



State Enterprise  
Special Telecommunications Center

# Public Key Certification Center of the Public Administration Authorities

# PKI Center - goals and services



By the Order of the Director General No. 21 of July 14, 2006, within the SE "Special Telecommunications Center" was created Public Key Certification Center of the Public Administration Authorities



The Center provides services of public key certification for public administration authorities, legal persons with various forms of business and for individuals

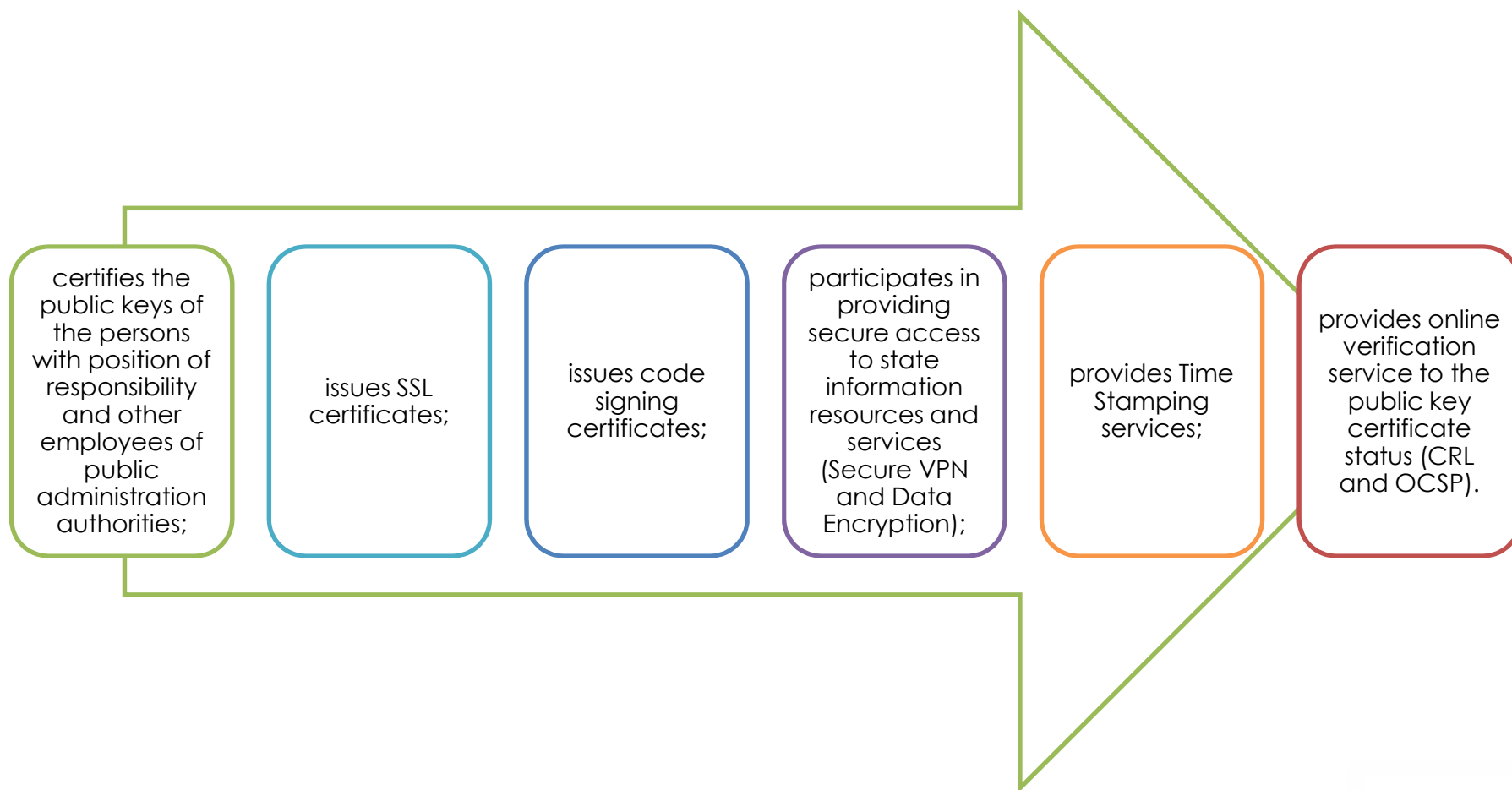


The objective of the Center is to assess the public key certification services and other services regarding the digital signature in both public administration authorities and legal and other persons with various forms of activity

# Legal Basis

- **Law** on electronic document and digital signature no.264-XV of 15.07.2004
- **Law** on electronic commerce no.284-xv of 22.07.2004
- **Government Regulation** no. 945 of 05.09.2005 on Public Key Certification Centers;
- **The Regulation** on the order of digital signature application on the electronic documents of the public authorities, approved by the Government Regulation no. 320 of 28.03.2006;
- **Order** of the Director of the Intelligence and Security Service no. 38 of 30.06.2006

# Functions of Public Key Certification Center



# Types of public key certificates

Public key certificates for digital signature with legal effects

- has the same legal effects like handwritten signature on paper;
- non-repudiation.

Public key certificates for digital signature without legal effects

- used to sign documents without the legal power;
- signing/encrypting E-mails.

Public key certificates for authentication and security services

- In security infrastructure refers to the process of identifying of the final users within a transaction and a series of measures to be implemented before its identity is to be confirmed;
- Secure VPN and Data Encryption.

# SSL Server certificate

## What is SSL?

SSL (secure sockets layer) certificate is a technology that can be integrated into a website to protect secure information. The main idea is to create a secure channel over an insecure network.

SSL is the standard security technology for establishing an encrypted link between a web server and clients' browser. This link ensures that all data passed between the web server and browsers remain private and integral.

## How it works?

When someone visits a Web page that is protected by an SSL certificate, the secure sockets layer authenticates itself with the website server. Once that connection is established, a unique session key is generated which will allow the session to be secure. When the information is transmitted, the data is encrypted so that a third party cannot read anything that was typed into the Web form.

## Where is used?

in e-commerce environment;  
internet secure transmission of sensitive data;  
remote working;  
In web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).  
The purpose of using SSL certificates is to make your Web visitors trust your site.

# Application

## digital signature with legal effects

- the “Credit Bureau” information system.
- the Ministry of Finance of Republic of Moldova

## digital signature without legal effects

- the automated interbank payment system;
- the e-Reporting system;
- the remote treasury account servicing system;
- the e-declaration system;

## authentication and security services

- the Bank - Client system;
- the “Electronic Mailbox” information system of public administration authorities;
- the e-Procurement service;
- the “AccesWeb” search information system.

# Technical means



CryptoCertum 3.0  
Cryptographic  
Smart Card



ACR38 Smart Card  
Reader



Aladdin eToken R2



Aladdin eToken PRO  
64k

# Technical means (characteristics)

## CryptoCertum 3.0 Cryptographic Smart Card:

- chip: Philips,
- memory: 72 Kbytes,
- cryptography: symmetric (DES, 3DES), asymmetric (DSA, RSA),
- protocols: T=0 and T=1.
- implementation of different Access Control Methods (authentication),
- encrypting data with RSA asymmetric keys – the length of up to 1024 bits,
- creating and verifying electronic signatures with the use of RSA and DSA algorithms,
- generating RSA keys –length up to 1024 bits – directly on the card.

## ACR38 Smart Card Reader:

<b>Brand</b>	ACR
<b>Model</b>	ACR-38
<b>Reader</b>	SMART CARD
<b>Standard</b>	ISO 7816 & EMV2 2000
<b>Host</b>	USB 2.0
<b>Transmission speed</b>	12 Mbps
<b>Power Consumption</b>	max. 50mA
<b>Dimensions</b>	97mm x 72mm x 18.5mm
<b>Temperature \ Humidity</b>	0° - 50° C \ 40% - 80% rH
<b>Color</b>	Black \ Golden
<b>Operability</b>	500 000 hours

## Aladdin eToken PRO 64k:

authentication based on the certificate providing protection against phishing attacks;  
authentication and digital signature support for PKCS # 11;  
does not require a battery to ensure long term sustainability;  
smart card chip of a high performance;  
compatibility with standard USB interface;  
full portability;  
does not need a driver;  
integrated logical and physical access option;

## Aladdin eToken PRO 64k:

memory chip EEPROM (16k);  
DES-X 120-bit processor;  
incorporates the key generation of RSA 1024-bit and 2048-bit;  
supports various security certificates and standards such as PKCS # 11v2.01;  
CAPI (Microsoft Crypto API) USB interface;

# PKI Software

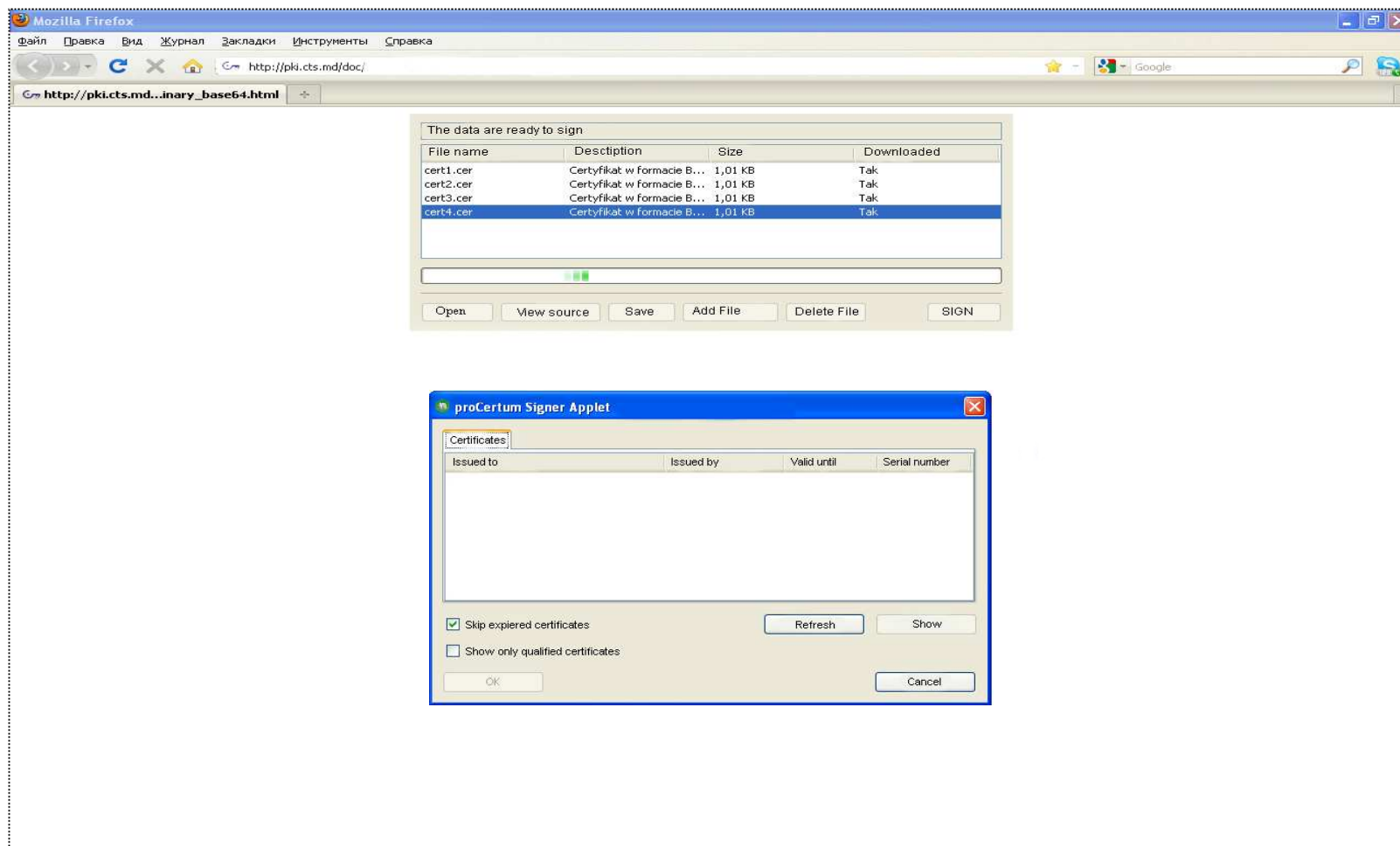
MoldSign CardManager - manages public key certificates profiles on CryptoCertum cryptographic smart card. The allows users to view and operate smart card profiles and generate PIN codes for each certificate profile. Independently delete certificates from cryptographic card.

MoldSign SmartSign - is an application for the creation and verification of the e-signature and the latter to be verified by a valid qualified or non-qualified certificate.

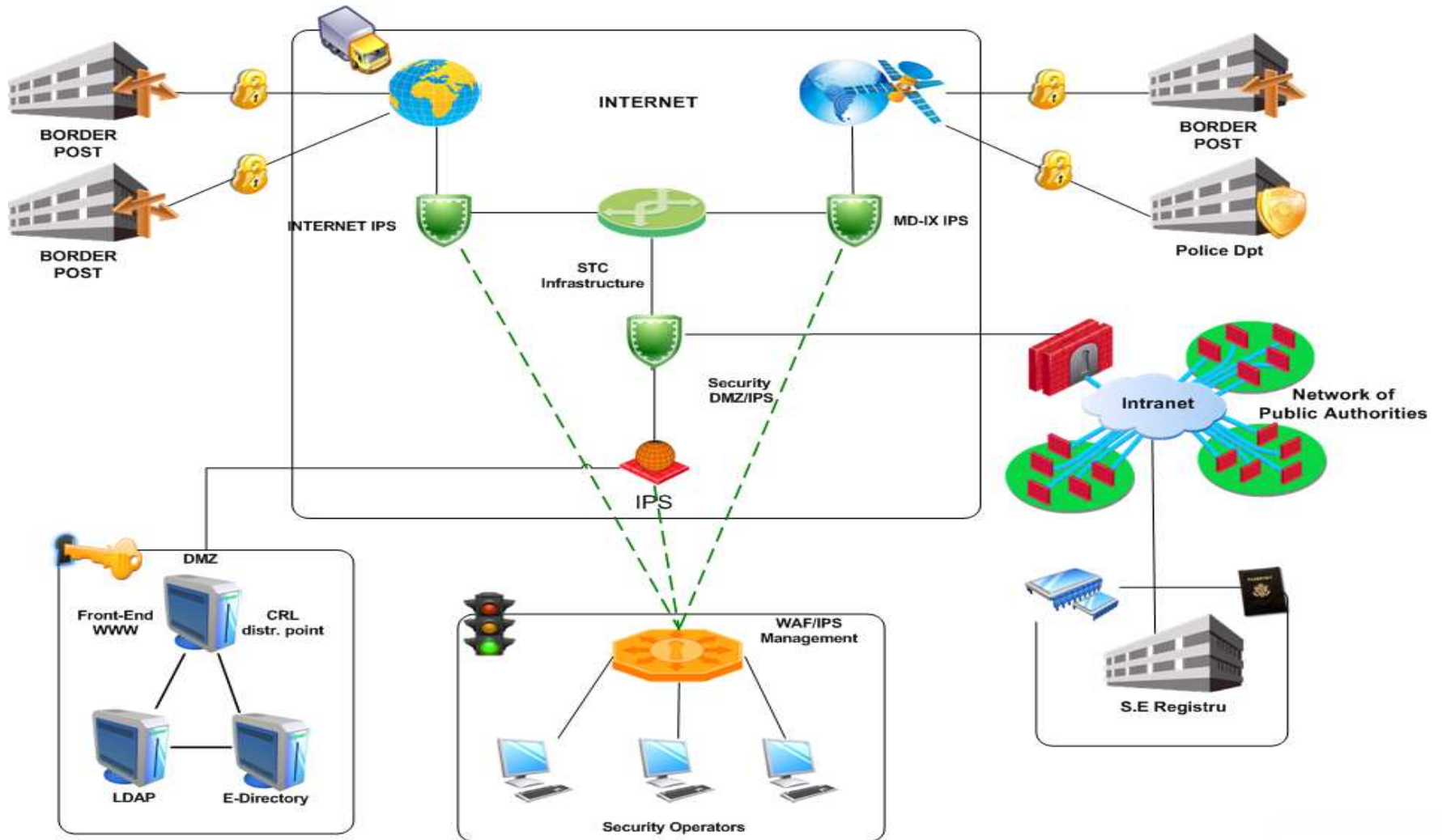
PKI Server - automates the generation of digital signatures, data verification, encryption, and decryption. PKI operations are completed using certificates stored in the HSM. PkiServer is usually integrated in information system using **Client-Server** model.

Signer Applet - is a Web Applet delivered to users in the form of Java byte code. Applets can run in a Web browser using a Java Virtual Machine. It brings the functionality of MoldSign SmartSign **on-line**.

# Signer Applet (default interface)



# Main Scheme





State Enterprise  
Special Telecommunications Center

## Contacts

### State Enterprise Special Telecommunications Center

Piata Marii Adunări Nationale, 1

Chişinău, Moldova Rep. of

tel: +373 22 820 900

fax:+373 22 250 522

[www.pki.cts.md](http://www.pki.cts.md)

e-mail: [pki@cts.md](mailto:pki@cts.md)