

## **SETECS, Inc.**

### **Design, Development and Deployment of Secure Network Applications**

**Global, integrated, end-to-end security system  
for secure Web services, mobile devices, and  
collaborative group applications**

**March 2005**



## **Internet Security Infrastructure**

**Collection of components, protocols, functions and interfaces for support of secure Internet applications**

## **SETECS Security Framework**

**Collection of methods, tools, components and interfaces for rapid and standardized design and development of secure Internet applications**

## **SETECS Secure Applications**

**Customized secure Internet applications built using Security Framework and supported by Security Infrastructure**

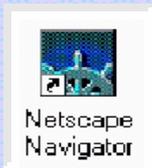
**Example : Integrated, global, end-to-end  
Web-based secure applications**

## Security Requirements :

- Local login (local authentication)
- Remote login (remote authentication – bilateral)
- Access control at the remote server (resources)
- Authorization (transactions)
- Protection of messages (confidentiality and integrity)
- Traffic protection and integrity (replay, lost messages, etc)
- Authenticity of a sender (digital signatures)
- Authenticity of a recipient (enveloping)
- Multi-party transactions and protocols
- Group transactions (conference, quorum)
- Non-repudiation



User



Browser

Request

Response



Web Server



DB

## **Problem :**

**Development and deployment of secure network applications**

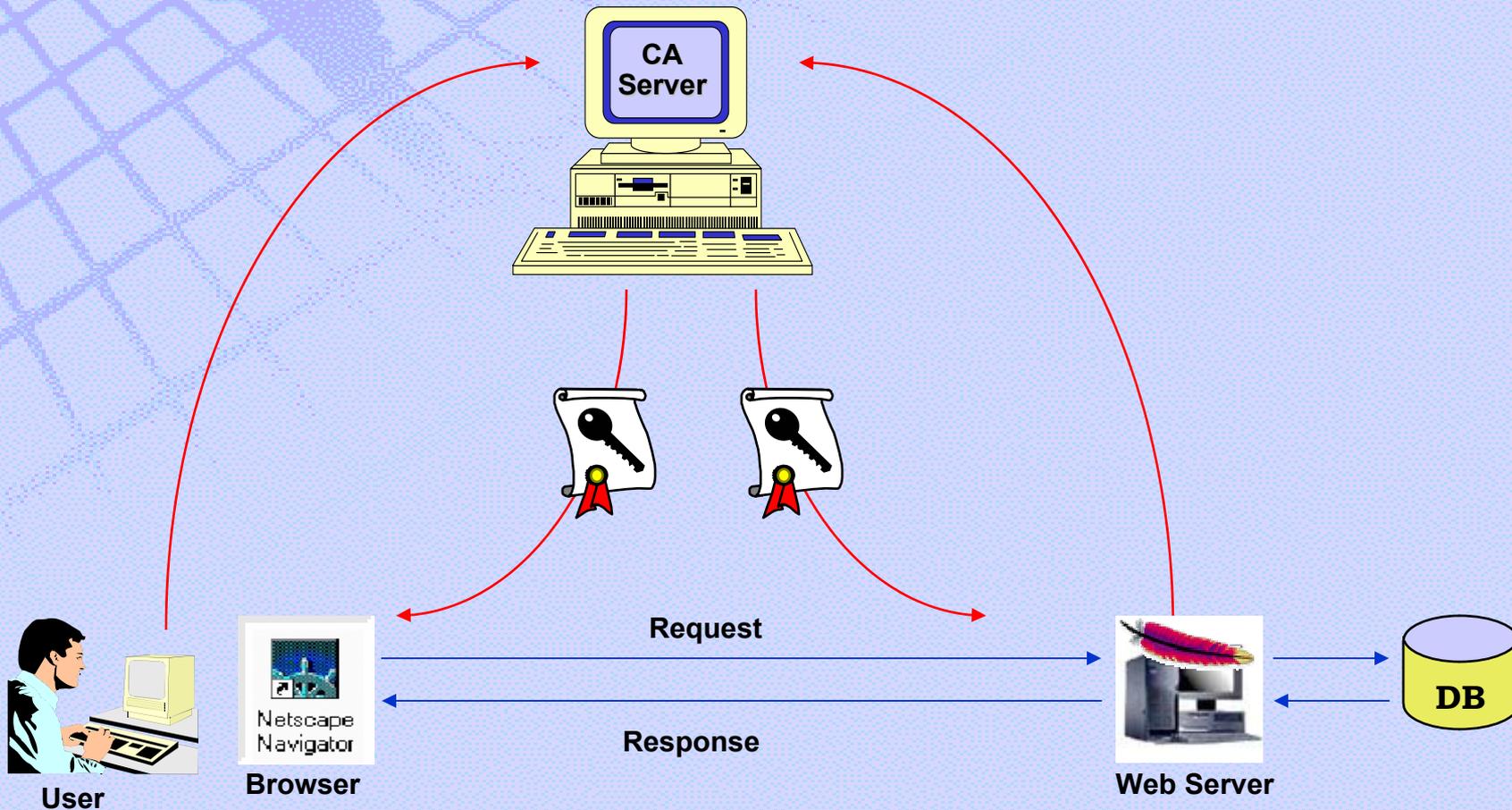
- **Complicated, expensive, long**
- **Compliance to standards and interoperability**
- **Not transparent and not user-friendly**

## **Solution :**

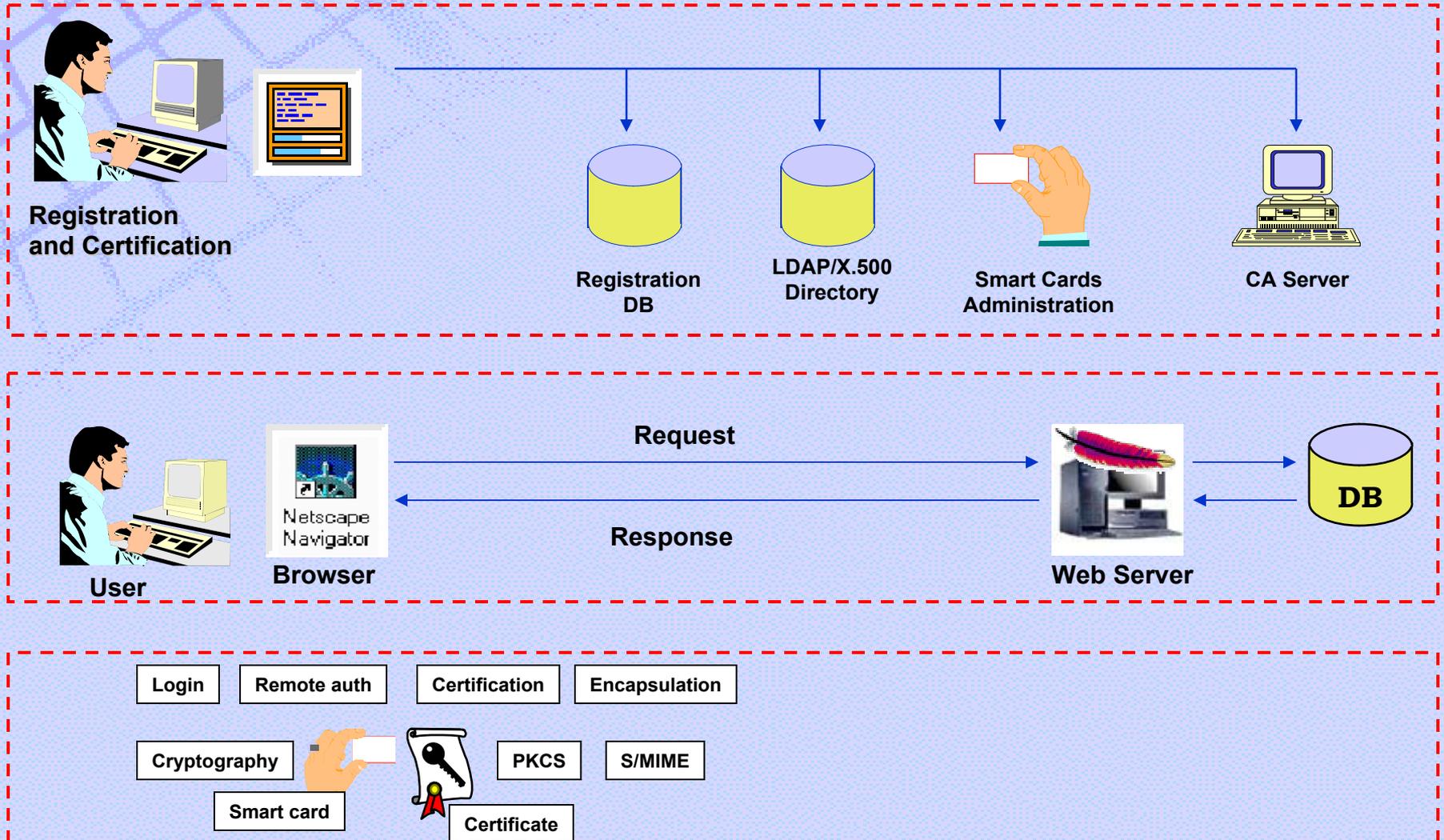
**Security Framework: collection of ready-made components (objects) for common PKI, smart cards, and crypto functions and protocols**

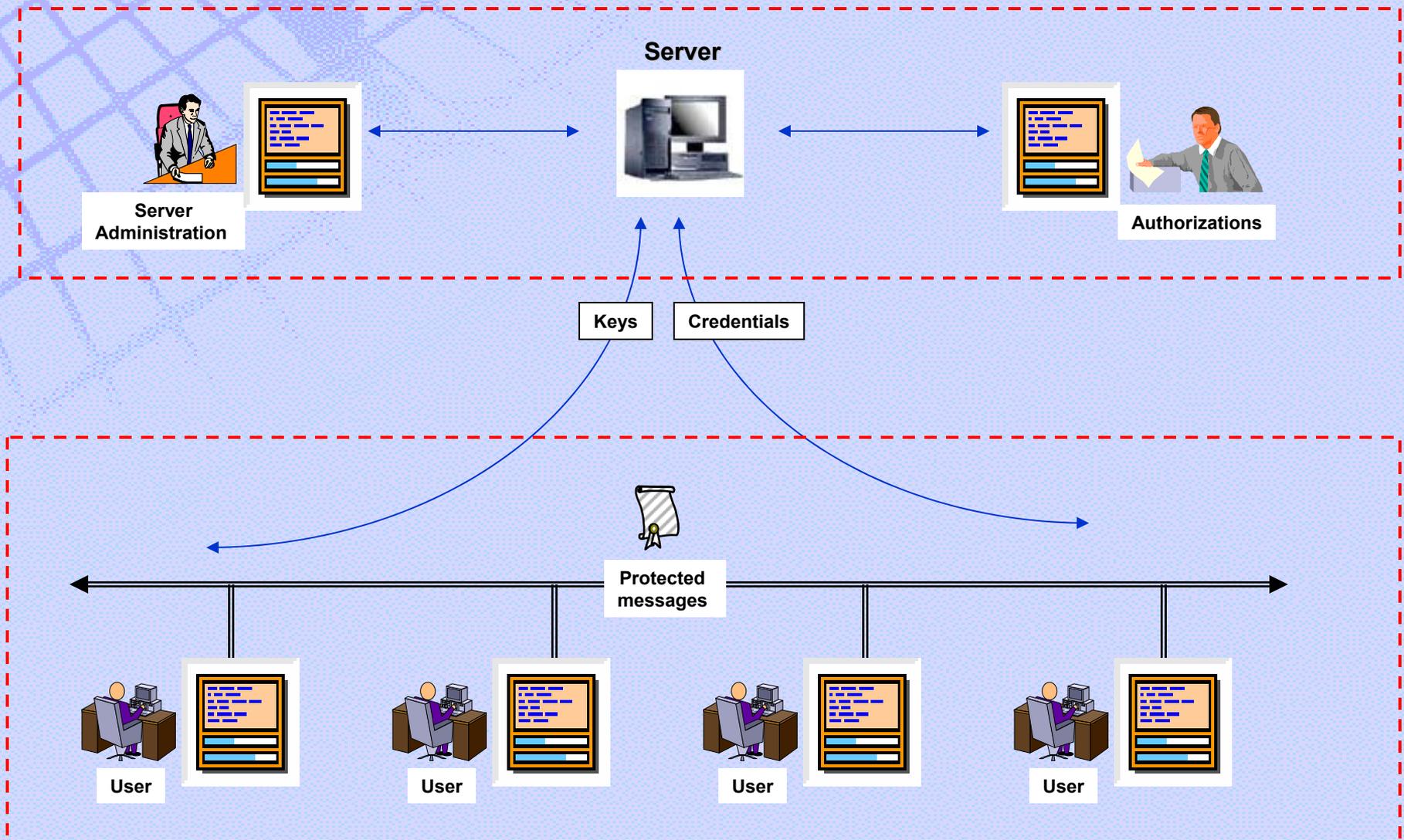
## **Security Framework :**

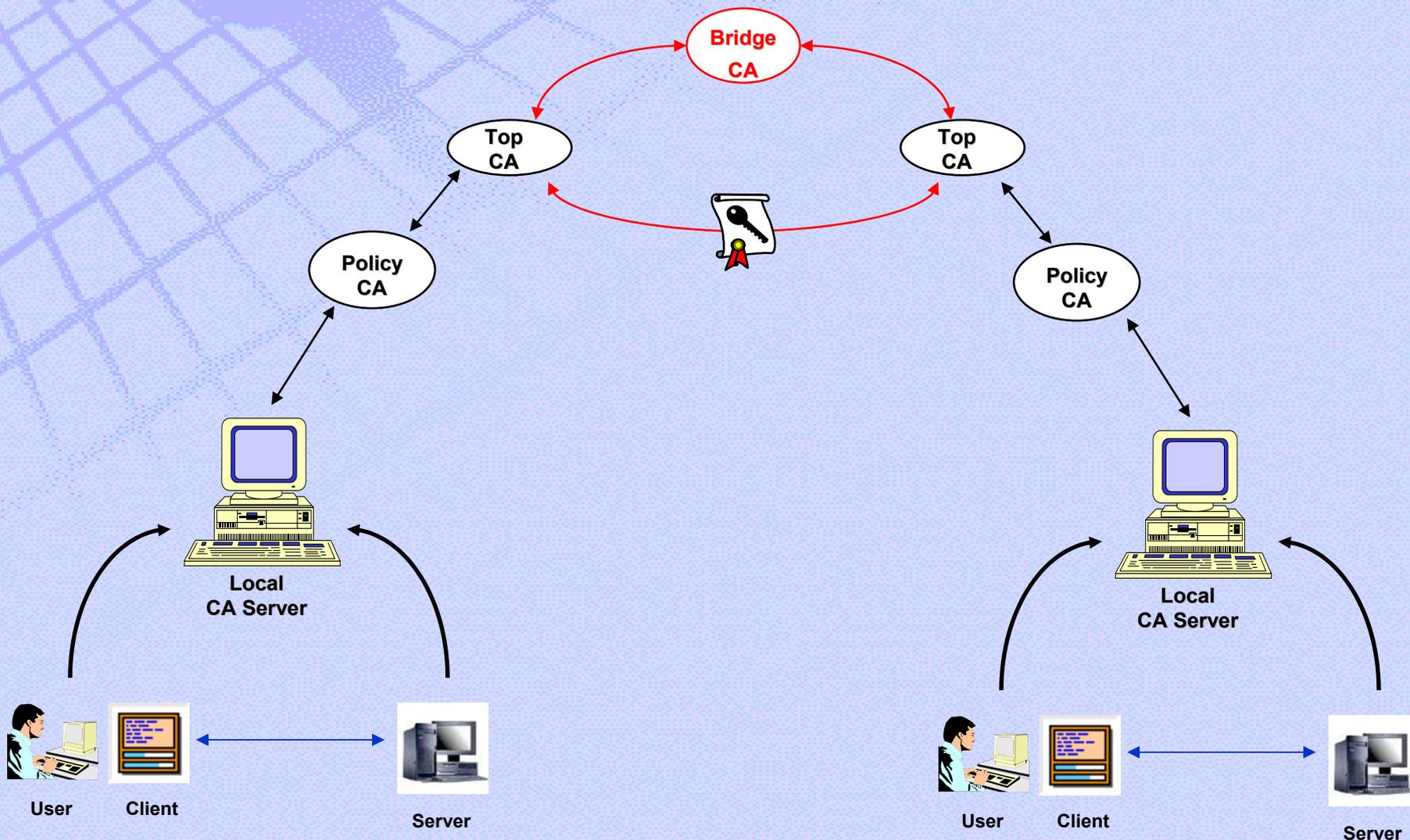
- **Concept (how to solve the problem)**
- **Methodology (approach to use the concept)**
- **Set of components (dev toolkit, plus run-time platform)**

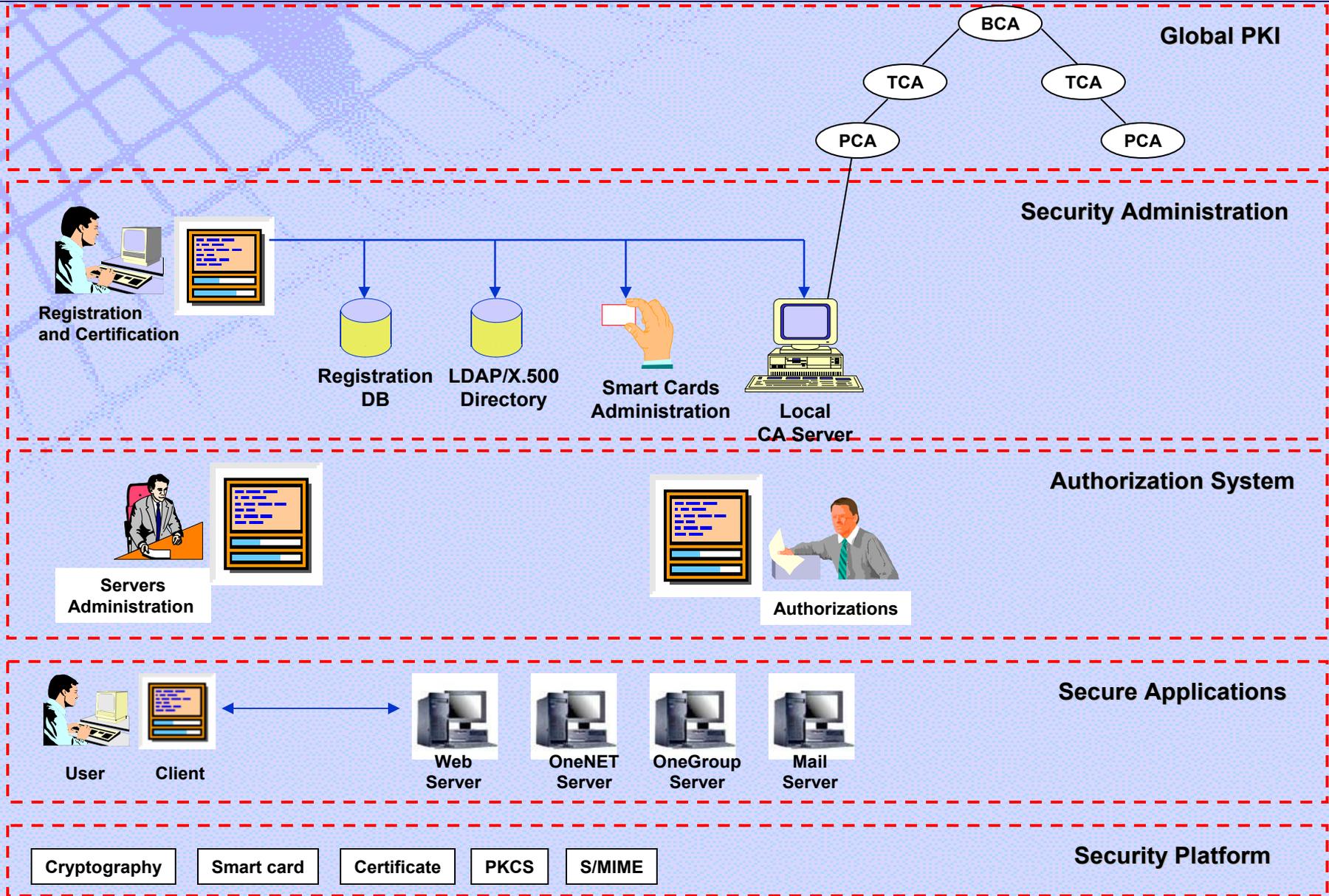


- Login
- Remote auth
- Certification
- Encapsulation
- Cryptography
- Smart card
- PKCS
- S/MIME
- Certificate









## Internet Security Infrastructure

Collection of components, protocols, functions and interfaces for support of secure Internet applications



## SETECS Security Framework

Collection of methods, tools, components and interfaces for rapid and standardized design and development of secure Internet applications

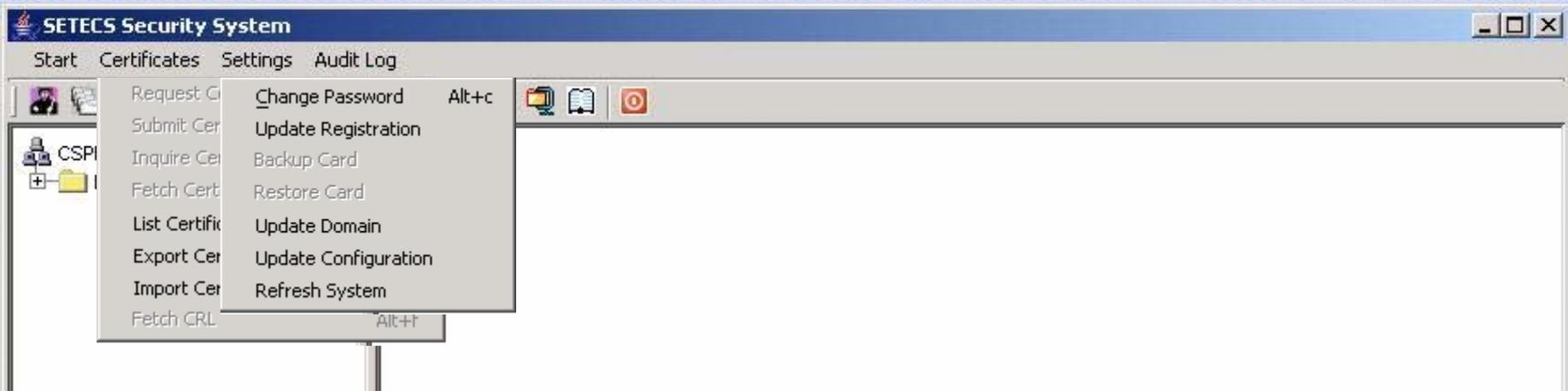
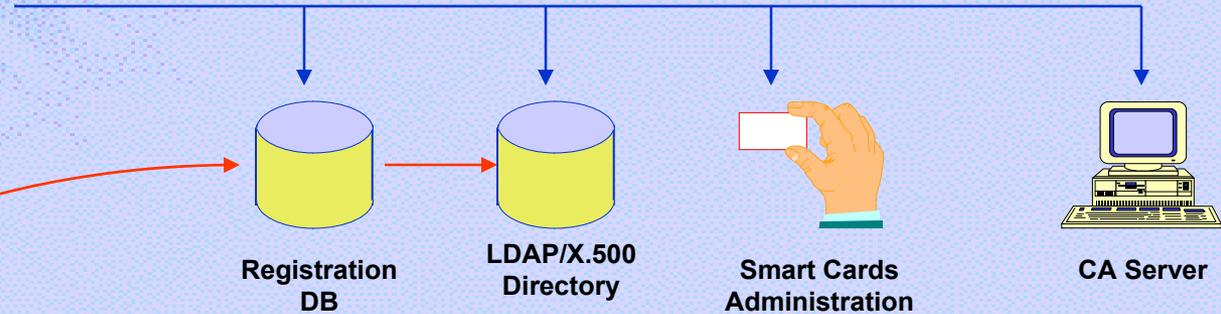
## SETECS Secure Applications

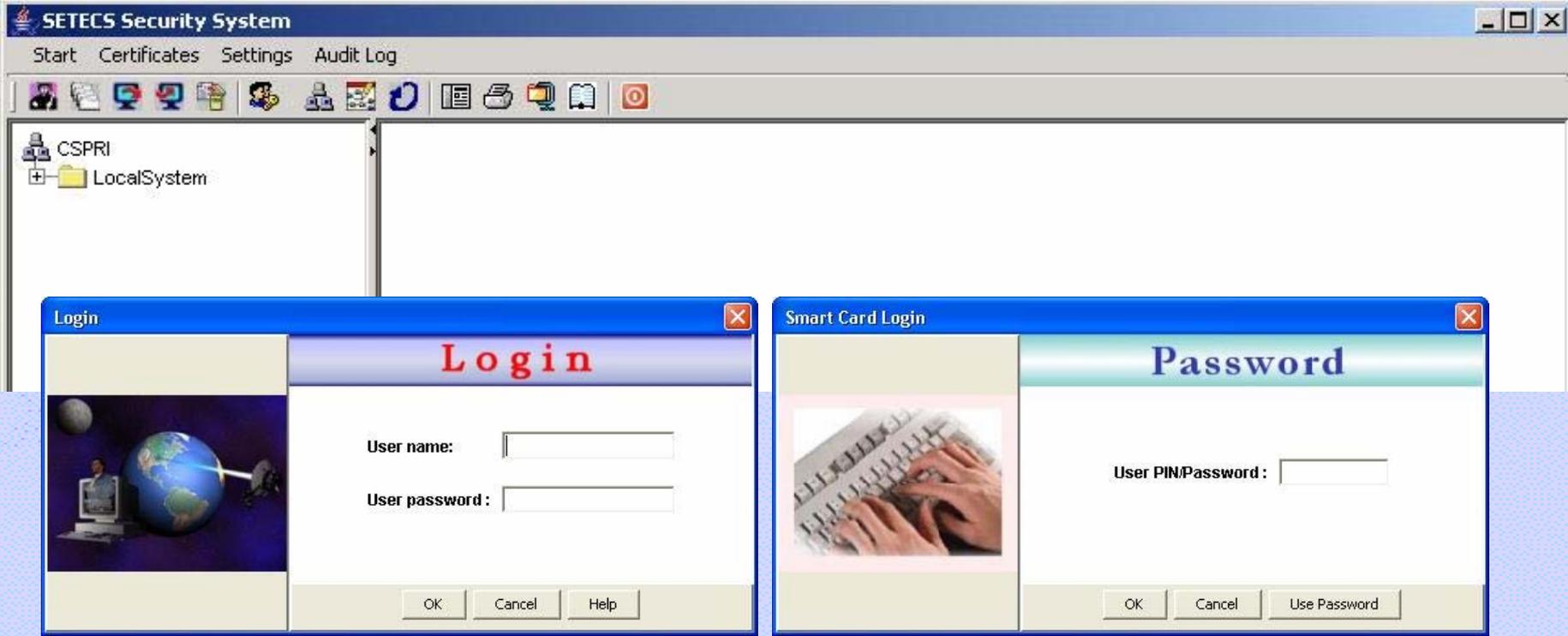
Customized secure Internet applications built using Security Framework and supported by Security Infrastructure

**Example : Integrated, global, end-to-end  
Web-based secure applications**

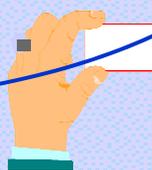


Registration  
and Certification

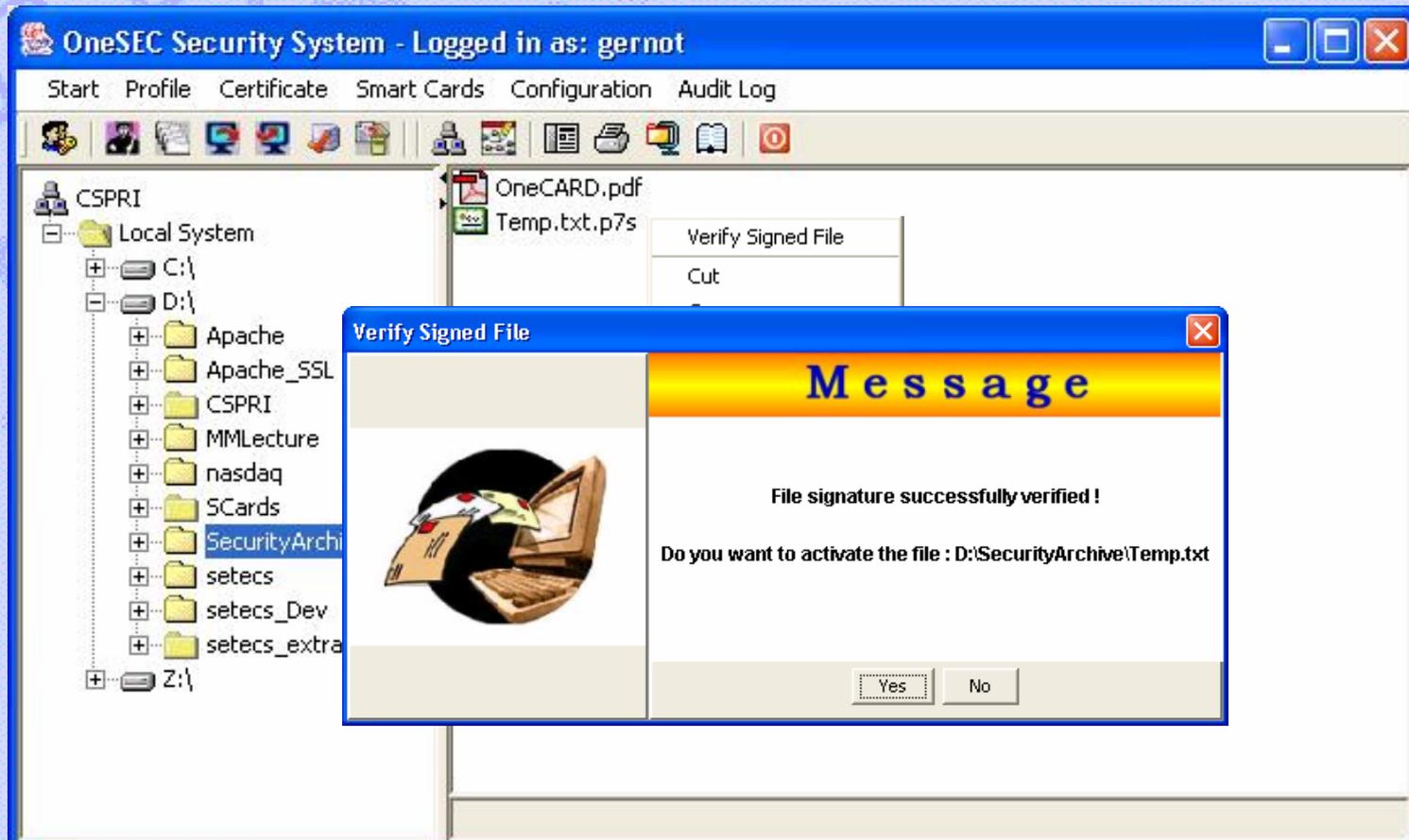


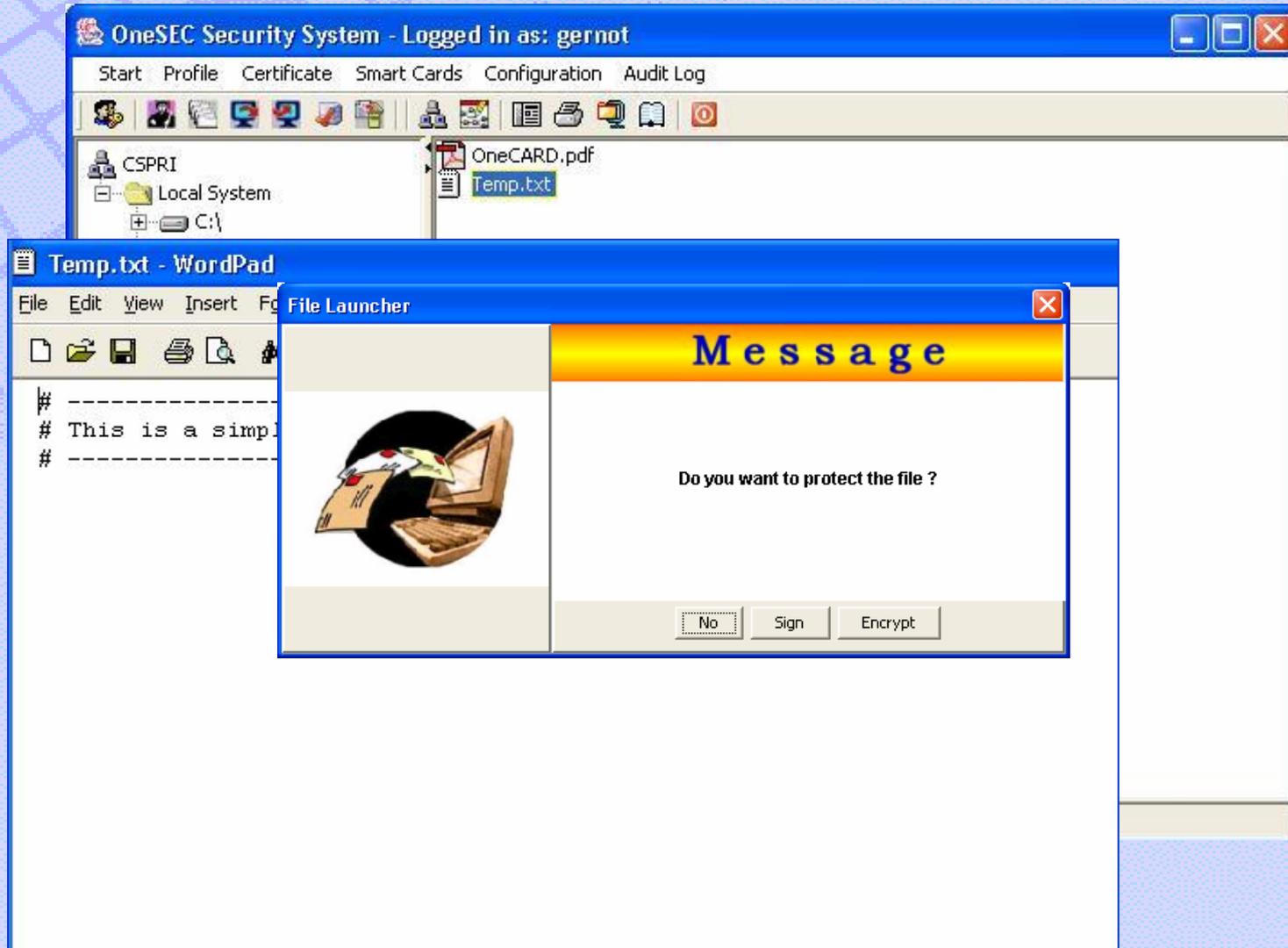


User



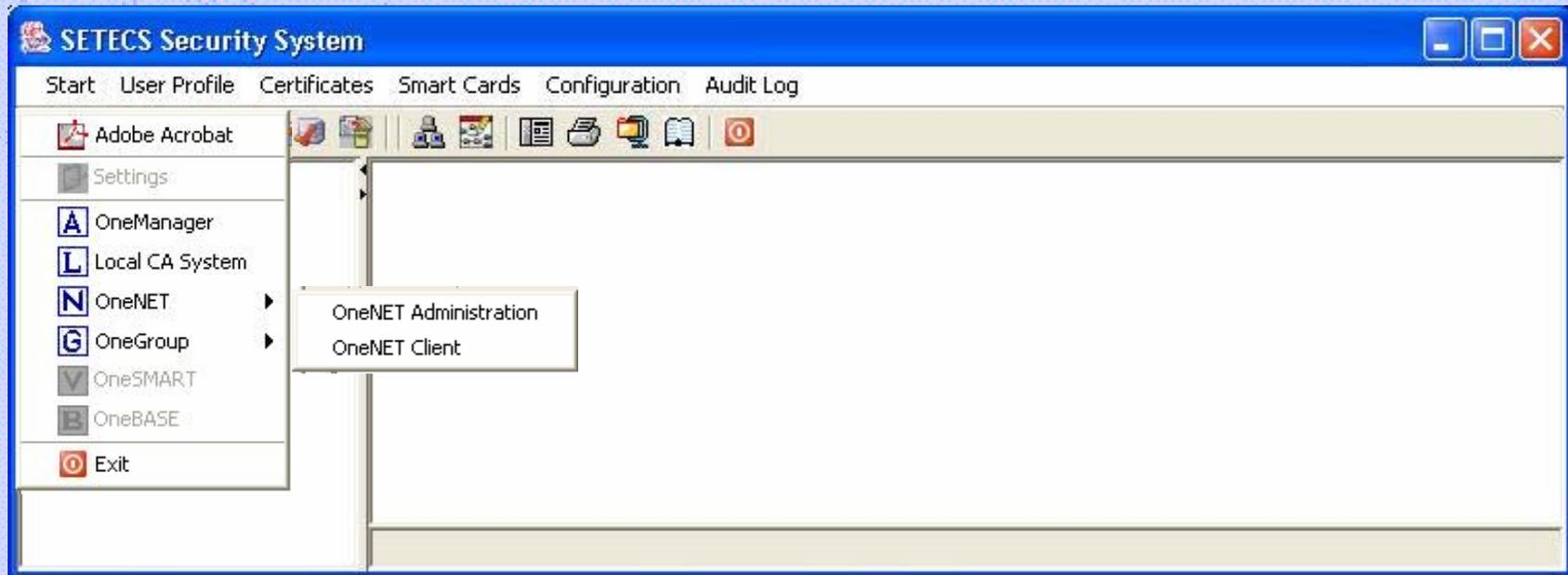


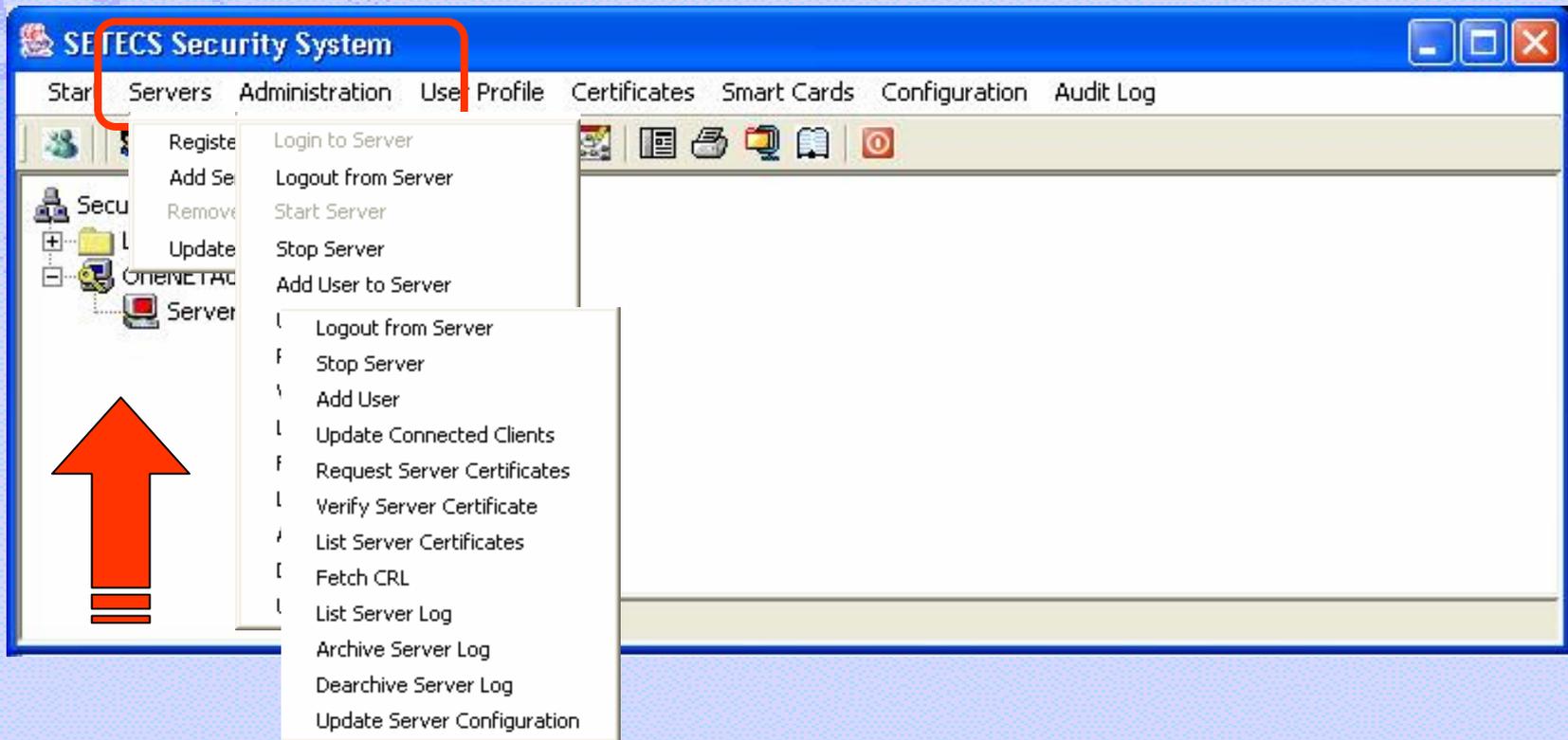


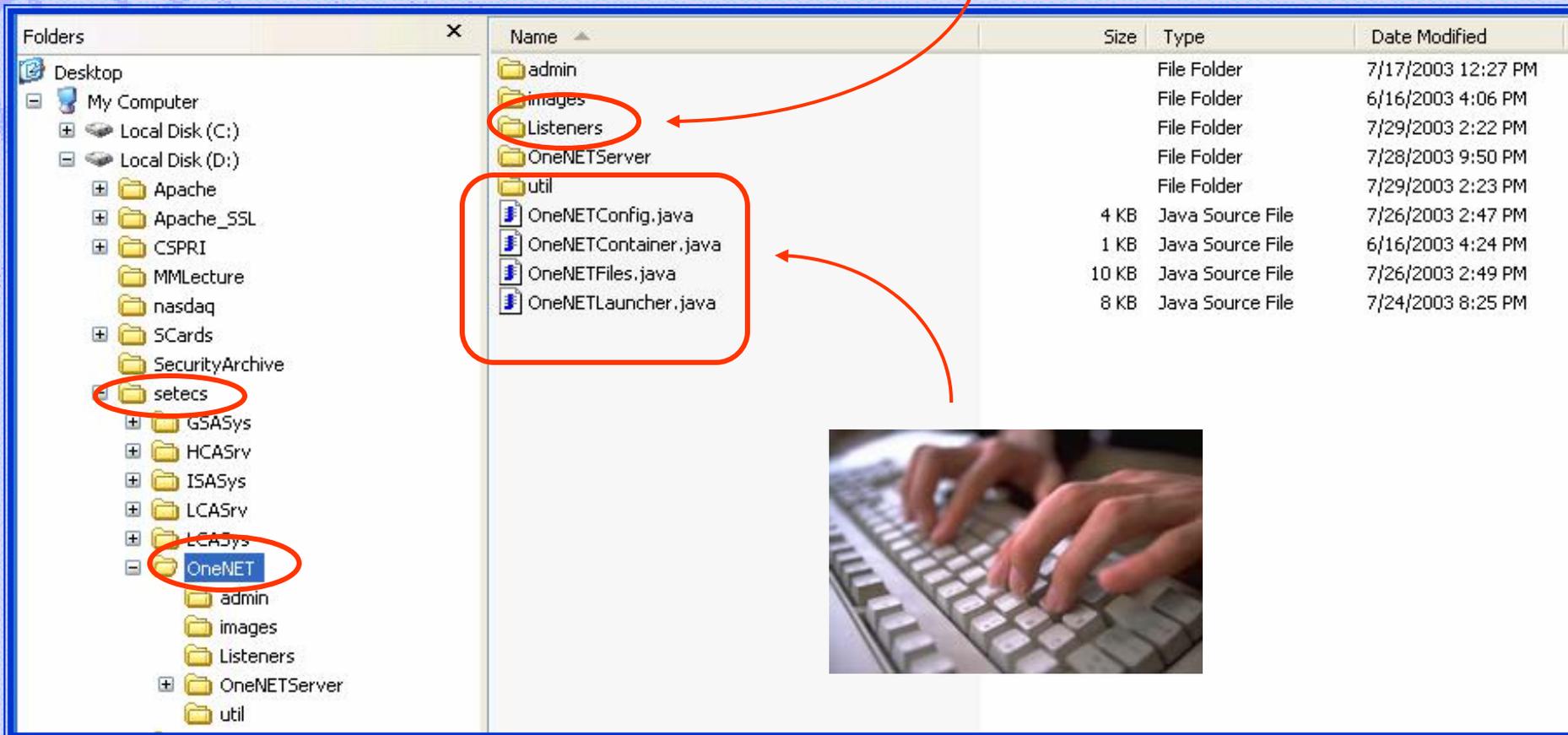


## Secure applications :

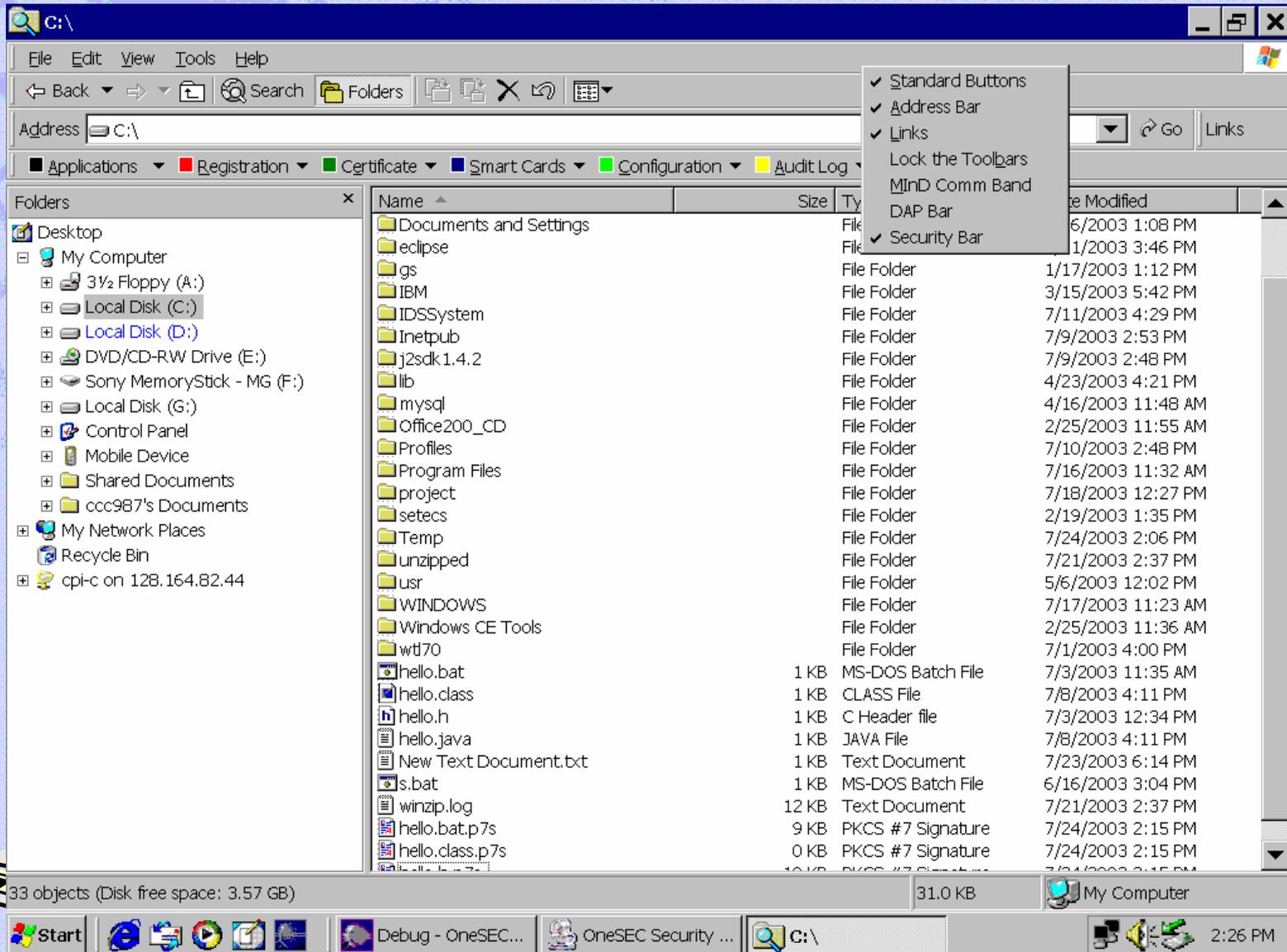
1. SETECS ready-made applications
2. Third-party development (new applications)
3. Existing (standard Windows) applications





| Name                 | Size  | Type             | Date Modified      |
|----------------------|-------|------------------|--------------------|
| admin                |       | File Folder      | 7/17/2003 12:27 PM |
| images               |       | File Folder      | 6/16/2003 4:06 PM  |
| Listeners            |       | File Folder      | 7/29/2003 2:22 PM  |
| OneNETServer         |       | File Folder      | 7/28/2003 9:50 PM  |
| util                 |       | File Folder      | 7/29/2003 2:23 PM  |
| OneNETConfig.java    | 4 KB  | Java Source File | 7/26/2003 2:47 PM  |
| OneNETContainer.java | 1 KB  | Java Source File | 6/16/2003 4:24 PM  |
| OneNETFiles.java     | 10 KB | Java Source File | 7/26/2003 2:49 PM  |
| OneNETLauncher.java  | 8 KB  | Java Source File | 7/24/2003 8:25 PM  |



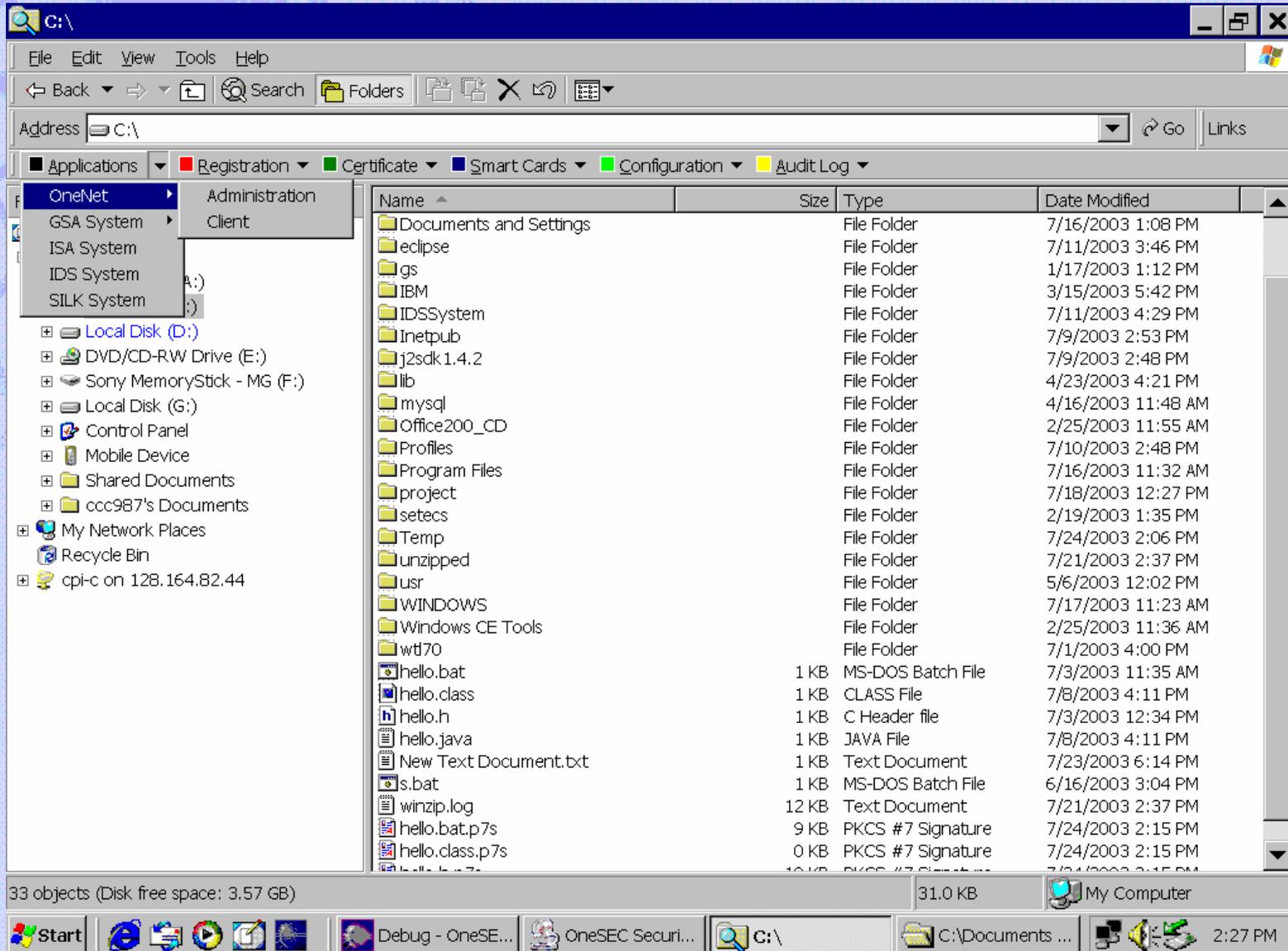
The screenshot shows a Windows Explorer window with the address bar set to C:\. The left pane shows the 'Folders' tree with 'Local Disk (C:)' selected. The right pane displays a list of files and folders in C:\. A context menu is open over the 'Security Bar' file, listing options: Standard Buttons, Address Bar, Links, Lock the Toolbars, MiND Comm Band, DAP Bar, and Security Bar. The 'Security Bar' option is checked.

| Name                   | Size  | Type              | Date Modified      |
|------------------------|-------|-------------------|--------------------|
| Documents and Settings |       | File Folder       | 6/2/2003 1:08 PM   |
| eclipse                |       | File Folder       | 1/2/2003 3:46 PM   |
| gs                     |       | File Folder       | 1/17/2003 1:12 PM  |
| IBM                    |       | File Folder       | 3/15/2003 5:42 PM  |
| IDSSystem              |       | File Folder       | 7/11/2003 4:29 PM  |
| Inetpub                |       | File Folder       | 7/9/2003 2:53 PM   |
| j2sdk1.4.2             |       | File Folder       | 7/9/2003 2:48 PM   |
| lib                    |       | File Folder       | 4/23/2003 4:21 PM  |
| mysql                  |       | File Folder       | 4/16/2003 11:48 AM |
| Office200_CD           |       | File Folder       | 2/25/2003 11:55 AM |
| Profiles               |       | File Folder       | 7/10/2003 2:48 PM  |
| Program Files          |       | File Folder       | 7/16/2003 11:32 AM |
| project                |       | File Folder       | 7/18/2003 12:27 PM |
| setecs                 |       | File Folder       | 2/19/2003 1:35 PM  |
| Temp                   |       | File Folder       | 7/24/2003 2:06 PM  |
| unzipped               |       | File Folder       | 7/21/2003 2:37 PM  |
| usr                    |       | File Folder       | 5/6/2003 12:02 PM  |
| WINDOWS                |       | File Folder       | 7/17/2003 11:23 AM |
| Windows CE Tools       |       | File Folder       | 2/25/2003 11:36 AM |
| wt170                  |       | File Folder       | 7/1/2003 4:00 PM   |
| hello.bat              | 1 KB  | MS-DOS Batch File | 7/3/2003 11:35 AM  |
| hello.class            | 1 KB  | CLASS File        | 7/8/2003 4:11 PM   |
| hello.h                | 1 KB  | C Header file     | 7/3/2003 12:34 PM  |
| hello.java             | 1 KB  | JAVA File         | 7/8/2003 4:11 PM   |
| New Text Document.txt  | 1 KB  | Text Document     | 7/23/2003 6:14 PM  |
| s.bat                  | 1 KB  | MS-DOS Batch File | 6/16/2003 3:04 PM  |
| winzip.log             | 12 KB | Text Document     | 7/21/2003 2:37 PM  |
| hello.bat.p7s          | 9 KB  | PKCS #7 Signature | 7/24/2003 2:15 PM  |
| hello.class.p7s        | 0 KB  | PKCS #7 Signature | 7/24/2003 2:15 PM  |
| hello.class.p7s        | 10 KB | PKCS #7 Signature | 7/24/2003 2:15 PM  |

33 objects (Disk free space: 3.57 GB)      31.0 KB      My Computer

Start    Debug - OneSEC...    OneSEC Security ...    C:\    2:26 PM



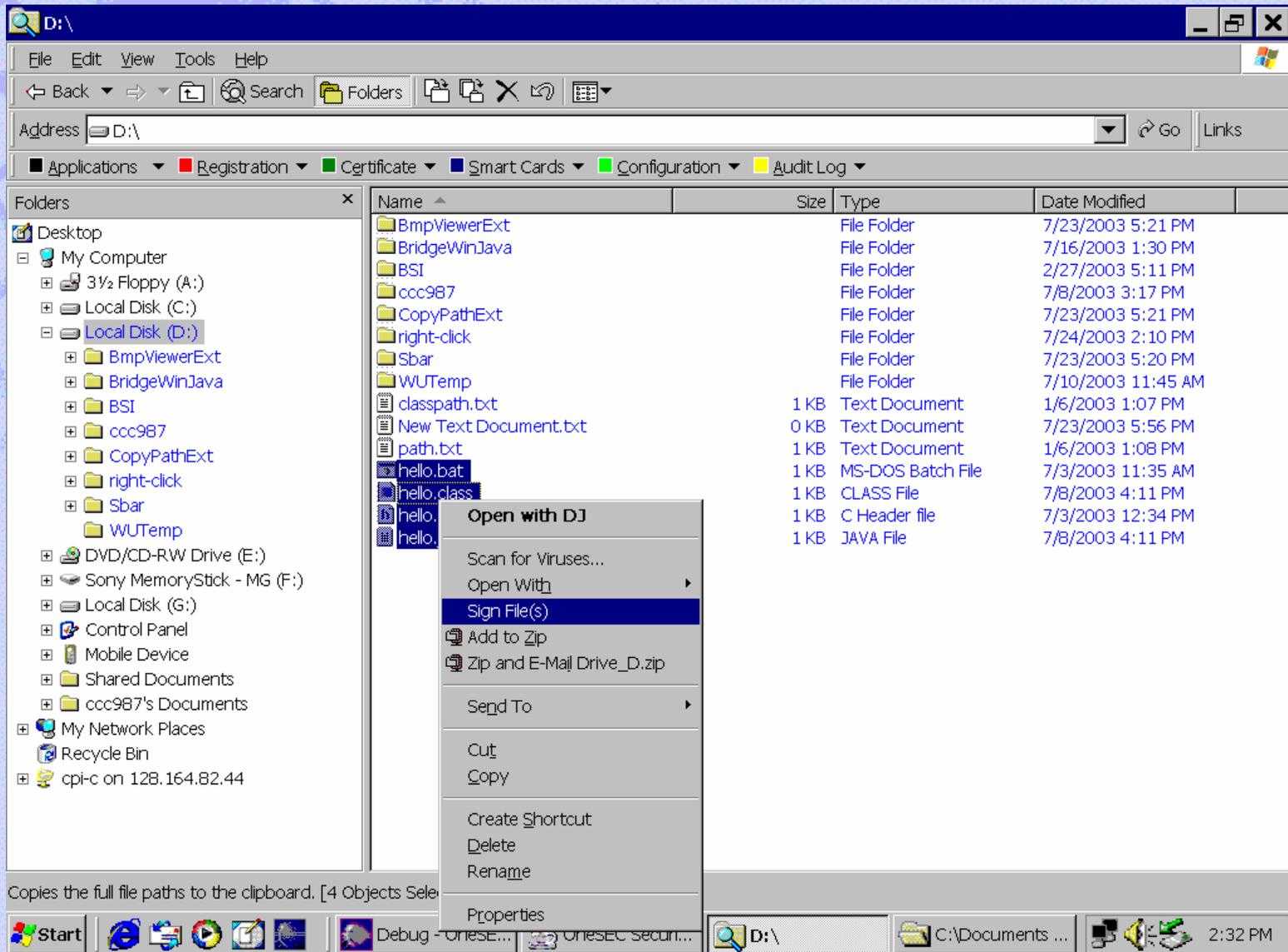


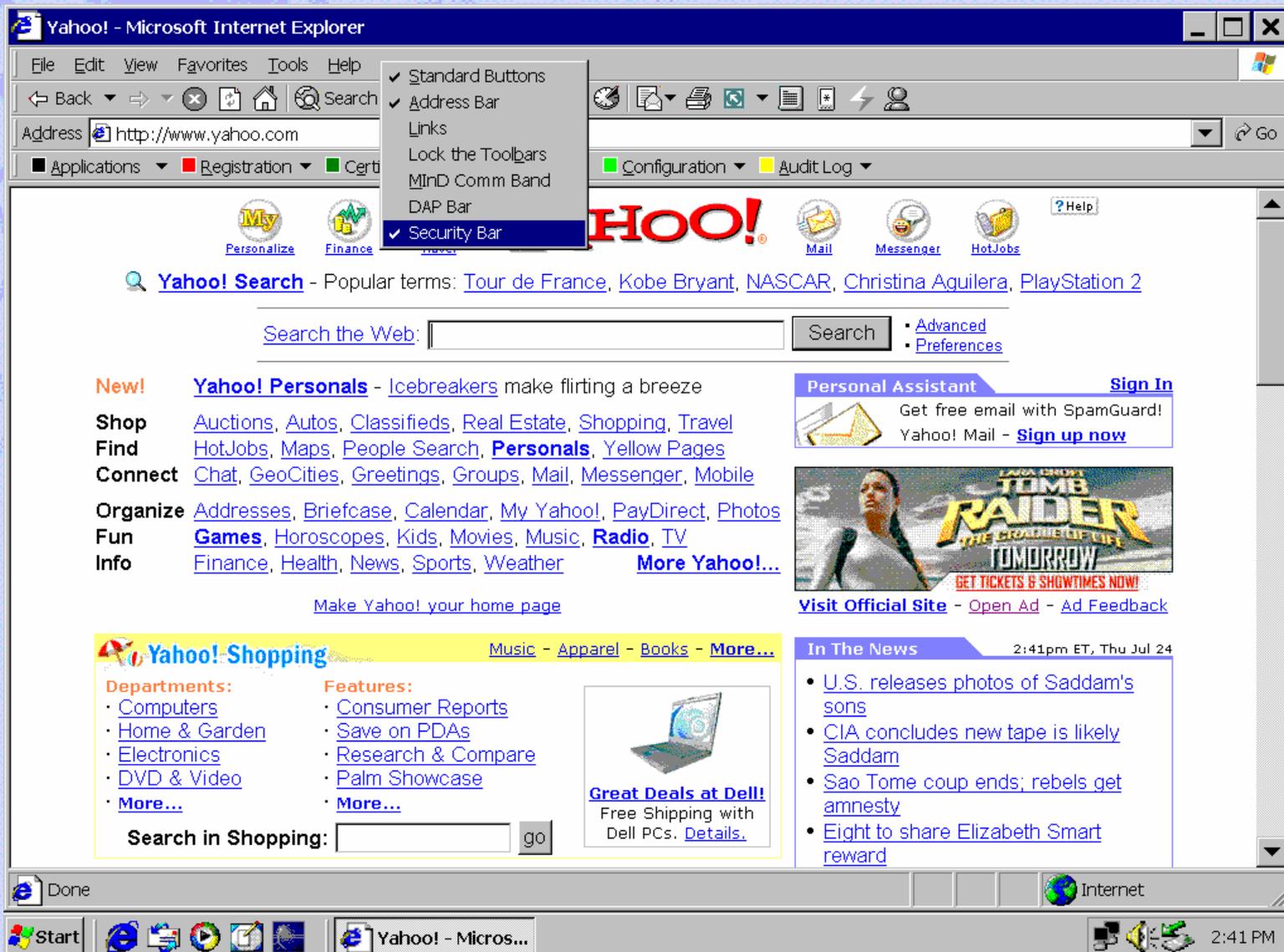
The screenshot shows a Windows Explorer window displaying the contents of the C:\ drive. A context menu is open over the 'OneNet' folder, showing sub-items: 'Administration' and 'Client'. The main pane lists various folders and files, including 'Documents and Settings', 'eclipse', 'gs', 'IBM', 'IDSSystem', 'Inetpub', 'j2sdk1.4.2', 'lib', 'mysql', 'Office200\_CD', 'Profiles', 'Program Files', 'project', 'setecs', 'Temp', 'unzipped', 'usr', 'WINDOWS', 'Windows CE Tools', 'wtl70', and several files like 'hello.bat', 'hello.class', 'hello.h', 'hello.java', 'New Text Document.txt', 's.bat', 'winzip.log', and PKCS #7 Signatures.

| Name                   | Size  | Type              | Date Modified      |
|------------------------|-------|-------------------|--------------------|
| Documents and Settings |       | File Folder       | 7/16/2003 1:08 PM  |
| eclipse                |       | File Folder       | 7/11/2003 3:46 PM  |
| gs                     |       | File Folder       | 1/17/2003 1:12 PM  |
| IBM                    |       | File Folder       | 3/15/2003 5:42 PM  |
| IDSSystem              |       | File Folder       | 7/11/2003 4:29 PM  |
| Inetpub                |       | File Folder       | 7/9/2003 2:53 PM   |
| j2sdk1.4.2             |       | File Folder       | 7/9/2003 2:48 PM   |
| lib                    |       | File Folder       | 4/23/2003 4:21 PM  |
| mysql                  |       | File Folder       | 4/16/2003 11:48 AM |
| Office200_CD           |       | File Folder       | 2/25/2003 11:55 AM |
| Profiles               |       | File Folder       | 7/10/2003 2:48 PM  |
| Program Files          |       | File Folder       | 7/16/2003 11:32 AM |
| project                |       | File Folder       | 7/18/2003 12:27 PM |
| setecs                 |       | File Folder       | 2/19/2003 1:35 PM  |
| Temp                   |       | File Folder       | 7/24/2003 2:06 PM  |
| unzipped               |       | File Folder       | 7/21/2003 2:37 PM  |
| usr                    |       | File Folder       | 5/6/2003 12:02 PM  |
| WINDOWS                |       | File Folder       | 7/17/2003 11:23 AM |
| Windows CE Tools       |       | File Folder       | 2/25/2003 11:36 AM |
| wtl70                  |       | File Folder       | 7/1/2003 4:00 PM   |
| hello.bat              | 1 KB  | MS-DOS Batch File | 7/3/2003 11:35 AM  |
| hello.class            | 1 KB  | CLASS File        | 7/8/2003 4:11 PM   |
| hello.h                | 1 KB  | C Header file     | 7/3/2003 12:34 PM  |
| hello.java             | 1 KB  | JAVA File         | 7/8/2003 4:11 PM   |
| New Text Document.txt  | 1 KB  | Text Document     | 7/23/2003 6:14 PM  |
| s.bat                  | 1 KB  | MS-DOS Batch File | 6/16/2003 3:04 PM  |
| winzip.log             | 12 KB | Text Document     | 7/21/2003 2:37 PM  |
| hello.bat.p7s          | 9 KB  | PKCS #7 Signature | 7/24/2003 2:15 PM  |
| hello.class.p7s        | 0 KB  | PKCS #7 Signature | 7/24/2003 2:15 PM  |
| hello.h.p7s            | 10 KB | PKCS #7 Signature | 7/24/2003 2:15 PM  |

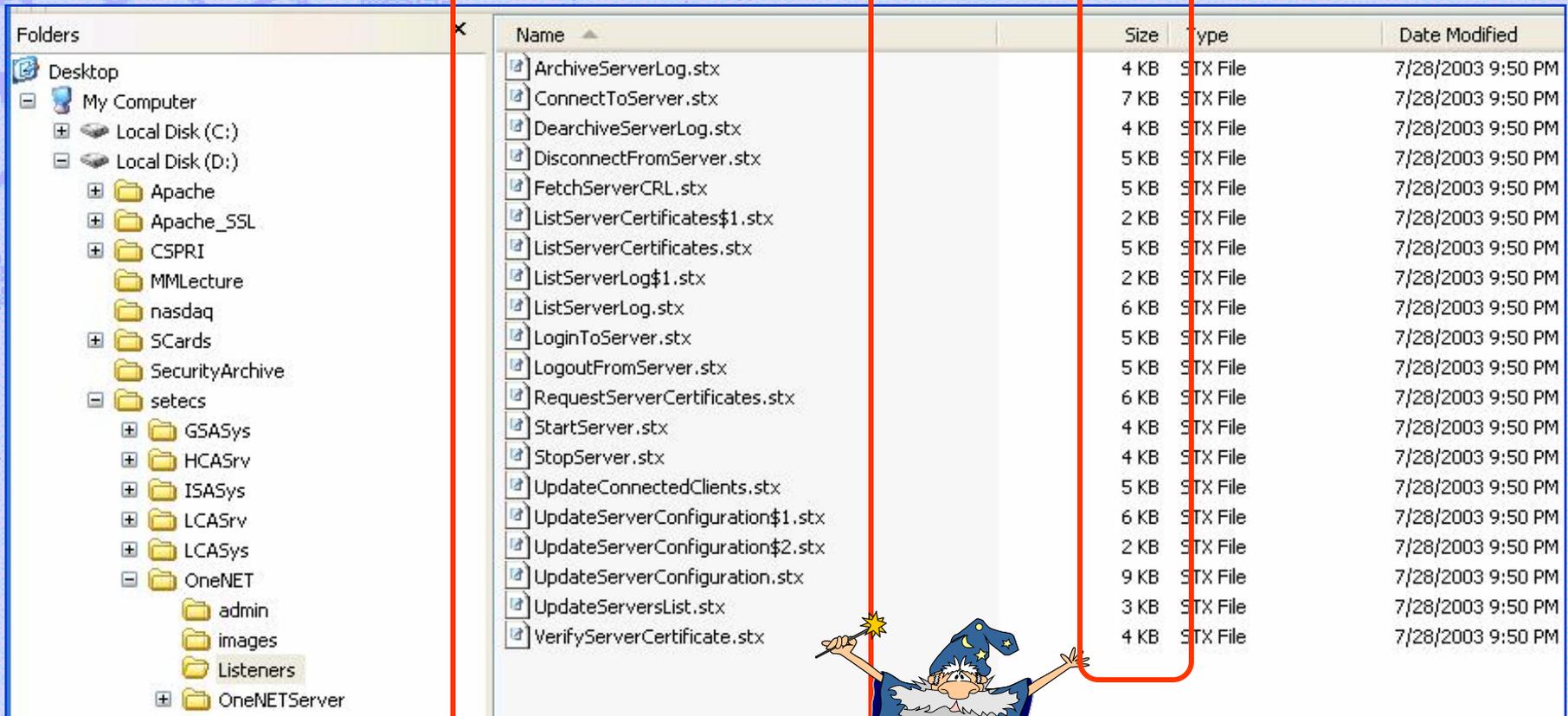
33 objects (Disk free space: 3.57 GB)      31.0 KB      My Computer

Start    Debug - OneSE...    OneSEC Securi...    C:\    C:\Documents ...    2:27 PM





The screenshot shows the Microsoft Internet Explorer browser window displaying the Yahoo! homepage. The 'Tools' menu is open, showing options like 'Standard Buttons', 'Address Bar', 'Links', 'Lock the Toolbars', 'MIND Comm Band', 'DAP Bar', and 'Security Bar'. The address bar shows 'http://www.yahoo.com'. The page content includes the Yahoo! logo, navigation links for Personalize, Finance, Mail, Messenger, and HotJobs, a search bar, and various promotional banners for Yahoo! Personals, Personal Assistant, and Yahoo! Shopping. The Windows taskbar at the bottom shows the Start button and several open applications, including Internet Explorer.



The screenshot shows a Windows Explorer window with the following structure:

- Folders:** Desktop, My Computer, Local Disk (C:), Local Disk (D:), Apache, Apache\_SSL, CSPRI, MMLecture, nasdaq, SCards, SecurityArchive, setecs, GSASys, HCASrv, ISASys, LCASrv, LCASys, OneNET (admin, images, Listeners), OneNETServer.
- File List:**

| Name                             | Size | Type     | Date Modified     |
|----------------------------------|------|----------|-------------------|
| ArchiveServerLog.stx             | 4 KB | STX File | 7/28/2003 9:50 PM |
| ConnectToServer.stx              | 7 KB | STX File | 7/28/2003 9:50 PM |
| DearchiveServerLog.stx           | 4 KB | STX File | 7/28/2003 9:50 PM |
| DisconnectFromServer.stx         | 5 KB | STX File | 7/28/2003 9:50 PM |
| FetchServerCRL.stx               | 5 KB | STX File | 7/28/2003 9:50 PM |
| ListServerCertificates\$1.stx    | 2 KB | STX File | 7/28/2003 9:50 PM |
| ListServerCertificates.stx       | 5 KB | STX File | 7/28/2003 9:50 PM |
| ListServerLog\$1.stx             | 2 KB | STX File | 7/28/2003 9:50 PM |
| ListServerLog.stx                | 6 KB | STX File | 7/28/2003 9:50 PM |
| LoginToServer.stx                | 5 KB | STX File | 7/28/2003 9:50 PM |
| LogoutFromServer.stx             | 5 KB | STX File | 7/28/2003 9:50 PM |
| RequestServerCertificates.stx    | 6 KB | STX File | 7/28/2003 9:50 PM |
| StartServer.stx                  | 4 KB | STX File | 7/28/2003 9:50 PM |
| StopServer.stx                   | 4 KB | STX File | 7/28/2003 9:50 PM |
| UpdateConnectedClients.stx       | 5 KB | STX File | 7/28/2003 9:50 PM |
| UpdateServerConfiguration\$1.stx | 6 KB | STX File | 7/28/2003 9:50 PM |
| UpdateServerConfiguration\$2.stx | 2 KB | STX File | 7/28/2003 9:50 PM |
| UpdateServerConfiguration.stx    | 9 KB | STX File | 7/28/2003 9:50 PM |
| UpdateServersList.stx            | 3 KB | STX File | 7/28/2003 9:50 PM |
| VerifyServerCertificate.stx      | 4 KB | STX File | 7/28/2003 9:50 PM |

## Security Framework :

- Concept (how to solve the problem)

**By creating a set of generic security modules for the most common security components, functions, and protocols and integrating them with existing (standard) and new (custom-developed) applications**

- Methodology (approach to use the concept)

**Templates for new applications, procedure for integration with standard applications, and transparent invocation**

- Set of components (Dev Toolkit, plus run-time platform)

**Crypto objects, security protocols, ready-made client/server components, and several available applications**

## Internet Security Infrastructure

Collection of components, protocols, functions and interfaces for support of secure Internet applications

## SETECS Security Framework

Collection of methods, tools, components and interfaces for rapid and standardized design and development of secure Internet applications



## SETECS Secure Applications

Customized secure Internet applications built using Security Framework and supported by Security Infrastructure

**Example : Integrated, global, end-to-end  
Web-based secure applications**

## SETECS Products :

### OneCARD™

Smart cards middleware system supporting Java and file cards, compliant with OCF, GSA, CAC, and ISO 7816 standards

### OneManager™

Security Administration and Management  
(Registration DB, LDAP Directory, smart cards)

### OnePKI™

Full PKI: Top Level CA Server  
Policy CA Server  
Hierarchy CA Server  
Local CA Server

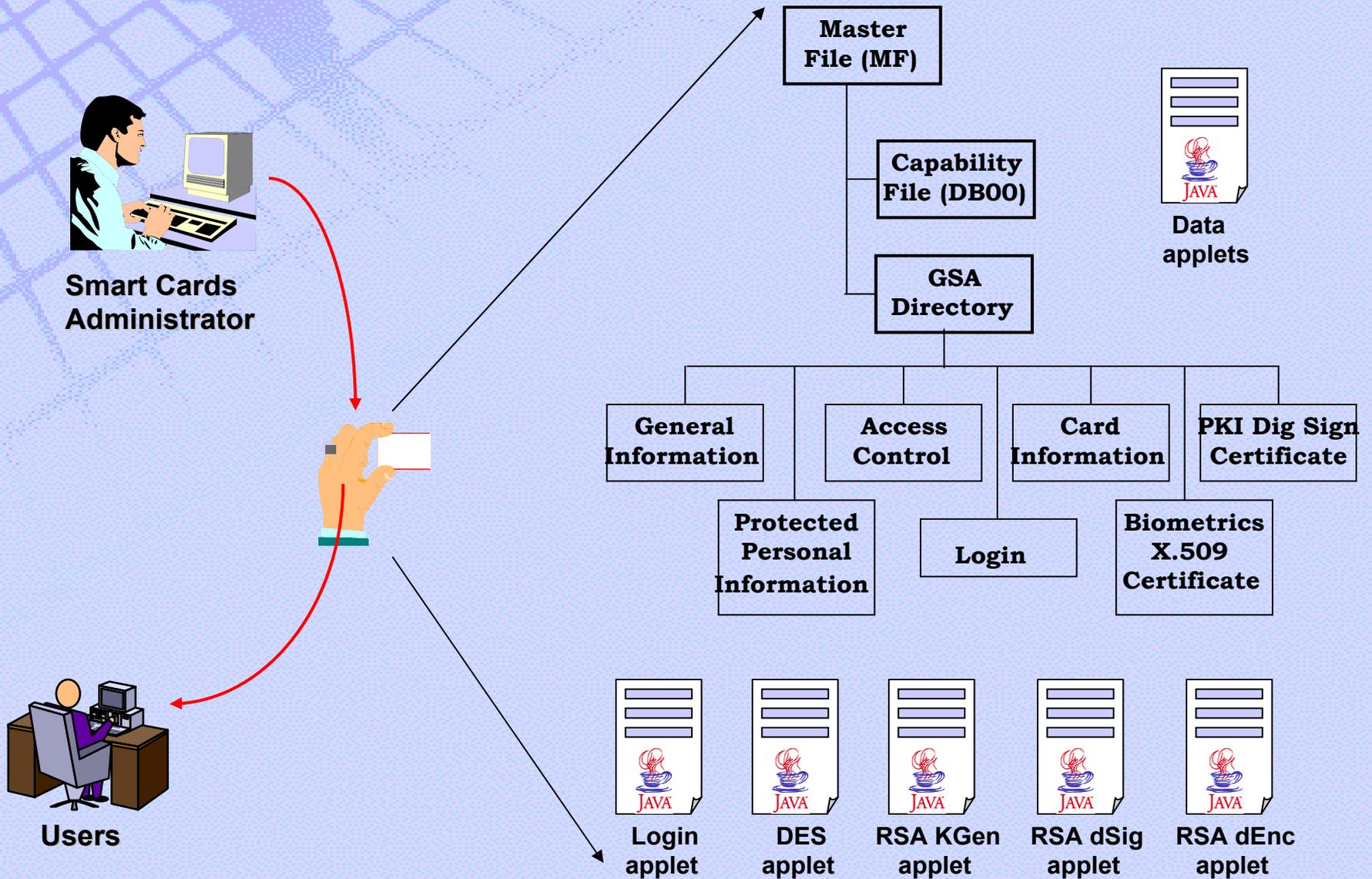
### OneNET™

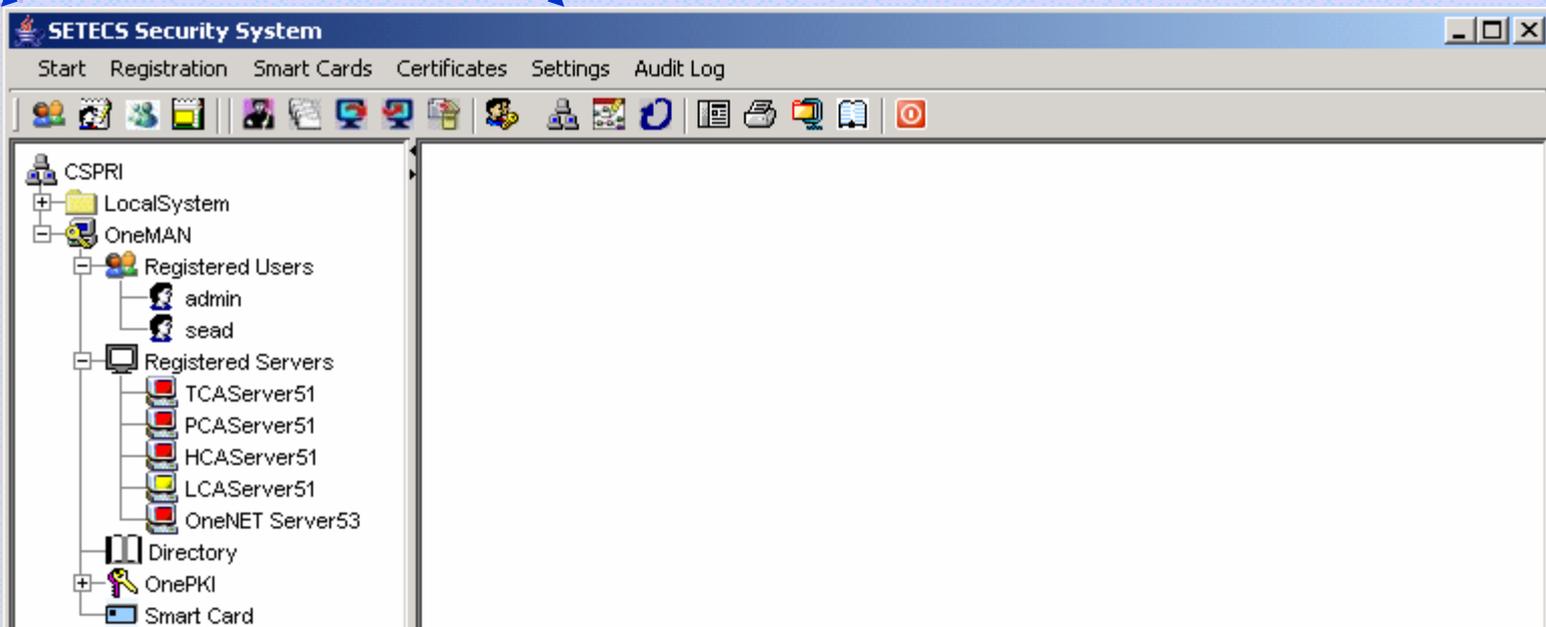
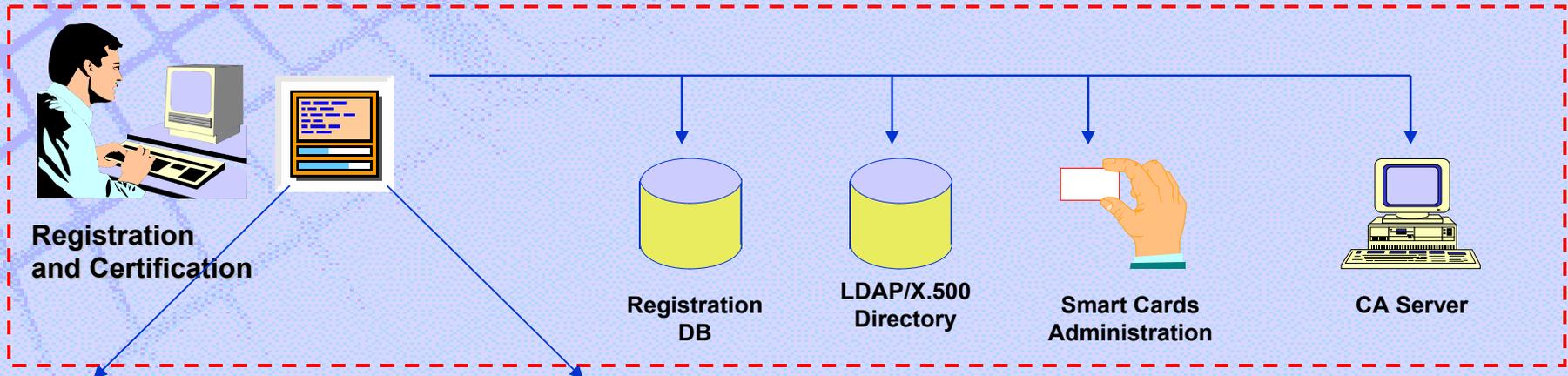
Client/server security system  
(Secure E-mail, SSL, SMIME, Java Security, WSS Security Server, OASSIS SAML Server)

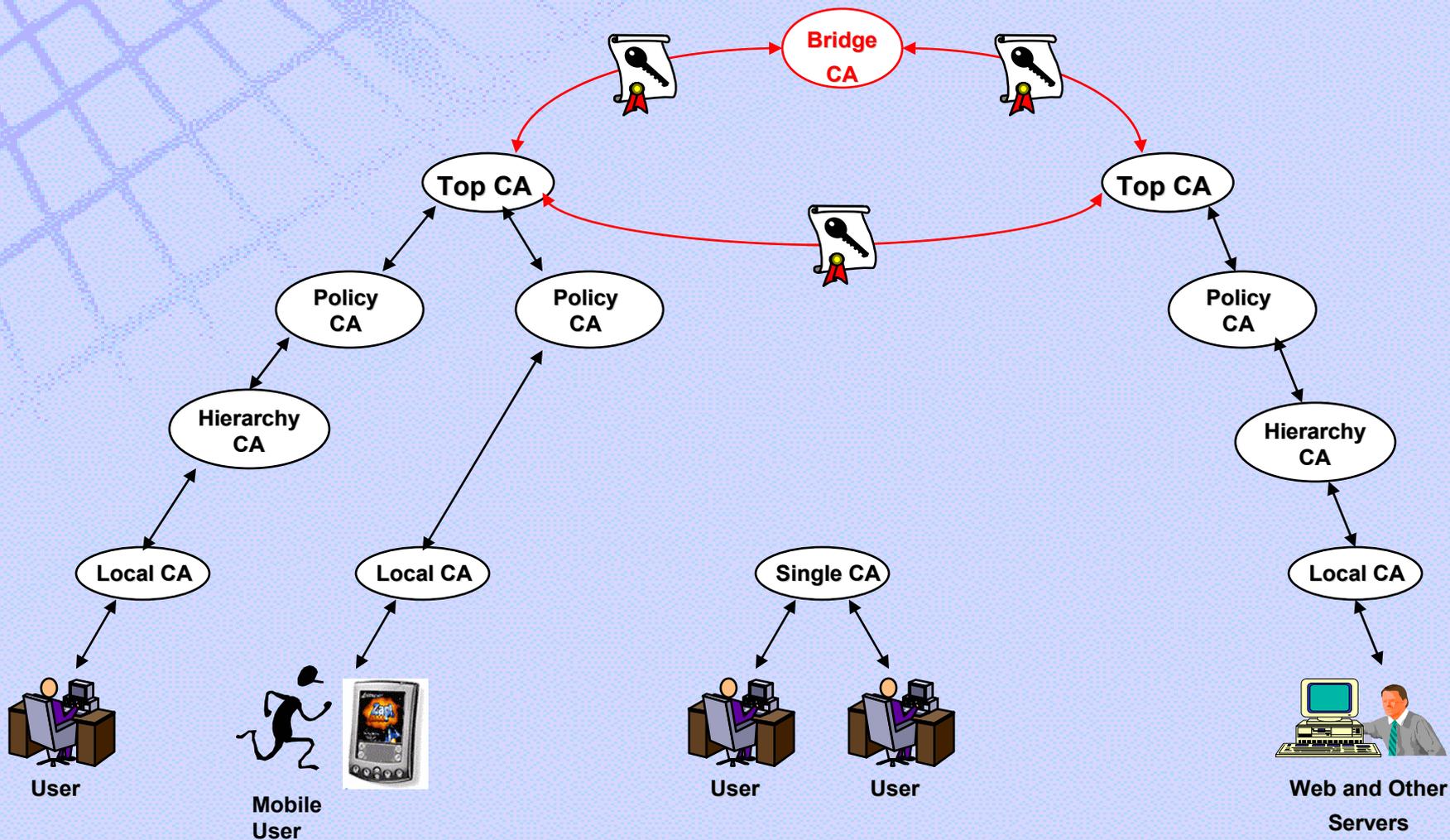
### OneGroup™

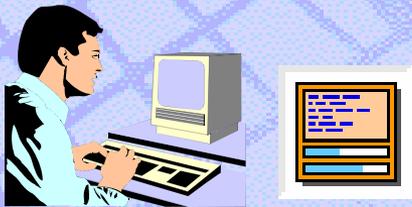
Group Security System compliant to GSAKMP standard  
(secure instant messaging, whiteboard, shared documents)



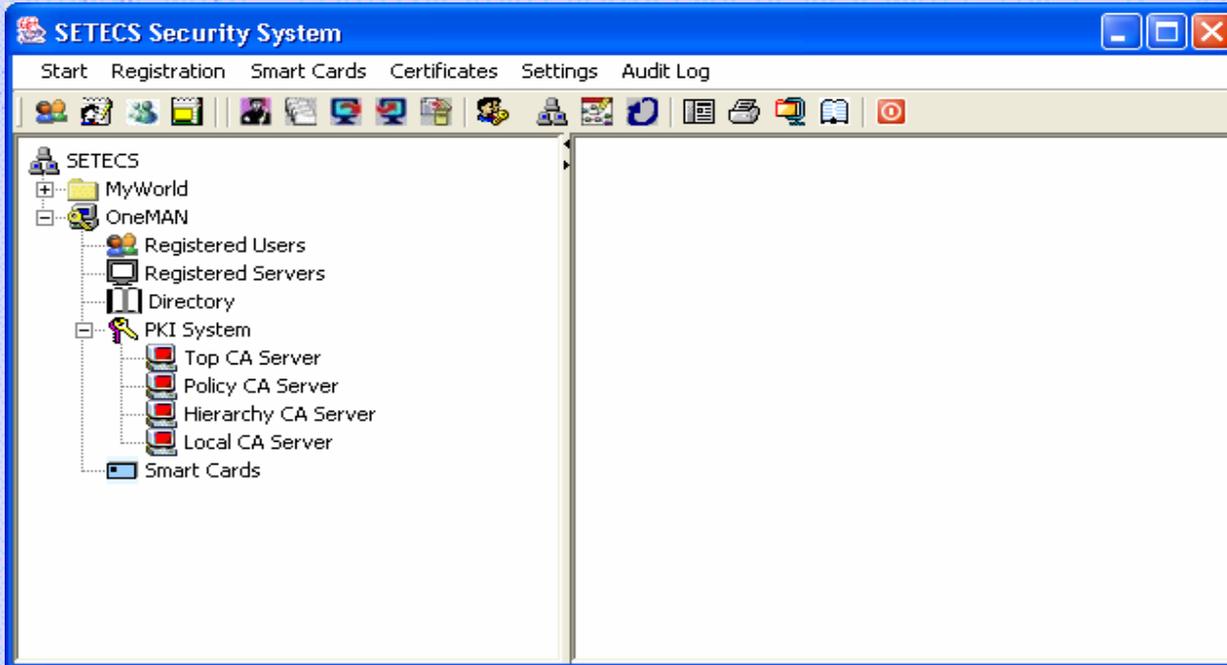
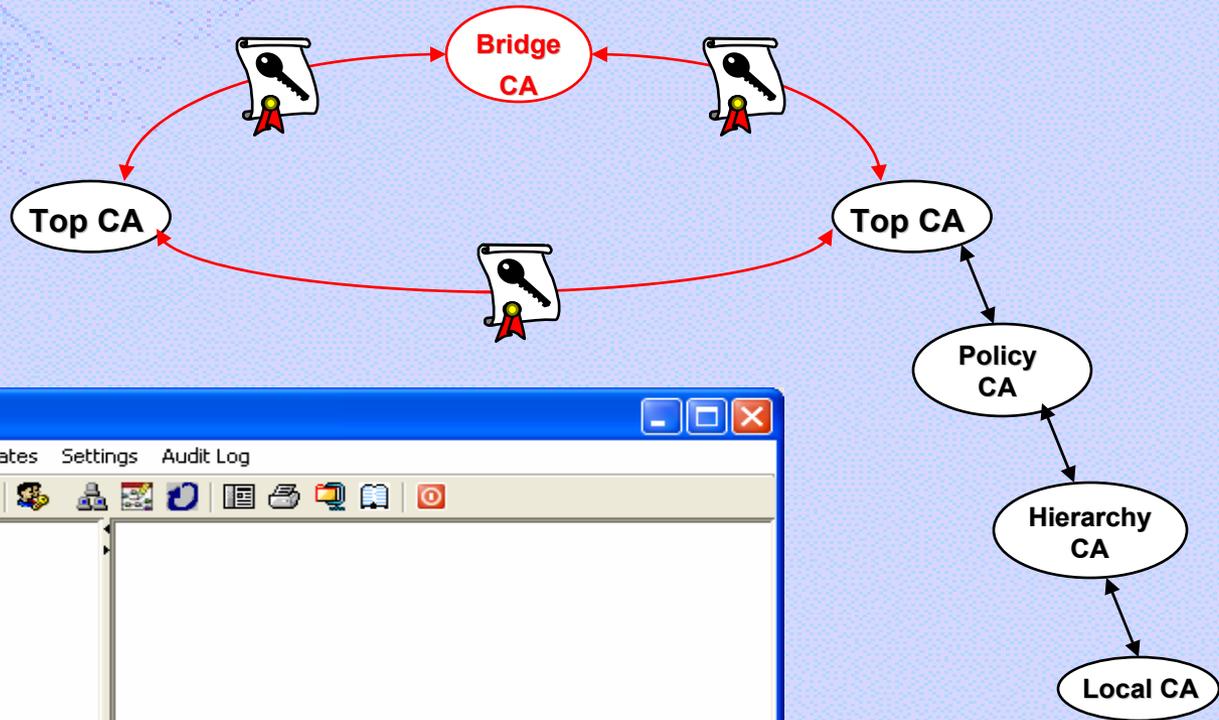


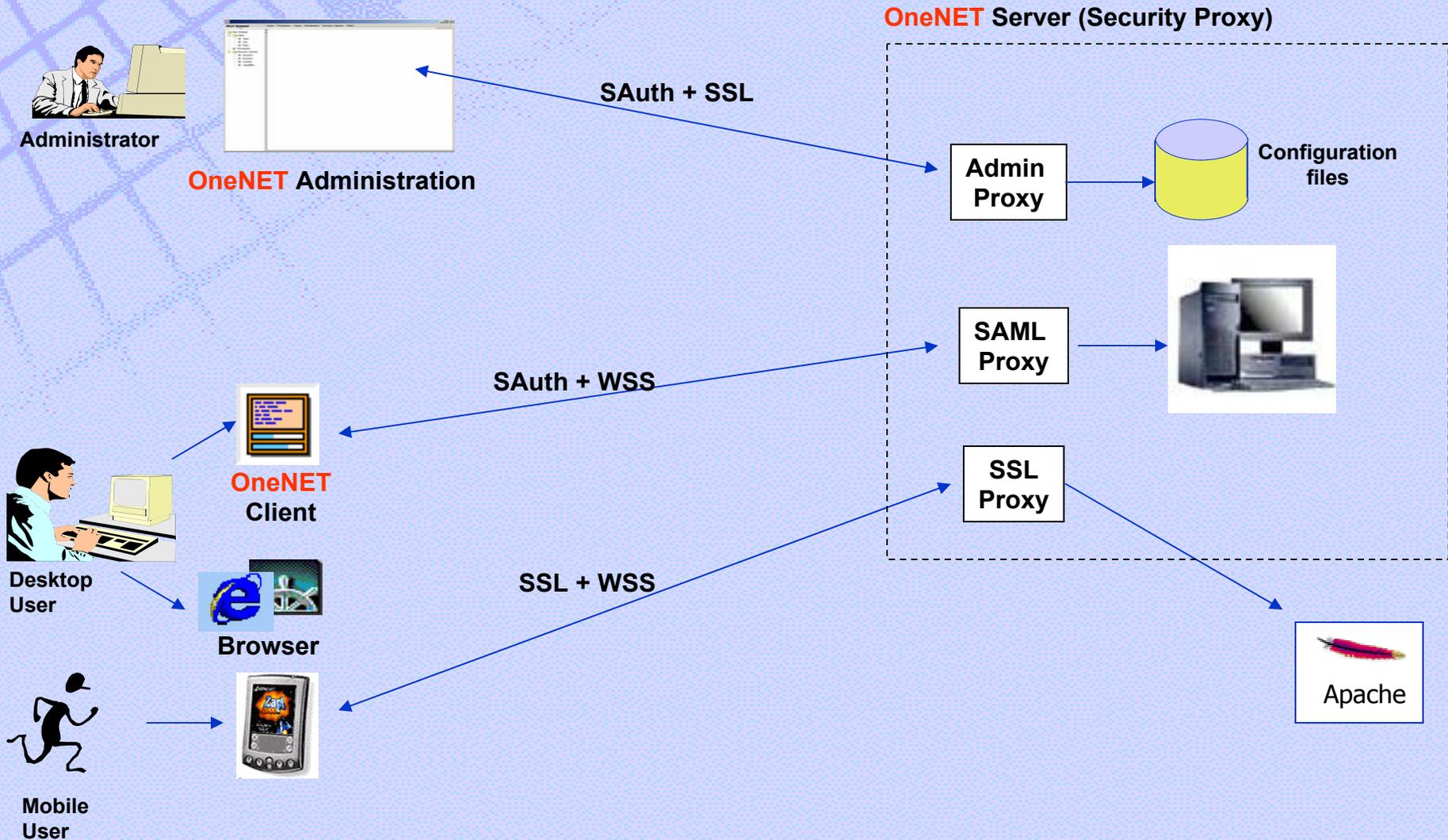


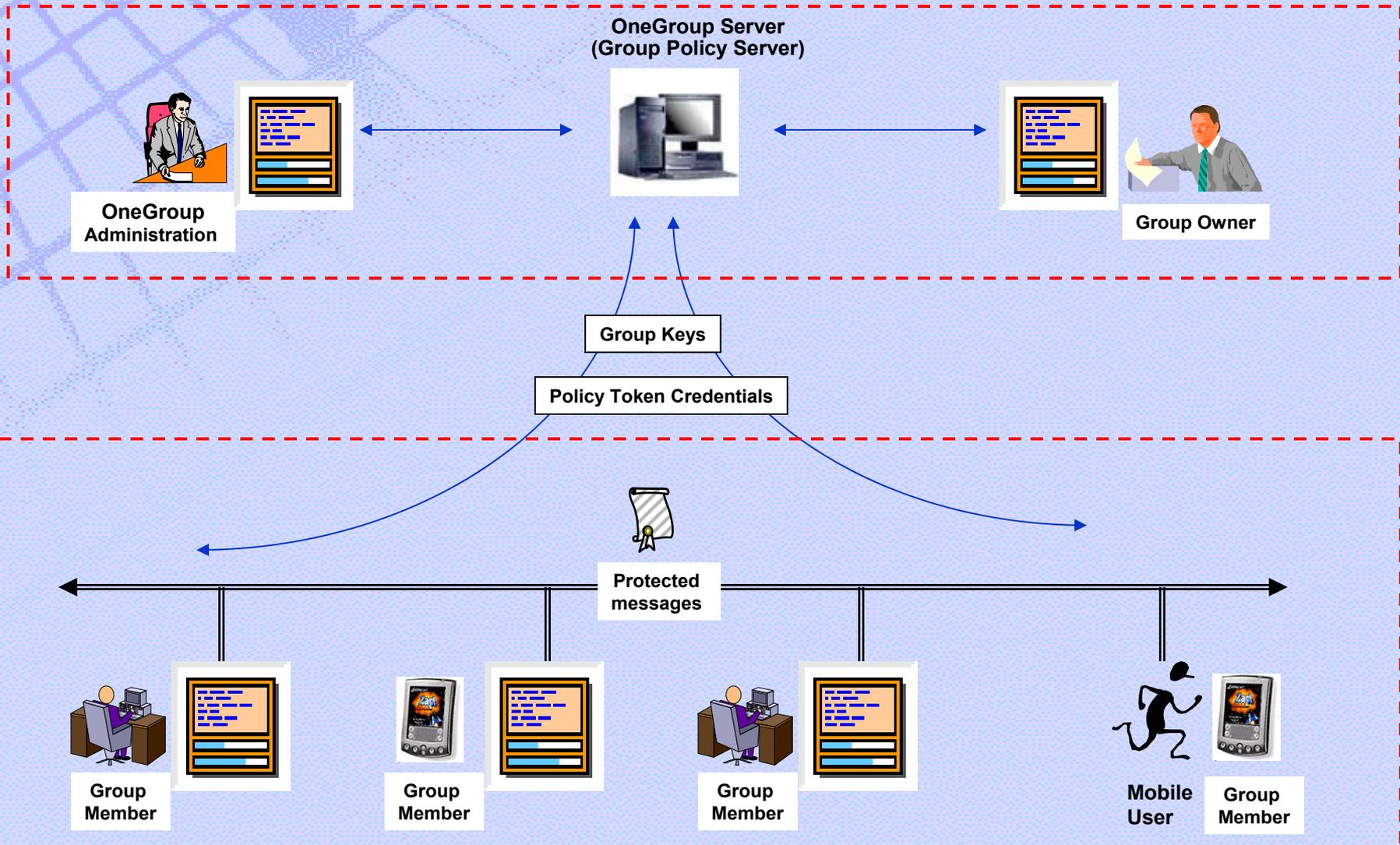


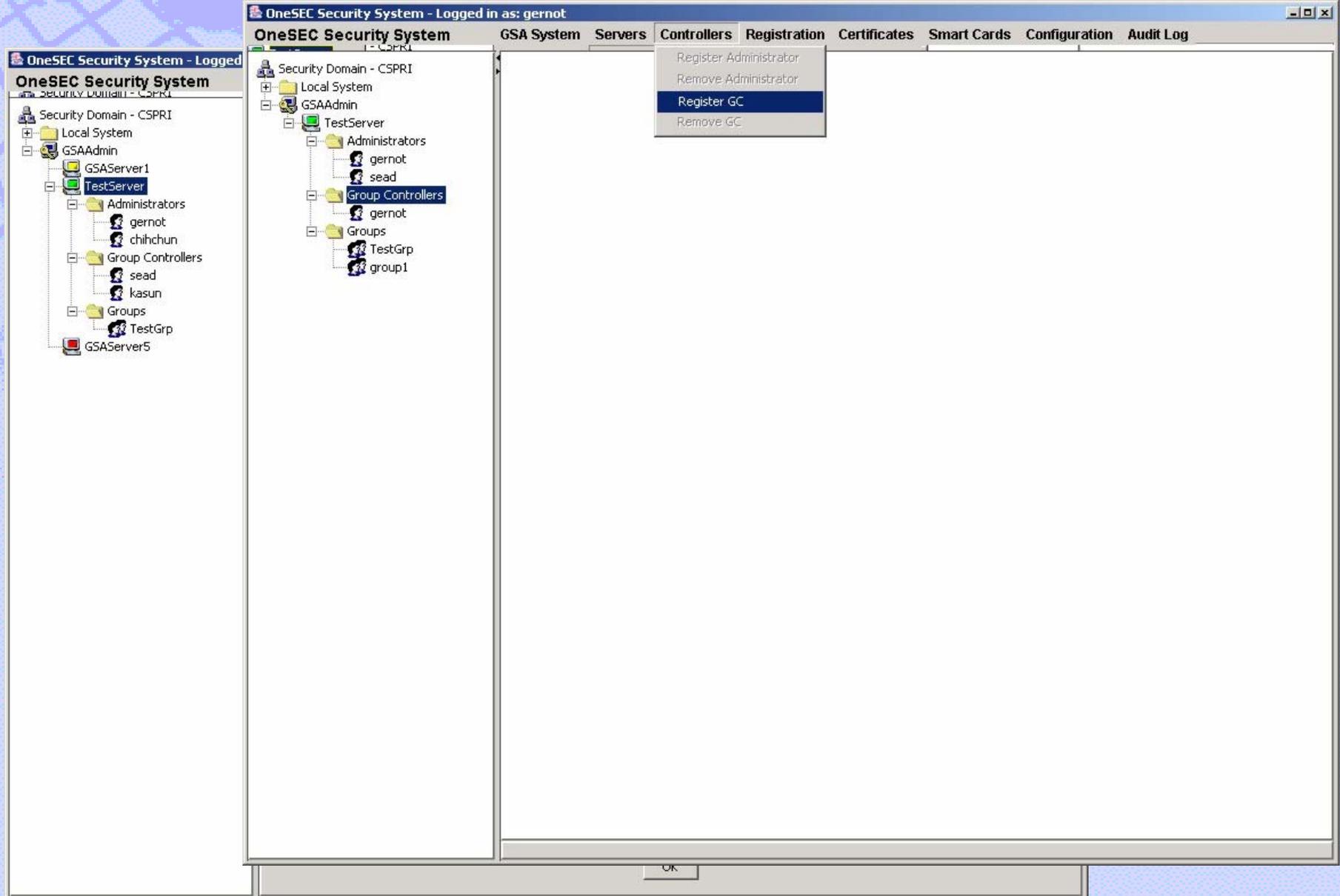


PKI Administration Interface (**OneMAN**)









The screenshot displays the OneSEC Security System administration console. The interface is titled "OneSEC Security System - Logged in as: gernot". The main window has a menu bar with the following items: "OneSEC Security System", "GSA System", "Servers", "Controllers", "Registration", "Certificates", "Smart Cards", "Configuration", and "Audit Log".

The left sidebar shows a tree view of the system structure:

- Security Domain - CSPRI
  - Local System
    - GSAAdmin
      - GSA Server 1
      - TestServer
        - Administrators
          - gernot
          - chihchun
        - Group Controllers
          - sead
          - kasun
        - Groups
          - TestGrp
        - GSA Server 5

## Internet Security Infrastructure

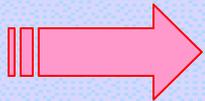
Collection of components, protocols, functions and interfaces for support of secure Internet applications

## SETECS Security Framework

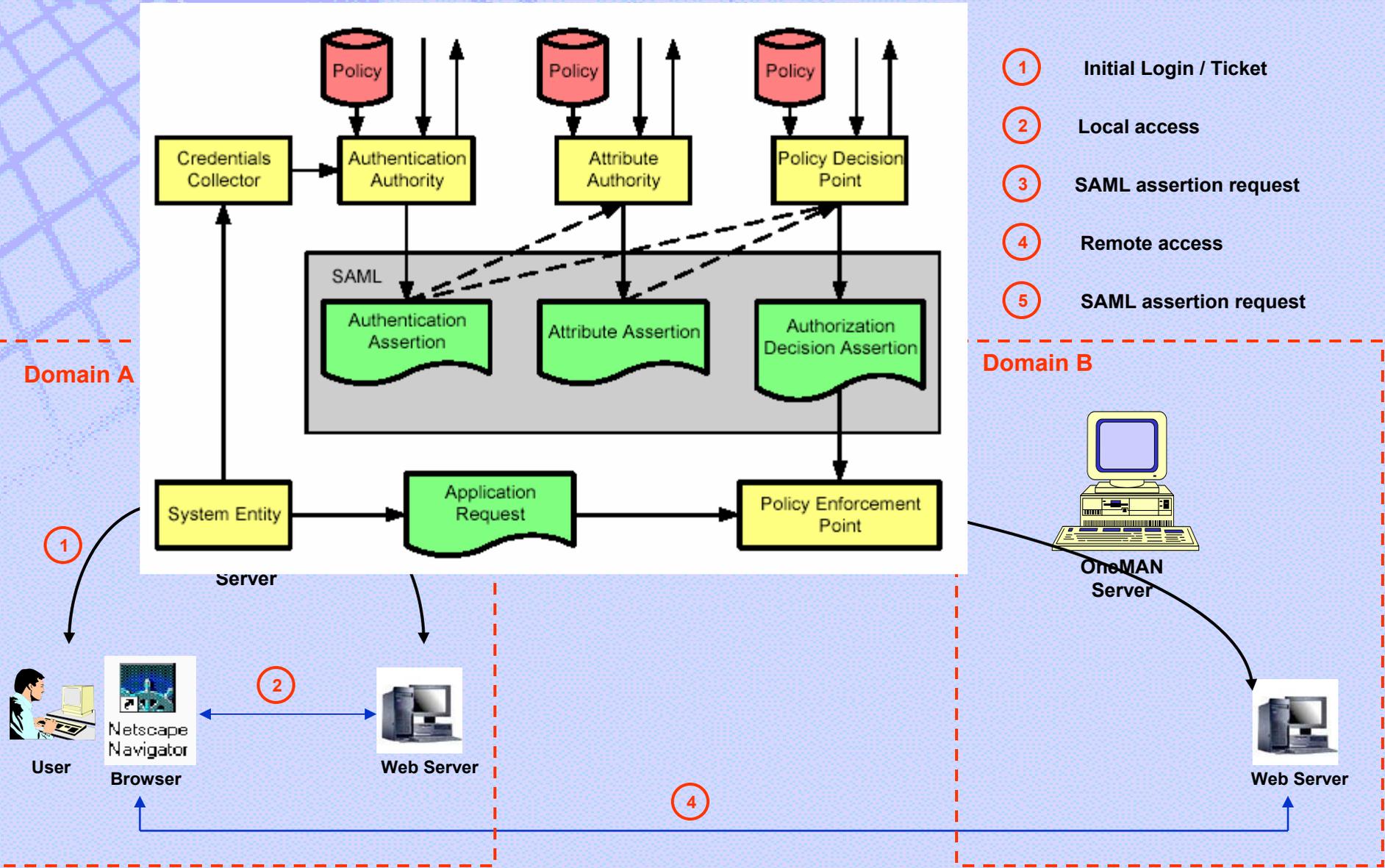
Collection of methods, tools, components and interfaces for rapid and standardized design and development of secure Internet applications

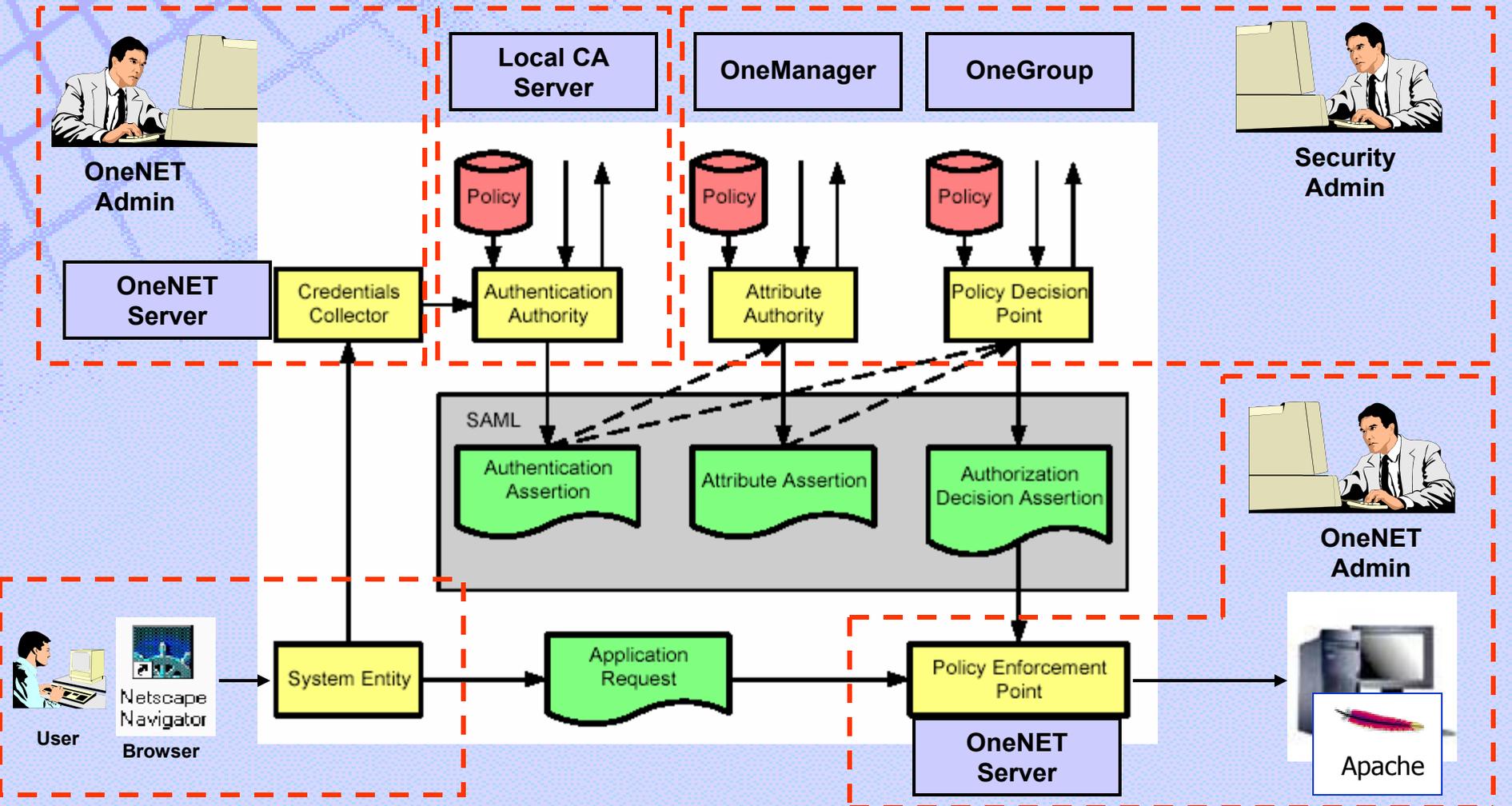
## SETECS Secure Applications

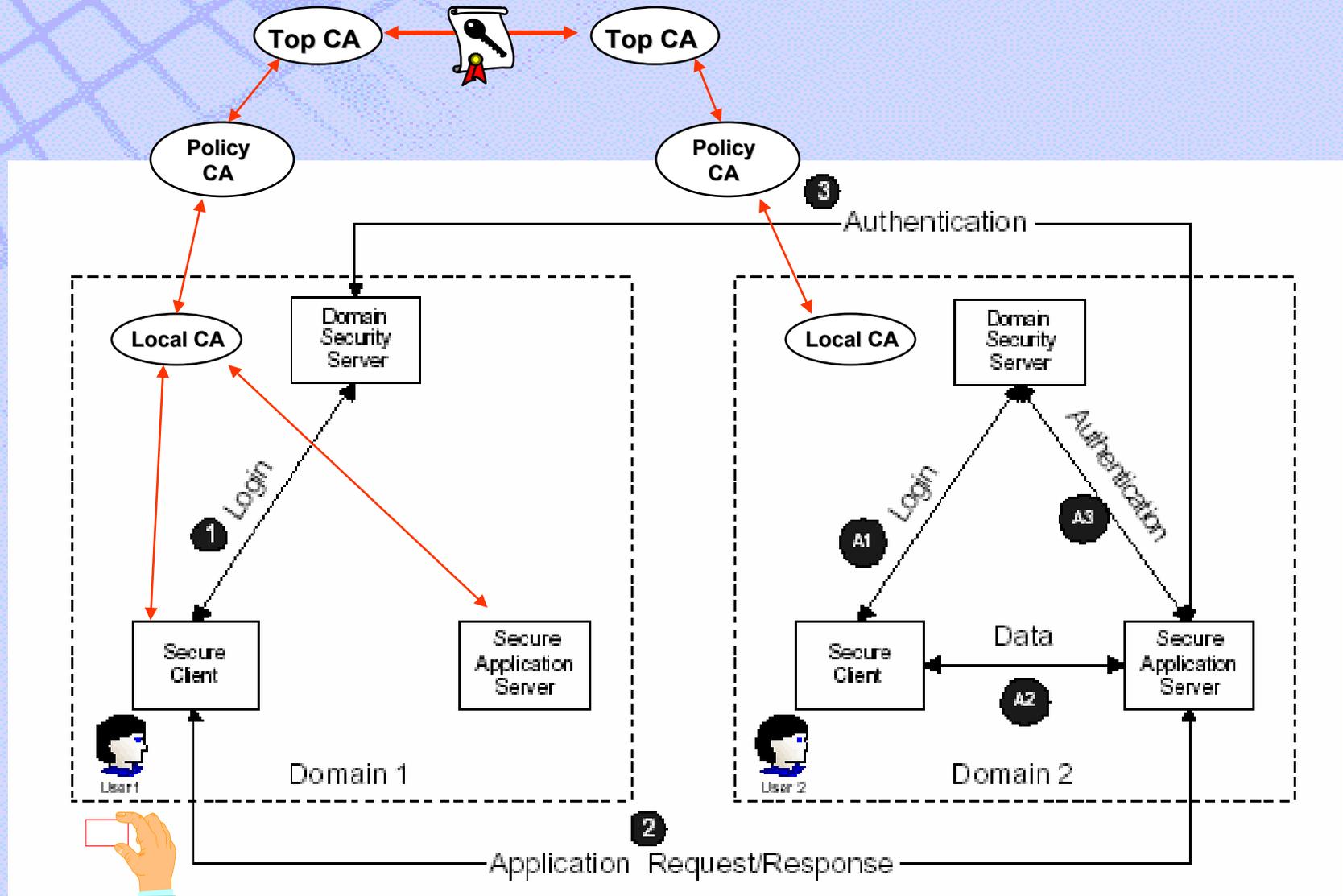
Customized secure Internet applications built using Security Framework and supported by Security Infrastructure



**Example : Integrated, global, end-to-end  
Web-based secure applications**









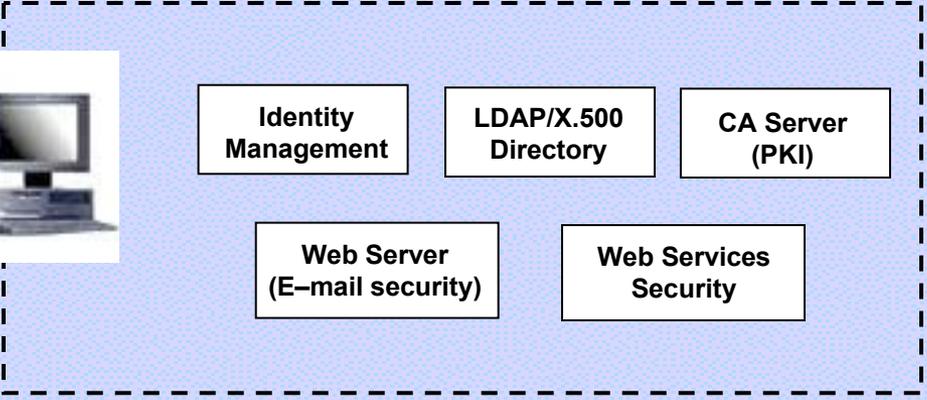
Sec Admin



Smart Cards Administration

**SC Vendors:**

- ActiveCard
- Gemplus
- G&D
- Schlumberger
- Oberthur



**PKI Vendors:**

- Entrust
- Verisign
- Baltimore
- beTrusted
- RSA Security

**WSS Vendors:**

- Netegrity
- Oblix
- DataPower
- RSA Security

**Clinet Vendors:**

- RSA Security
- Entruts
- SafeBoot
- PointSec

**Firewall:**

- Bluefire
- Intermec
- Certicom
- TrustDigital

**VPN Box:**

- NetScreen
- NOKIA
- Symantec
- Whale

Mobile Security



XML/SAML Protocol



Mobile Security

Web Services Security



SSL Protocol



Web Services Security

Group Security ~~X~~



GSA Protocol



Group Security ~~X~~



- All products implemented in Java (run on all platforms)
- Encrypted software modules (self-protected against viruses)
- Smart cards enabled
- Combined and integrated with SELinux RBAC policy
- Applicable to a federated environment (multiple security domains) through cross-certified PKIs
- Single (“Windows Explorer” – like) interface for all products
- Standards compliant (verification and interoperability)
- Supports GSAKMP standard for group key management

|                             | Initial cost<br>(\$000s) | Annual recurring<br>(\$000s) | Examples                             |
|-----------------------------|--------------------------|------------------------------|--------------------------------------|
| <b>Base platform</b>        |                          |                              |                                      |
| E-collaboration software    | 295-750                  | 55-115                       |                                      |
| Secure hosting              | 45-65                    | 550-745                      | ServerVault                          |
| Application server software | 35-50                    | 5-10                         | BEA WebLogic, Apache Tomcat          |
| Web server software         | 5-10                     | 2-5                          | Sun ONE (IPlanet), Apache HTTPD      |
| <b>Subtotal</b>             | <b>\$380-875</b>         | <b>\$612-875</b>             |                                      |
| <b>Security products</b>    |                          |                              |                                      |
| Data encryption software    | 165-220                  | 30-40                        | Evincible, ASI, Protegrity           |
| Client digital certificates | 160-215                  | 160-215                      | VeriSign, Entrust                    |
| Single sign-on software     | 85-115                   | 15-20                        | Netegrity SiteMinder, RSA ClearTrust |
| Encryption hardware         | 25-40                    | 5-10                         | nCipher, Chrysalis                   |
| <b>Subtotal</b>             | <b>\$435-590</b>         | <b>\$210-285</b>             |                                      |
| <b>Services</b>             |                          |                              |                                      |
| Security integration        | 295-750                  | -                            | @stake                               |
| Security testing            | 50-150                   | 60-85                        | @stake                               |
| <b>Subtotal</b>             | <b>\$345-900</b>         | <b>\$60-85</b>               |                                      |
| <b>Total</b>                | <b>\$1,160-2,365</b>     | <b>\$882-1,245</b>           |                                      |
| <b>Cost of Security</b>     | <b>\$790-1,490</b>       | <b>\$270-370</b>             |                                      |
| <b>SETECS</b>               | <b>\$190-220</b>         | <b>\$110-140</b>             |                                      |

*"Securing e-Collaboration", Andrew Jaquith, @stake, Inc., Dec 2002*

- **Over 70% cost reduction**
- **First with GSAKMP-based secure group applications**
- ***On-demand* security for mobile applications**

## **SETECS, Inc.**

### **Design, Development and Deployment of Secure Network Applications**

**Global, integrated, end-to-end security system  
for secure Web services, mobile devices, and  
collaborative group applications**

**March 2005**