Authentication

Introduction

Communication between an Client and TaxCore.API is carried out via the HTTPS protocol.

The Client is authenticated by TaxCore.API using a either client certificate (stored on PKI Applet) or an authentication token received from TaxCore.API, after a client certificate authentication has been successfully conducted as the first step. For more information see Request Authentication Token.

Once token has been obtained HTTP request must contain *TaxCoreAuthenticationToken* key in the request header with value is a valid token string.

Role of the PKI Applet

PKI (public key infrastructure) Applet is installed along with the Secure Element Applet on the same Smart Card.

The role of the PKI applet is to support the secure communication and client certificate authentication of the Client with TaxCore.API using HTTPS protocol. The certificate used to establish a secure connection is stored on a smart card and it can be accessed from the PKI Applet using PKSC#11 API.

The certificate is loaded in the slot / token structure on the PKI Applet.

After the certificate is extracted from the smart card (in DER format) it can be used as a standard X.509 certificate for TLS/SSL and HTTPS protocols.

Valid PIN is required to read the certificate from PKI Applet using PKCS#11 API. Pin for PKI Applet is the same as the PIN for the Secure Element Applet.

Content

1. Required Drivers
   Smart Cards are programmed with PKI firmware according to GIDS (Generic Identity Device Specification) standard. Appropriate drivers shall be installed/programmed on an E-SDC in order to enable PKI Applet usage.

Required Drivers

Smart Cards are programmed with PKI firmware according to GIDS (Generic Identity Device Specification) standard. Appropriate drivers shall be installed/programmed on an E-SDC in order to enable PKI Applet usage.

Windows OS Drivers

Windows OS Drivers

GIDS driver is an integral part of Windows OS since Windows 7 SP1, enabling the instant use of a smart card. No additional driver installation is required.

Linux OS Drivers

In order to use PKI Applet on Linux based OS, a pkcs11 driver from the OpenSC library is required. OpenSC libraries and tools are freely available on https://github.com/OpenSC.

In the following example, the installation of required drivers, libraries and tools on Debian / Ubuntu flavor of Linux OS with USB based card reader is shown. It is assumed that OpenSSL is used for TLS/SSL communication.

1. Install card reader driver

```
apt-get install libudev-dev
wget https://alioth.debian.org/frs/download.php/file/4126/pcsc-lite-x.y.z.tar.bz2
tar -xf pcsc-lite-x.y.z.tar.bz2
cd pcsc-lite-x.y.z
./configure
make
make install
aptitude install libusb-1.0-0-dev
wget https://alioth.debian.org/frs/download.php/file/4111/ccid-x.y.z.tar.bz2
tar -xf ccid-x.y.z.tar.bz2
cd ccid-x.y.z
./configure
make
make install
copy 92_pcscd_ccid.rules file from src directory to /etc/udev/rules.d/
# aptitude install libltdl-dev
wget http://ftp.de.debian.org/debian/pool/main/o/openct/openct_x.y.z.orig.tar.gz
tar -xf openct_x.y.z.orig.tar.gz
cd openct_x.y.z
./configure
# make
make all
```

2. Install OpenSSL development library

```
apt-get install libssl-dev
```

3. Install OpenSC package

```
wget http://cznic.dl.sourceforge.net/project/opensc/OpenSC/opensc-x.y.z/opensc-x.y.z.tar.gz
tar -xf opensc-x.y.z.tar.gz
cd opensc-x.y.z
./configure
make
make install
```

Run opensc-tool command from terminal

If message that libopensc.so.3 cannot be loaded find it with

```
find / -name "libopensc.so"
```

```
[illegible]
```

Copy found library to /usr/lib

4. Install libp11 library

```
apt-get install libp11-2
```

5. Install engine_pkcs11 library

- Download source code from https://github.com/OpenSC/engine_pkcs11/releases/
- Build and install library according to instructions found project page

After the above steps are executed, the certificate shall be accessible from the appropriate slot/token using a PKCS11 family of functions from the lipb11 library. ENGINE family of functions can be used to load the pkcs11 engine in the OpenSSL.

Other Platforms and Operating Systems

Please contact OpenSC community (https://github.com/OpenSC) for further information.