TrustNETWORK
Digital certificate authority

CPS (Certificate Practice Statement)

Date of accepting: 01/02/2024 (January 2, 2024)

Version: v1.0

General information

TrustNETWORK is an international certification authority that issues DV, OV and EV SSL certificates, as well as EV Code Signing certificates. The TrustNETWORK certification center is accredited in accordance with PCI DSS requirements, which guarantees a high level of security for the services provided.

Legal information

The digital certification center TrustNETWORK is registered in the Republic of Belarus as a commercial organization under the name: *LLC "TrustNetwork" (Limited Liability Company "TrustNetwork")* at the address: *Brest, 224000, Varshavskoe highway, building 43, floor 10* with Payer Account Number: *698508470* .

Purpose of CPS

The purpose of this document is to provide information about the TrustNETWORK Certificate Authority's policies and procedures regarding the issuance of DV, OV and EV SSL certificates and EV Code Signing certificates.

Scope of application

This document applies to all SSL certificates issued by the TrustNETWORK CA, including:

- DV SSL certificates
- OV SSL certificates
- EV SSL certificates
- EV Code Signing Certificates

Definitions

For the purposes of this document, the following definitions apply:

- Certification Authority is a legal entity that issues electronic signature certificates.
- An SSL certificate is an electronic document confirming that a specific domain or IP address belongs to a specific owner.
- A DV SSL certificate is the simplest type of SSL certificate that does not require verification of the owner's identity.
- OV SSL Certificate - A higher trust SSL certificate that requires verification of the owner's identity.
- EV SSL Certificate is the highest trust SSL certificate that requires extensive verification of the identity of the owner and organization.
- EV Code Signing certificate is an SSL certificate designed for signing software, requiring extended verification of the identity of the owner and/or organization.

Procedure for issuing SSL certificates

The procedure for issuing SSL certificates at the TrustNETWORK CA depends on the type of certificate.

— DV SSL certificates

To obtain a DV SSL certificate, you must provide the following information:

1. The domain name or IP address for which a certificate is required.
2. Email address of the certificate owner.

— OV SSL certificates

To obtain an OV SSL certificate, you must provide the following information:

1. The domain name or IP address for which a certificate is required.
2. Email address of the certificate owner.
3. A document confirming the identity of the certificate holder and/or organization.

— EV SSL certificates

To obtain an EV SSL certificate, you must provide the following information:

1. The domain name or IP address for which a certificate is required.
2. Email address of the certificate owner.
3. A document confirming the identity of the certificate owner.
4. A document confirming the registration of the certificate holder's organization.

Procedure for verifying the identity of the certificate holder

The procedure for verifying the identity of the certificate owner depends on the type of certificate.

— DV SSL certificates

There is no need to verify the identity of the owner of the DV SSL certificate.

— OV SSL certificates

Verification of the identity of the owner of the OV SSL certificate is carried out by comparing the provided data with data from official registries.

— EV SSL certificates

Verification of the identity of the owner of an EV SSL certificate is carried out by checking the provided data with data from official registries, as well as by telephone conversation with the certificate owner.

Validity period of SSL certificates

SSL-certificates are valid for 1 year, 2 years or 3 years. Code Signing certificates are valid for 2, 3 or 5 years.

Refusal to issue an SSL certificate

The TrustNETWORK certification authority may refuse to issue an SSL certificate in the following cases:

- The provided data does not meet the requirements of the certification authority.
- The certification authority cannot confirm the identity of the certificate owner **(when issuing an OV / EV certificate)** .
- The certification authority cannot confirm the registration of the certificate owner's organization **(when issuing an OV / EV certificate)** .

Revocation of an SSL certificate

The TrustNETWORK CA may revoke an SSL certificate in the following cases:

- The owner of the certificate has violated the terms of use of the certificate.
- The certificate authority has detected that the certificate was issued based on incorrect information.
- Data privacy protection.

TrustNETWORK Certification Authority takes all necessary measures to protect the confidentiality of data provided by certificate holders.

Final provisions

This document is an integral part of the terms of use of SSL certificates from the TrustNETWORK certification authority.

Общество с ограниченной ответственностью "ТрастНэтворк" |

Date of accepting: **01/02/2024 (January 2, 2024)**