Integration with a trusted third party

foreign country

Table of contents

1 Intro

This document describes the process of interaction during integration with the Trusted Third Party of the Republic of Kazakhstan and the Trusted Third Party of a foreign country.

2 Definitions and abbreviations

The following key concepts are used in this document:

Certificate - a document in paper or electronic form, issued by a certification authority to confirm compliance of an electronic digital signature with established requirements.

Certificate Revocation List (hereinafter - **CRL**) - a part of the certificate registry containing information about certificates whose validity has been terminated, including their serial numbers, date, and reason for revocation (cancellation).

Certification Authority (hereinafter - **CA**) - a legal entity certifying the correspondence of the public key of an electronic digital signature to the private key of an electronic digital signature, as well as confirming the authenticity of the certificate.

Trusted Third Party of the Republic of Kazakhstan (hereinafter - **TTP RK**) - a state technical service confirming the authenticity of a foreign electronic digital signature using the Trusted Third-Party software complex.

X.509 Data Validation and Certification Server Protocols of the Internet Public Key Infrastructure (Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols, hereinafter - RFC 3029) - a protocol based on which the TTP RK provides services for authenticating electronic digital signatures.

Trusted Third Party of a Foreign State (hereinafter - **TTP FS**) - an organization authorized by the legislation of a foreign state to carry out activities in automated mode to verify the electronic digital signature in electronic documents at a fixed point in time regarding the person who signed the electronic document.

Electronic Digital Signature (hereinafter - **EDS**) - a set of electronic digital characters created by electronic digital signature means and confirming the authenticity of an electronic document, its ownership, and the integrity of its content.

Receipt for verification of a foreign electronic digital signature according to RFC 3029 (hereinafter - **Receipt**) - an electronic document certified by the EDS of the TTP RK and confirming the authenticity of the foreign EDS.

Validation of Digitally Signed Document Service (hereinafter - **VSD**) - a service that verifies the authenticity of the EDS.

Cryptographic Information Protection Tools (hereinafter - **CIPT**) - cryptographic information protection tools - a set of software and technical means implementing cryptographic transformation algorithms, key generation, formation, distribution, or management, ensuring the use of electronic digital signatures and encryption in information systems. CIPT can be used both as standalone software modules and as instrumental tools embedded in application software.

SDK (software development kit) - a set of development tools that allow creating applications to work with VSD.

VSD-request - a request generated to VSD according to RFC-3029.

3 Interaction Schemes

There are two types of interaction schemes between TTP RK and TTP FS:

- One-way interaction scheme;
- Two-way interaction scheme.

3.1 One-way interaction scheme

Regulation of interaction between parties in a one-way interaction scheme:

1. If necessary, TTP RK provides TTP FS with an SDK for generating VSD-requests according to RFC-3029;

2. TTP FS provides TTP RK with its certificate, CA certificates (issuing certificates for services and for signing receipts), and links to CRLs;

3. TTP RK provides TTP FS with its certificate, CA certificate, and a link to the CRL;

4. TTP FS provides TTP RK with its CIPT;

5. If the interaction is via the https protocol, TTP FS and TTP RK exchange SSL certificates;

6. TTP RK provides TTP FS with its URL and necessary policies (if any) to be specified in VSD;

7. TTP FS generates VSD-requests;

8. TTP FS signs the VSD-request (see paragraph 3.3.2);

9. TTP FS sends the signed VSD-requests to TTP RK, receives responses, and analyzes them.

3.2 Two-way interaction scheme

Regulation of interaction between parties in a two-way interaction scheme:

1. TTP RK and TTP FS (hereinafter referred to as parties) provide SDKs for generating VSD-requests.

2. Parties exchange:

a. Certificates;

b. CA certificates that issued certificates;

c. CA certificates that issued certificates for signing receipts;

d. Certificates that will be sending requests;

e. Links for downloading CRLs for CAs (listed above);

f. Links to their URLs;

g. SSL certificates if the interaction occurs based on https.

3 Parties configure necessary policies (adding certificates to trusted ones, setting up URLs for redirecting requests).

4. Parties exchange valid detached signatures in PKCS#7 format;

5. Parties generate VSD-requests with embedded receipts from the above points;

6. Parties sign VSD-requests (see paragraph 3.3.2);

7. Parties send signed VSD-requests, receive responses, and analyze them.

3.3 Additional

3.3.1 If TTP RK receives a VSD-request containing a detached signature, i.e., the verified electronic document is not included in the request to TTP RK, then the signature verification is performed not based on the content of the electronic document but based on the hash from the embedded receipt for the content of the electronic document. In this case, the validity of the signature is recommended to be checked based on the following checks:

1. response from TTP RK;
2. matching the hash specified in the response from TTP RK with the hash computed on the received electronic document.

3.3.2 The format of the signed VSD-request is an attached PKCS#7 signature with signed attributes, where the signed data is the VSD-request, signed by the keys of the IS.

3.3.3 In addition to RFC 3029, TTP RK supports the following type DVCSRequest:data: DVCSRequest:data:

```
DVCSRequest:data ::= CHOICE {
message OCTET_STRING,
messageImprint DigestInfo,
cers [0] IMPLICIT SEQ_OF_TargetEtcChain,
messageInfo [1] IMPLICIT MessageInfo
}
MessageInfo ::= SEQUENCE {
message OCTET_STRING,
externalData DigestInfos
}
```

3.3.4 TTP RK uses the following response statuses for DVCSResponse:

```
PKIStatus ::= INTEGER {
granted (0),
-- you got exactly what you asked for
rejection (2),
-- you don't get it, more information elsewhere in the message
}
```

3.3.5 CMS (Cryptographic Message Syntax) or PKCS#7 is a cryptographic standard (RFC5652) for representing cryptographic data in ASN.1 format. The standard describes six types of data: data, signedData, envelopedData, signedAndEnvelopedData, digestedData, and encryptedData.

The CMS standard describes the structure of cryptographic messages, including protected data together with information necessary for their correct opening or use. For example, the message contains protected data, information about the hash and signature algorithm, signing time, public key certificate, certification chain, etc. Some of these attributes are optional, but the application may determine the need for their presence. Each algorithm has a set of parameters that must be agreed upon by both parties: for GOST 34.10-2012, in addition to the public key, these are the p modulus, coefficients of the elliptic curve a and b, and the order of the cyclic subgroup of points of the elliptic curve q.