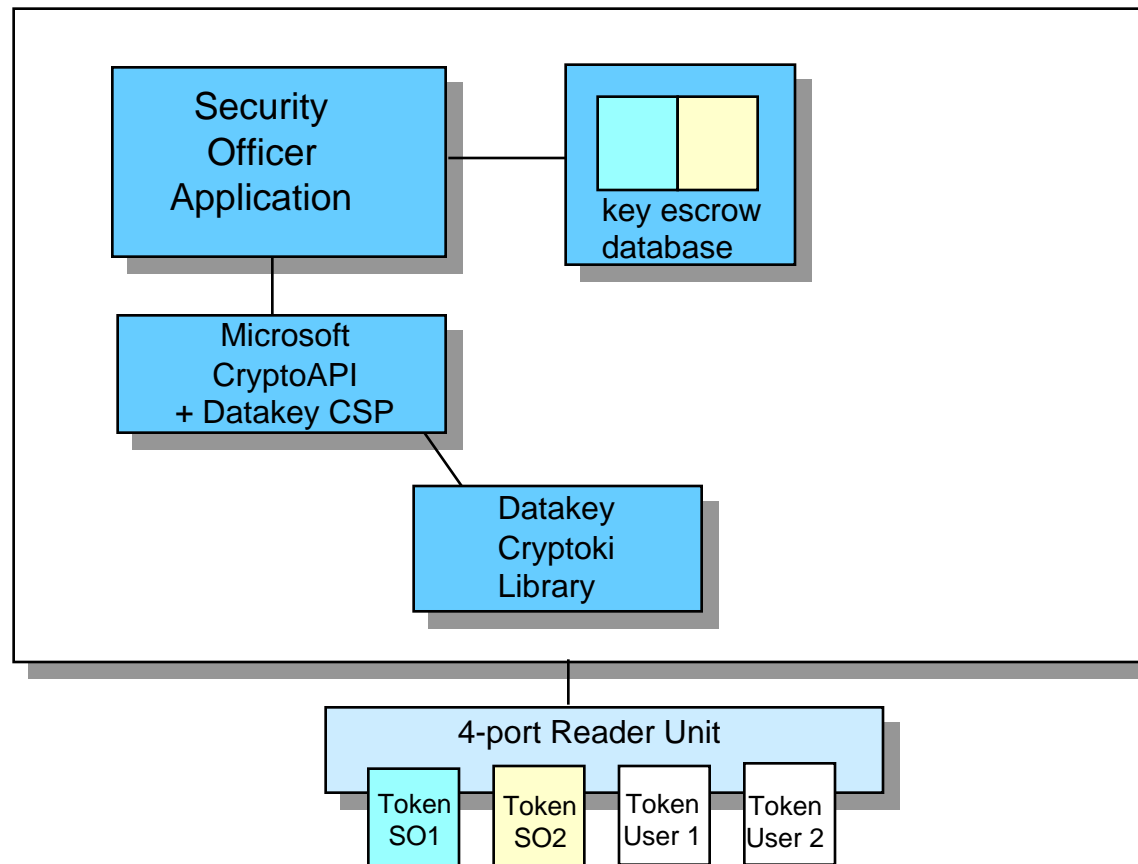
- Datakey-supplied PC system and Security Officer Station application software:
 - > Microsoft Windows 95 or Windows NT Workstation
 - > offline system for added escrow database security
 - > integrated Smartcard reader unit - four (4) tokens
 - > SO access controlled by SignaSURE smart tokens:
 - “single SO” or “dual SO” station control options
 - list of registered security officers, smartcards
 - > complete SO audit trail and key escrow database
 - each entry double-signed by security officers
 - each entry double-encrypted for security officers
 - escrow user “exchange keys” only
 - key recovery in the event of Smart token loss or failure

Security Officer Station

- Initialize/configure smart tokens for users
 - > inject or generate the RSA exchange key-pair
 - default: BSAFE generate then inject into token
 - default: do not install signature key-pair(s)
 - option: restore from escrow db
 - option: overwrite (reuse the token)
 - > escrow the RSA exchange key-pair
 - > install organization's security policies
 - key-pair generation policy
 - min. passphrase length and max. timeout value
 - signature algorithm options (RSA, DSA, or both), etc.
 - > initial user passphrase/PIN
 - > initial security token ID, etc.

Security Officer Station

Personal Computer with 32 bit Windows™ Operating System



Security Officer Station

Initialize Token

SO PIN

Status: Pete D's SO Token

Token: 90000009

Status: Pam S's SO Token

Token: 80000008

Status: Init Sig Keys Completed in 0:0:03

Token: 10000001 Recipient: Sally Fields

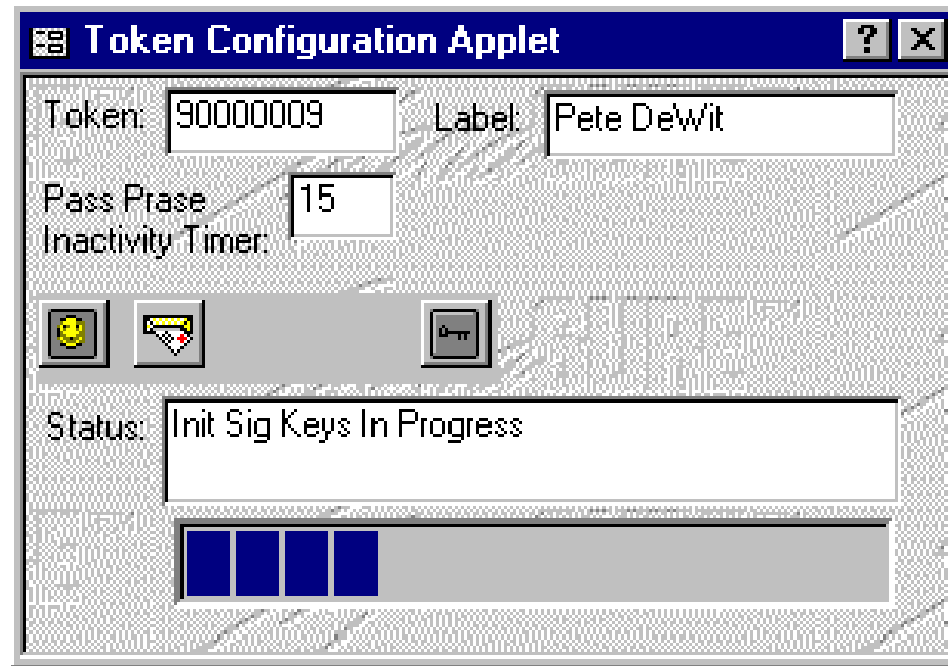
Reset Lock

Init Exch Keys Re-Init Exch Keys

Smart-Token Manager

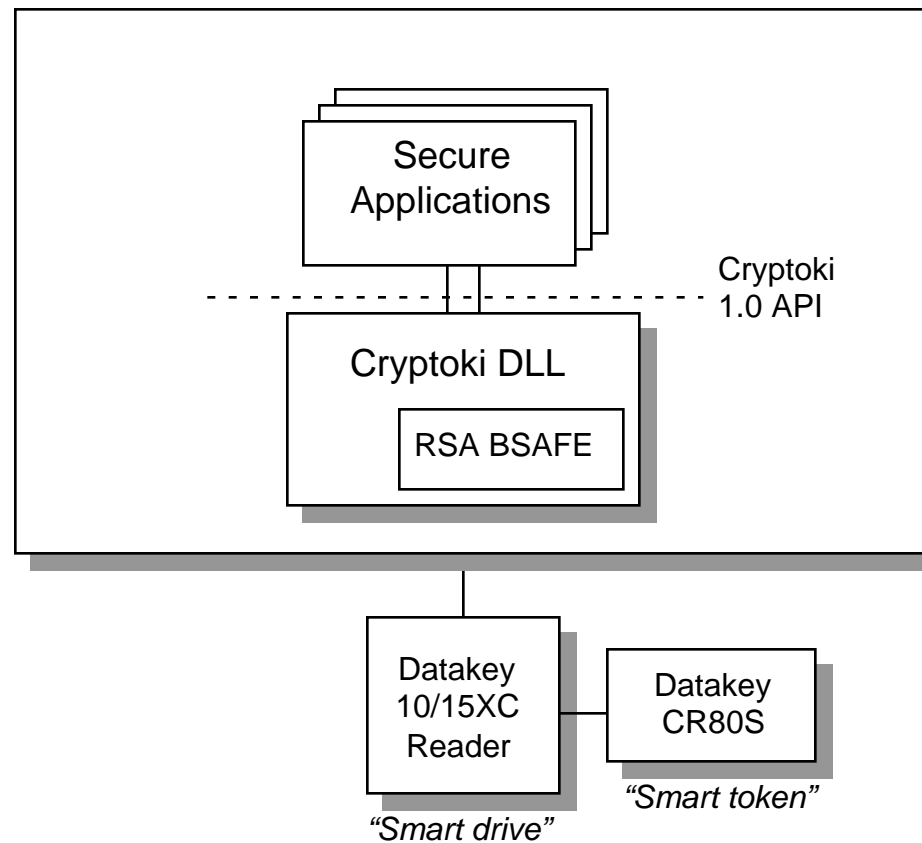
- Datakey-supplied Windows[™] Application
 - > Windows 3.1, Windows 95, Windows NT (16 or 32-bit)
 - > Performs smart-token management functions as directed by an authenticated user:
 - generate signature key pairs (RSA, DSS, or both)
 - change user PIN/passphrase
 - define or modify smart token ID
 - display smart token status
 - exercise public/private key-pairs
 - RSA exchange key
 - RSA signature key
 - DSA signature key
 - modify user PIN/passphrase timeout value

Smart-Token Manager



PKCS#11/Cryptoki Library

Personal Computer with 16 or 32 bit Windows™ Operating System



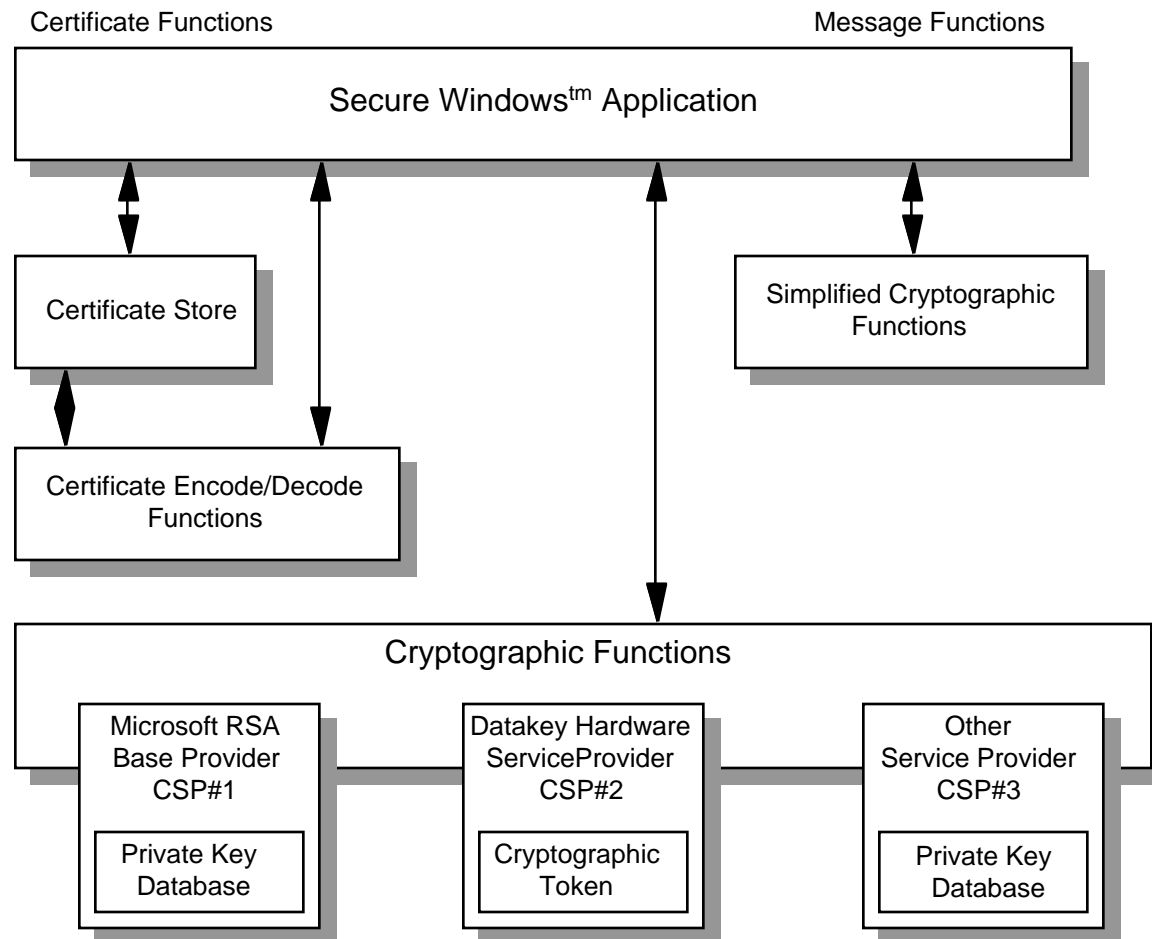
PKCS#11/Cryptoki Library

- Standard Cryptoki 1.0 Library
 - > all private key operations performed on the smart-token
- Supports Datakey extensions to PKCS#11 (used primarily by Datakey-supplied programs):
 - > D_GetAtr
 - > D_SetUIS, D_GetUIS
 - > D_SetDKIS, D_GetDKIS
 - > D_GetSeed
 - > D_UnlockToken
 - > D_SetTokenPresentCallback

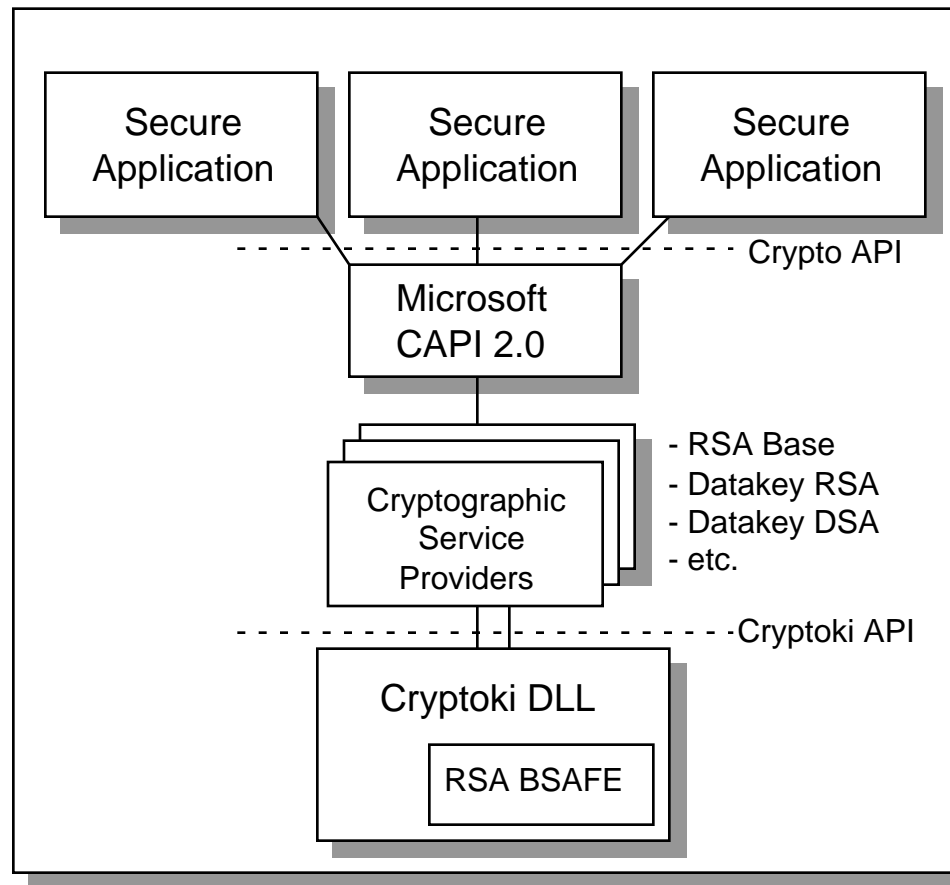
Crypto Service Provider (CSP)

- Standard Cryptographic Service Provider as defined by Microsoft's CryptoAPI Architecture
 - > RSA BSAFE cryptographic engine
 - > RSA key exchange (512, 1024)
 - > RSA Signature/Verification (512, 1024)
 - > DSA Signature/Verification (512)
 - > Message Digest/Hashing Algorithms (MD2, MD5, SHA-1)
 - > Symmetric Encryption Algorithms
 - RC2, RC4
 - DES (FIPS 46-2)
 - Triple DES

Microsoft's CryptoAPI 2.0 Architecture

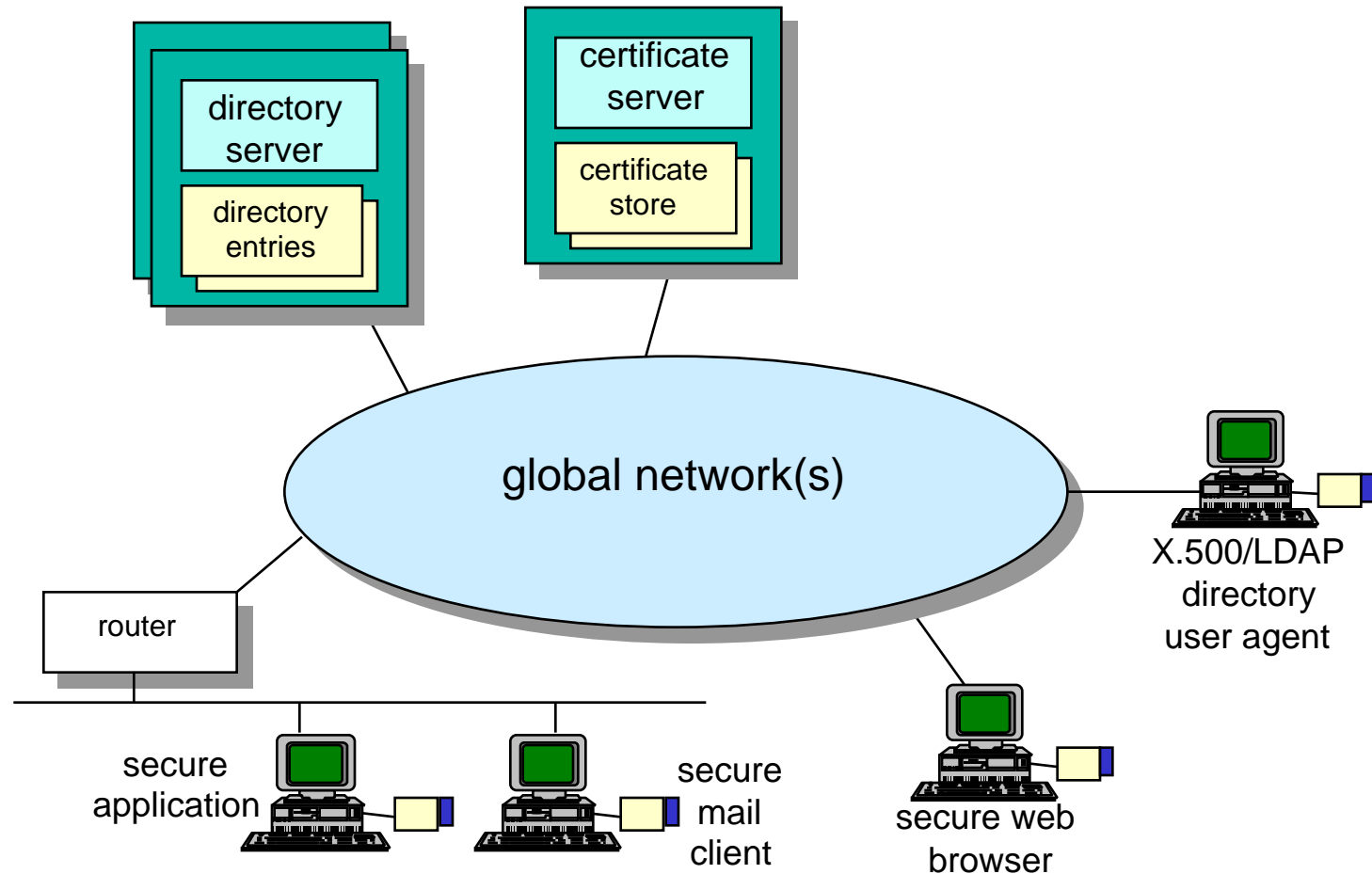


Datakey Cryptographic Service Provider (CSP)



Personal Computer
with 32-bit Windows™
Operating System:
- Windows 95
- Windows NT

Data Security Architecture



Secure Web Browser/Mail Client

- Netscape Communicator 1.0 with integrated Datakey Smart Token
- token-enabled SSL 2/3 for secure web server access
 - server and client authentication
- token-enabled secure e-mail (S/MIME) for business messaging
 - sign message option
 - encrypt message option
- local key exchange (encryption) certificate caching for secure correspondents (e-mail address book)
- recipient look-up (via Directory/LDAP server)

Certificate Server

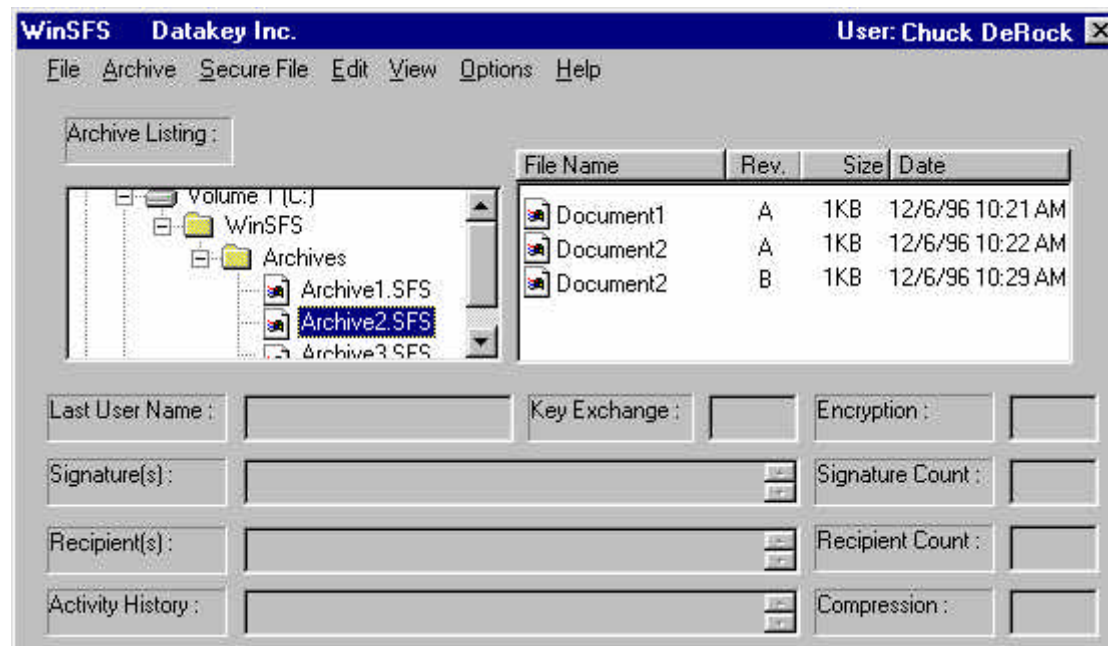
- Corporate users can generate and distribute certificates for their employees, etc.
- Netscape Certificate Server
- Certificate issuing and life-cycle management controlled by authorized administrative personnel
 - > browser access with 2-way strong authentication
- Issued certificates posted to Directory (LDAP) Servers

Directory Server

- Netscape Directory Server
- LDAP Server = access to directory information
 - > user name
 - > e-mail address
 - > phone number
 - > X.509 Identification Certificate
 - > etc., etc.
- supports large, distributed corporate directories
 - > Supports distributed directory operation through sophisticated replication capabilities
 - > Safeguards directory information via access control lists and SSL server/client (strong) authentication

Secure File Services

hardware-based information security for your notebook computer, confidential business files, etc.



Secure File Services

- Provides scalable, general purpose data security for 16 and 32 bit Windows PC systems
- Secures data files produced by any Windows application
- personal key protection, data portability, data integrity, and data security ensured through use of Datakey Smart-tokens
- public key encryption technology
 - uses RSA, DSA public key algorithms
 - uses X.509 v3 ID Certificates

Secure File Services

- Users manage a library of secure electronic documents:
 - library consists of one or more “secure archives”
 - each archive contains a number of secure electronic documents (files)
 - user assigns persistent security properties to individual files, file lists, directories, etc.:
 - > compression algorithm
 - > encryption algorithm, key size
 - > list of authorized users and their respective file/document access permissions (create, write, update, read, delete)

Secure File Services

- Integrated with Windows File Manager, File Explorer, and other widely used apps:
 - File|Move-to-Archive
 - File|Copy-to-Archive
- Easily integrated with user's e-mail client(s)
 - send secure archive as a binary attachment
- Full selection of cryptographic algorithms and key sizes:
 - RSA, DSA, DES, 3DES, DESX, RC2, RC4

Futures

- Secure archive remote access
- Exchange key “self-escrow” option

Summary

- Premium, hardware-based data security components and solutions for a standards-driven environment:
 - > Smart Cryptographic Tokens - ISO 7816
 - > Secure Web Clients and Servers - SSL 3.0
 - > Secure E-mail Clients - S/MIME
 - > Cryptographic APIs
 - PKCS#11/Cryptoki
 - CryptoAPI
 - > Cryptographic Algorithms - RSA, DSA, DES, 3DES, etc.

Contact Information

Dale Gustafson

Datakey, Inc.

407 West Travelers Trail

Minneapolis, MN 55337

612.890.6850

612.890.2726 fax

web: <http://www.datakey.com>

email: daleg@datakey.com

END