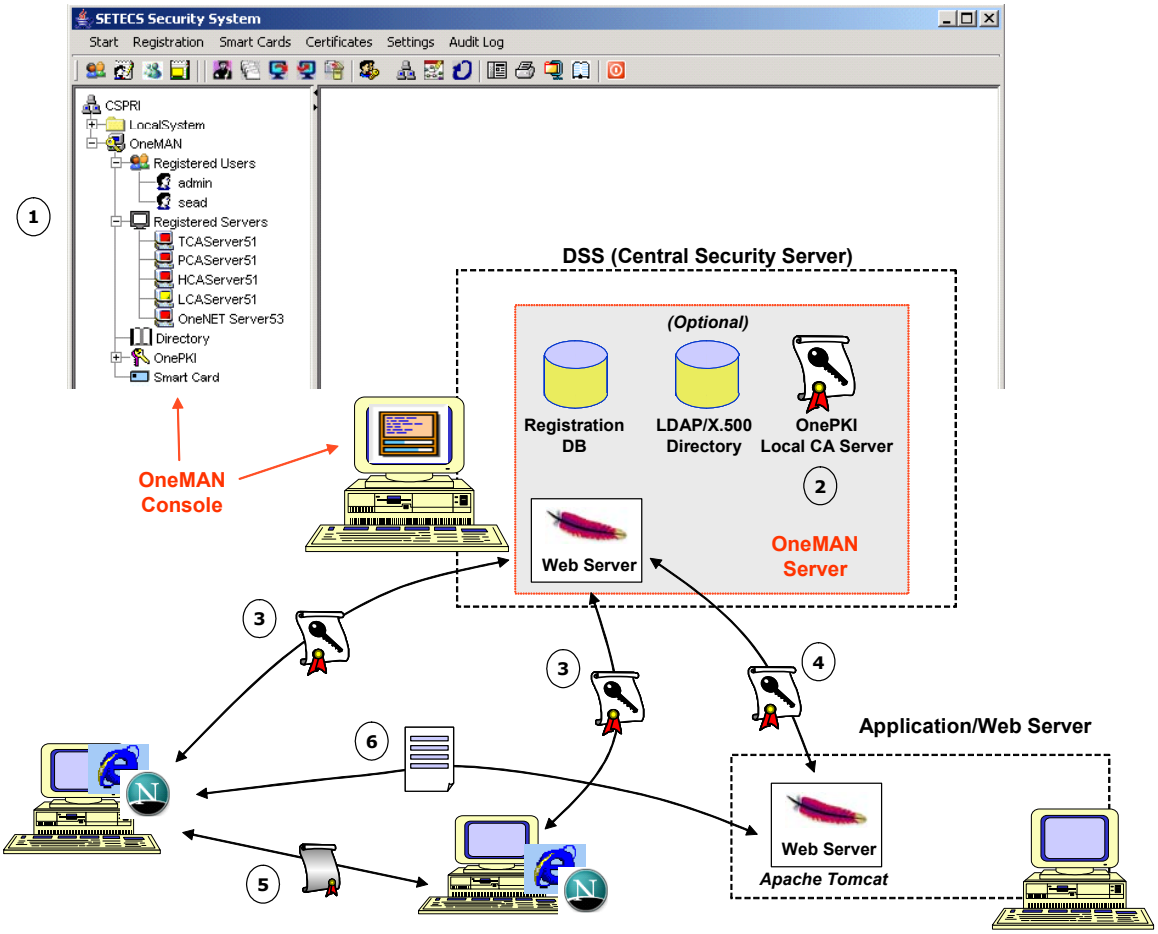
SETECS, Inc. *Internet Security Technologies*

Secure Enterprise Applications enabled by SETECS Security Infrastructure Products

1. Secure E–mail/Secure Web (SSL)
2. Secure Web Services: Identity Management, Single Sign–On, and Web Authorization
3. Public–Key Infrastructure
4. Smart Card Management and Applications: Windows Login, Secure E–mail, Secure Web (SSL)
5. Secure Group (Shared) Documents
6. Secure Collaborative Applications: Secure Instant Messaging and Secure Whiteboard
7. Secure Desktop

Secure E–mail/Secure Web (SSL)

User Needs	1. Protection of E–mail letters (signed and encrypted) 2. Secure browsing based on strong authentication and message protection
SETECS Products	1. OneMAN™ Server – Registration of users and Web servers, including OnePKI™ Local CA Server – Certification of users and Web servers (No installation on users' PCs or Web servers)
Activation	Start OneMAN™ server, register users and OnePKI™ Local CA server (step ①) and create self–signed certificates for OnePKI™ Local CA server (step ②)
Usage	Using a browser, access OnePKI™ Local CA server to get browser's certificate (step ③); request and receive Web server's certificate (step ④); use browser's certificate to create/send and receive/verify signed and encrypted E–mail letters (step ⑤); use browser's and Web server's certificates for secure browsing (SSL) (step ⑥)



Secure Web Services:

Identity Management, Single Sign–On, and Web Authorization

User Needs

1. Centralized identity and password management
2. Single sign–on (authentication) to multiple Web servers
3. Authorization for applications at multiple Web servers

SETECS Products

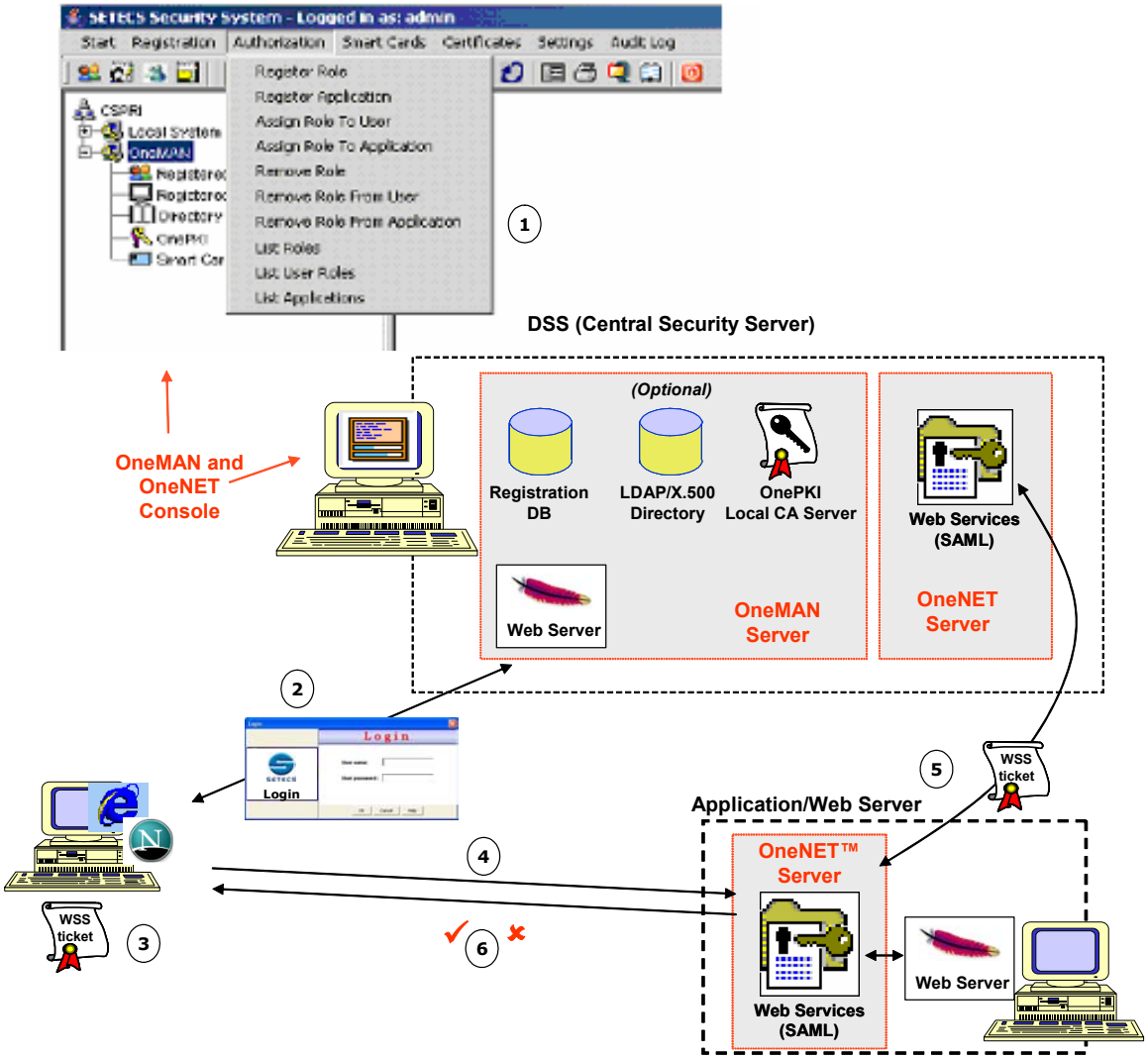
1. OneMAN™ Server including OnePKI™ Local CA server, as for Secure E–mail/Secure Web
2. OneNET™ Server at the Domain Security Server and at each Web server, including Client Applets. (No installation on users' PCs required)

Activation

After activation for secure E–mail/Web, register applications and roles at the OneMAN™ server, and assign roles to users and applications (step ①)

Usage

Using a browser, login to OneNET™ Server at the Domain Security Server (step ②), get Master Ticket for Web services (step ③); click to any other Web server (step ④); authentication is performed transparently by the central OneNET™ server using the Master Ticket – single sign-on (step ⑤); authorization is also performed by the central OneNET™ Server (step ⑤ and ⑥)



Public Key Infrastructure

User Needs

1. Support for multiple certification policies and assurance levels
2. Scaling to multiple domains and cross–certification with other PKIs
3. Distribution and verification of certificates using X.500 Directory system

SETECS Products

1. OneMAN™ Server – Registration and management of multiple CA servers, including OnePKI Local CA Server, as for Secure E-mail/Secure Web.
2. OnePKI™ Servers – Top (Root), Policy and Hierarchy servers

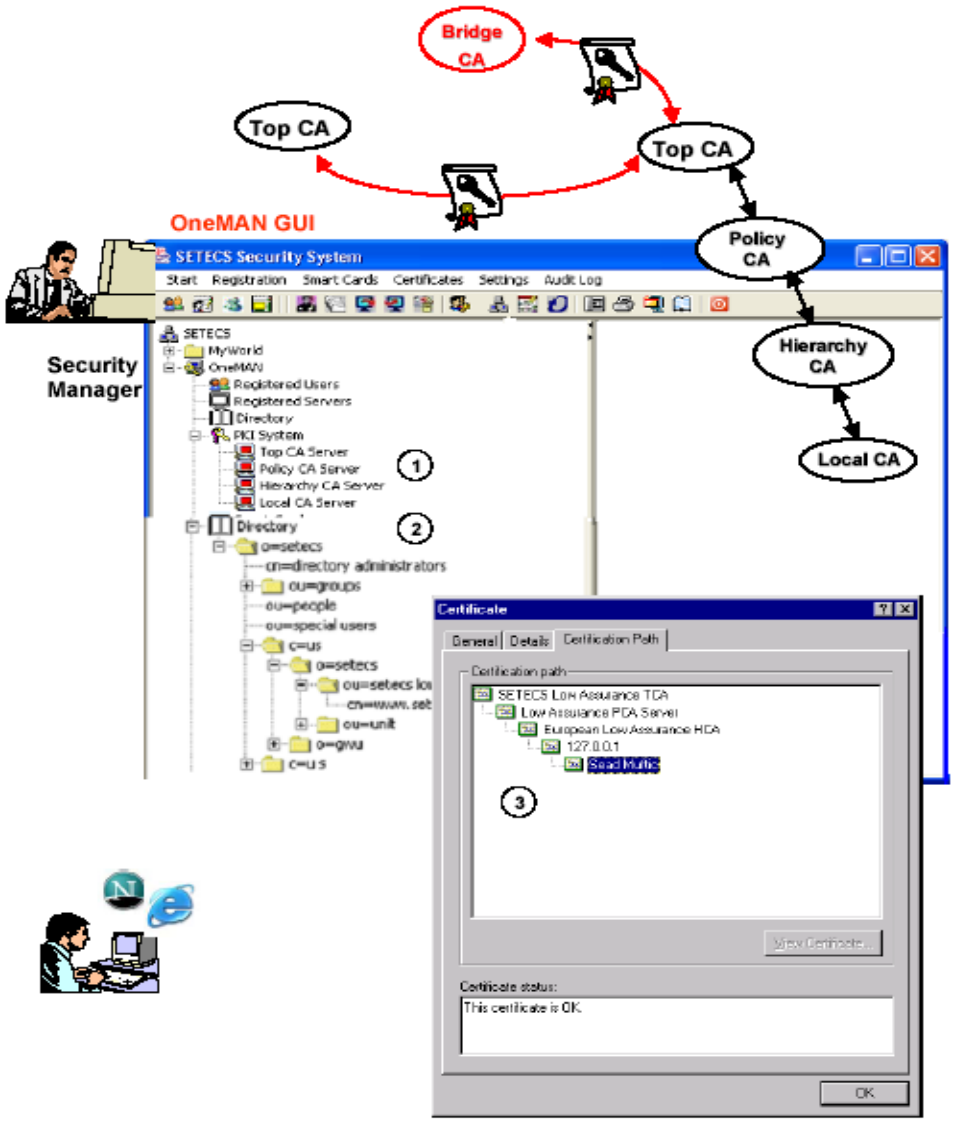
(No installation on users' PCs)

Activation

Start OneMAN™ Server, register four OnePKI™ CA servers (step ①); initiate PKI by create self–signed certificates for Top server and certificates for other CA servers; store certificates in the Directory (step ②)

Usage

For users, Web servers and OneNET™ servers usage is equivalent to secure E-mail/Web, except that certificates are processed in a hierarchy (step ③)



Smart Card Applications:

Windows Login, Secure E–mail, Secure Web (SSL)

User Needs

1. Issuing of smart cards in combination with certificates
2. Local and remote login using smart card
3. Secure E-mail and secure Web (browser) using smart cards

SETECS Products

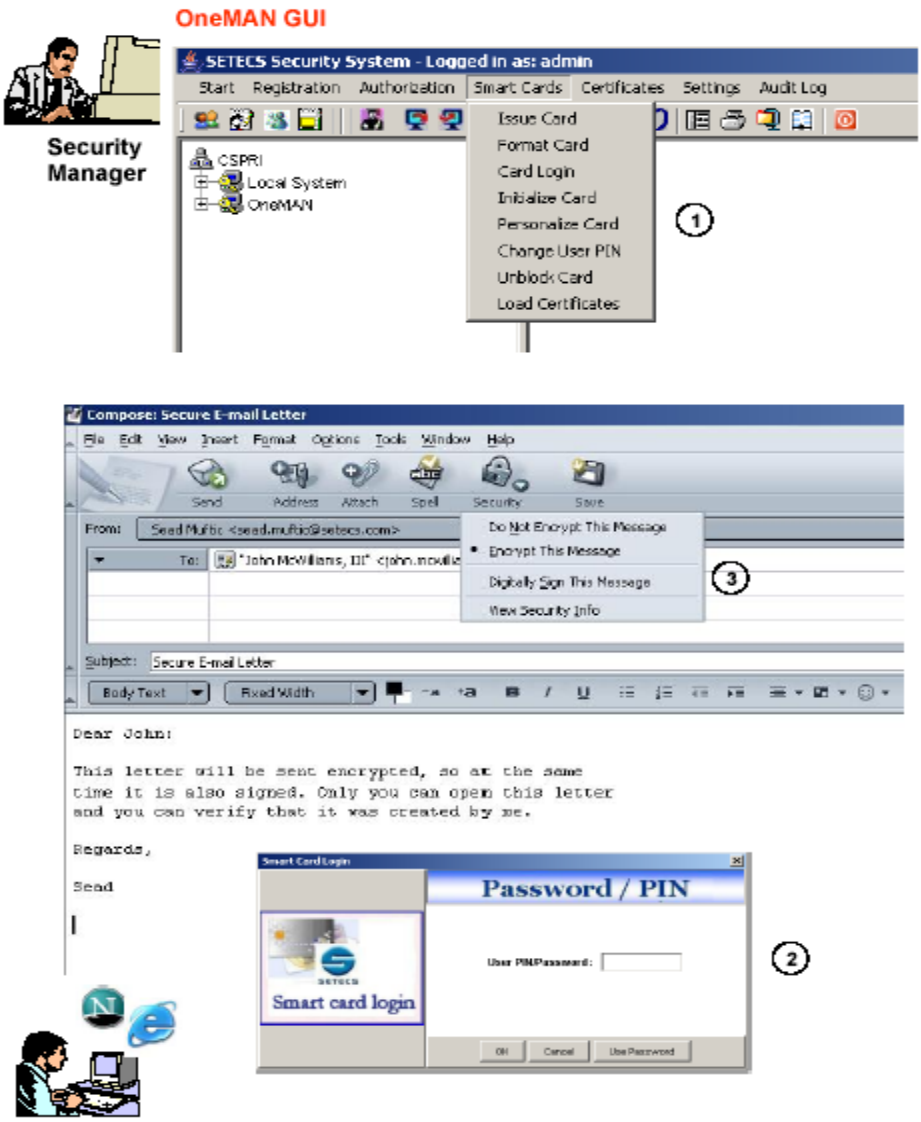
1. OneMAN™ Server including OnePKI™ Local CA Server as for Secure E–mail/Secure Web, or with Public Key Infrastructure
2. OneCARD™ Management System
3. OneCARD™ middleware at each user workstation

Activation

For Security Managers equivalent to secure E–mail/secure Web (SSL).
For users, double–click and install OneCARD™ middleware

Usage

For Security Managers, register users, and then issue them smart cards (step ①).
For users, login to Windows through smart cards login panel (step ②) and use smart card transparently with a mailer and browser, as with secure E–mail/Web (step ③).



Secure Shared Documents

User Needs

1. Protection of shared group documents (signing and encryption)
2. Sharing and protection of documents based on group keys and policies
3. Access authorization for documents based on roles and identities

SETECS Products

1. OneMAN™ Server including OnePKI™ Local CA Server, as for Secure E-Mail/ Secure Web, or with Public Key Infrastructure or with SC Mgmt. Sys.
2. OneGroup™ Server

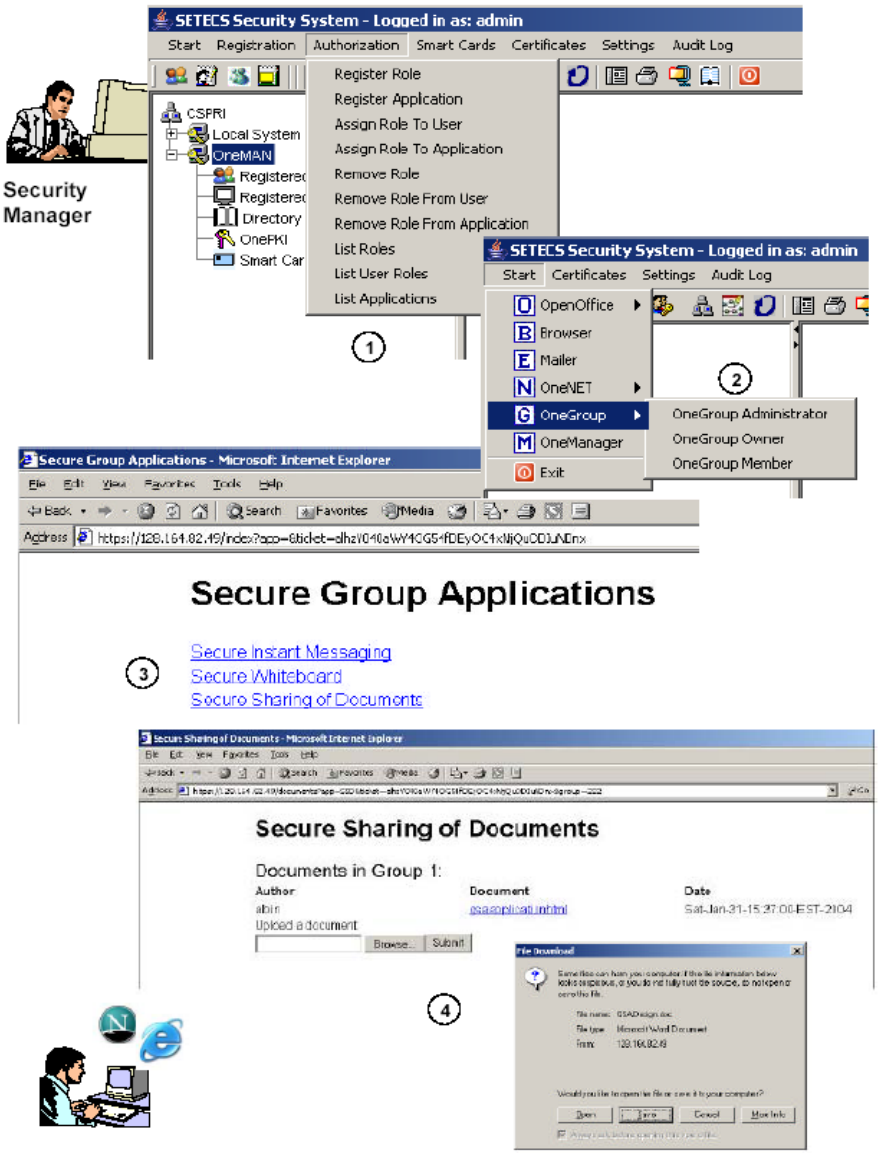
(No installation on users' PCs)

Activation

After same activation as for secure E–mail/Secure Web, register applications and roles at the OneMAN™ server, and assign roles to users and applications (step ①). Activate OneGroup™ server and register groups (step ②)

Usage

Start the Web Browser; click on the Web interface of the OneGroup™ server (step ③); access group documents, if authorized; upload (with encryption) or download (with decryption) group documents (step ④)



Secure Collaborative Applications:

Secure Instant Messaging and Secure Whiteboard

User Needs

1. Exchange of protected short instant messages within a group
2. Exchange of protected longer messages within a forum
3. Group keys management (authorization, renewal, archiving, usage)

SETECS Products

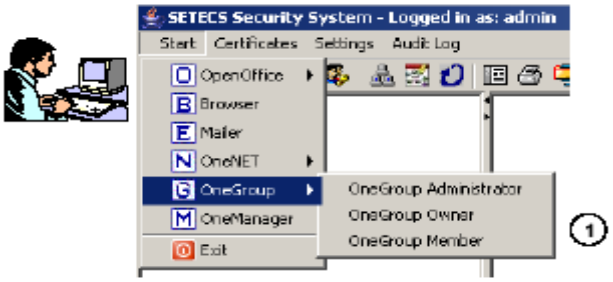
1. For servers, OneMAN™ and OneGroup™, as for secure shared documents.
2. For clients, OneGroup™ Client.

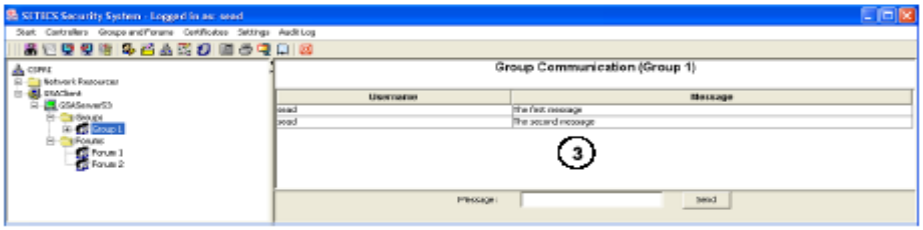
Activation

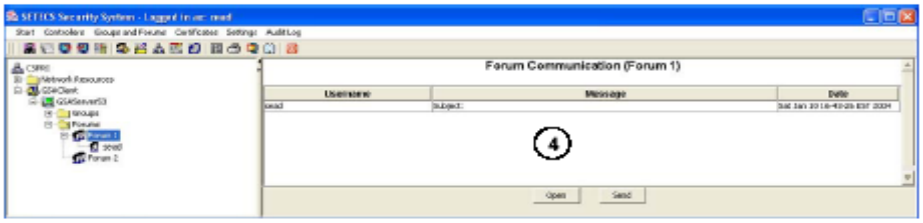
No special activation

Usage

Switch to OneGroup™ client (step①), select OneGroup™ server and a group or forum on it (step ②); Exchange instant messages within a group (step ③); create or read forum documents (step ④)







Secure Desktop

User Needs

1. Login to local workstation and to security domain server
2. Signing, encryption, and enveloping of local files
3. Signing, encryption, and enveloping of OpenOffice documents

SETECS Products

OneSEC™ security system on users' PCs

Activation

Double–click SETECS icon, login, and adjust configuration file

Usage

Start SETECS Secure Desktop, login using either user name/password or smart card (step ①); create self signed certificates or request and fetch certificates from the Local CA server (step ②); protect local files by a right–click (step ③); protect OpenOffice documents using drop–down menu (step ④)

①