SETECS® Cloud Client

PIV Authentication and Authorization

Functionality

SETECS® Cloud Client performs authentication and authorization of users when accessing Cloud Portals. Authentication to the Central Security Server is based on three–factors authentication protocol, using user's PIN, PIV card, and PIV Authentication certificate from the PIV card. Authentication to the Portal security Server is based on SAML ticket and Single Sign–On (SSO) protocol. Authorization is based on Role–based Access Control (RBAC) and XACML Authorization Policy.

Licensing

Institutional users license *SETECS® Cloud Client* in bulk subscriptions. Such Clients are customized to receive usage authorizations from SETECS. Subscriptions are paid annually, in advance.

Prerequisites

SETECS® Cloud Client can be used on all versions of Windows: XP, Windows 7 and Windows Server 2008. Internet Explorer must be adjusted to declare SETECS Security Server as the Trusted Site and to accept/execute active content (ActiveX). These adjustments are performed through Tools | Internet Options | Security of Internet Explorer.

Installation

SETECS® Cloud Client is downloaded in the form of its self–installer:

SETECS_Cloud_Login_Install.exe

Put the Installer in any temporary directory and double-click on it. It will be installed in the SETECS_Cloud_Login run–time directory and its icon will appear on the desktop.

Configuration

After installation:

- `Servers.file` must be manually edited, specifying the name and IP number of the Central Security Server(s) that will initially authenticate the user and issue SAML Ticket, so its entries have the form

```
SETECS Server 207.188.192.233
```

- `Config.file` must be manually edited, replacing the IP number in it with the IP number of the default Portal:

```
http:// 207.188.192.234:8080/SETECSCloud
```

Multiple Central Security Servers may be specified and Internet Explorer will automatically be launched and directed to the Portal Security Server.

The workstation must have smart card reader with its driver activated and ready to use.

Activation of the PIV Card

After double-clicking the icon, *SETECS® Cloud Client* will display Login Panel. This panel depends on the type of smart card reader connected to user's workstation: if the reader does not have PIN Pad (so PIN is entered using the keyboard), the panel in Figure 1 will show; if PIN Pad reader is used, the panel in Figure 2 will be shown.

Figure 1: Reader without PIN Pad

Figure 2: Reader with PIN Pad

After entering the correct PIN, PIV card will be activated.

Initial Authentication

SETECS® Cloud Client reads PIV Authentication certificate from the PIV card and submits it to the Strong Authentication Server, located at the Central Security Server.

Using certificate, Strong Authentication Server will perform three validation steps:

- It will verify using IDMS that the user, indicated in the certificate is registered and in a good standing
- It will verify the validity of the certificate, using certification path up to the Trusted Root Certificate and CRLs of all Certificate Authority (CA) Servers along the certification path
- It will verify, using Card Management System, that the PIV card is valid

After successful validations, Strong Authentication Server will perform strong authentication (challenge / response protocol) with the PIV card of the user.

SAML Ticket

After successful strong authentication protocol, Strong Authentication Server will contact Policy Decision Point (PDP) Server. That server will issue SAML ticket for the user. The ticket will be passed to the user.

If user's PIV card has been issued by SETECS, the ticket is stored in the card. Otherwise, for other PIV cards, the ticket is stored in a file on users workstation. Success message is displayed to the user, as shown in Figure 3:

Figure 3: Completion of Initial Authentication

Access to Portal – SSO

After successful initial authentication, *SETECS® Cloud Client* will immediately activate Internet Explorer, which will be directed to the Portal Security Server. SSO protocol will be performed, using SAML ticket from the PIV card. After successful verification of the user and the ticket, Portal Security Server will display success message:

Figure 4: Successful SSO

After that, user's request will be directed to the Portal and it will display its home page.