Organisation for Co-operation between Railways (OSJD)

Translated from RU original: JSC “RZD“

P 941-4

Typical technical specifications of cross-border cooperation between public key infrastructures used by railways operated by member countries of the OSJD

Table of Contents

Abbreviations used in the document

AS	–	Automated System
BCh	–	Belarusian Railway
TTP	–	Trusted Third Party
TCA	–	Trusted Certificate Authority
EC	–	European Commission
PKI	–	Public Key Infrastructure
RZD (JSC "RZD")	–	Russian Railways
HSC	–	Hardware and software complex
DET	–	Data Encryption Tools
IC	–	Identity Certificate
PKC	–	Public Key Certificate
DTN	–	Data Transmission Network
EDMS	–	Electronic Document Management System
UZ	–	Ukrainian Railway
CA	–	Certificate Authority
EDF	–	E-Document Flow
ED	–	Electronic Document
(Q)DS	–	(Qualified) Digital Signature
DS	–	Digital Signature

Glossary

EDI	–	Electronic Data Interchange
EDI System	–	System used by foreign railways to transfer data electronically
HSM	–	Hardware Security Module, a device generating and securely storing electronic keys
OCSP	–	Online Certificate Status Protocol, used to determine PKC status
RFC 3029	–	Document determining a general Data Validation and Certification Server (DVCS) and the protocols to be used when communicating with it
RSA	–	Public-key cryptosystem
TLS	–	Transport Layer Security, data encryption protocol used to transfer data securely over the Internet
TSP	–	Time-Stamp Protocol, a cryptographic protocol used by time stamping authority

UN/EDIFACT	–	United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport, the international EDI standard developed under the UN
VSD	–	Validation of Digitally Signed Document, a check for QDS/DS validity at a specific point in time with respect to a particular document
XML	–	eXtensible Markup Language, a set of rules for encoding documents
E-Document Recipient	–	Intended audience of a particular digitally signed e-document, according to its issuer
Public Key Infrastructure	–	Technical and managerial structure intended to apply DS, identify persons issuing DS and digitally signing e-documents and validating integrity and authenticity of e-documents by means of DS in accordance with the laws and regulations of the parties involved
Qualified Digital Signature	–	An electronic signature exhibiting all the characteristics of an unqualified electronic signature, as well as the following properties: 1) its identity certificate contains the public key used to validate the signature; 2) the electronic signature is created and validated by means approved under the effective legislation
Public Key	–	A unique string of characters uniquely paired with a corresponding private key and used to validate electronic signatures
Private Key	–	A unique string of characters used to create an electronic signature
Unqualified Electronic Signature	–	An electronic signature that: 1) is created by a data encryption algorithm using a key; 2) allows unique identification of the signatory of an electronic document; 3) allows any possible alterations introduced upon signing of the document to be tracked; 4) is created using electronic signature facilities
ED Issuer	–	Person who (on behalf of whom) creates an electronic document and electronically signs it in

		accordance with legislation of the jurisdiction of which the person is a subject
DS Facilities	–	Data encryption tools and services used for at least one of the following functions: DS creation, DS validation, private key creation, public key creation.
E-Document (Electronic Document)	–	Formalized data recorded electronically, signed with an DS and subject to the legislation of the jurisdiction of which the document issuer is a subject
Electronic Signature	–	A piece of electronic data paired or associated with another piece of electronic data being signed and used to identify the signatory
Digital Signature	–	A character string, built into an ED, used to verify the integrity and authenticity of a document and/or to identify the signatory of a document in accordance with the jurisdiction of which they are a subject

1. General Conditions

In the age of economic globalization, big transnational corporations and integration of some countries' transport systems into the international economy, transport axes rapidly form that allow major freight and passenger flows between different countries to be speeded up. At the same time, the new economic conditions and stricter quality assurance and price control practices demand a new system of control and management of railways.

Successful development of railway transport, its marketability and investment appeal are predicated on rational cost reduction and greater efficiency.

Implementation of legally binding electronic documents in international transit processes creates the legislative, organizational and technological conditions needed for speeding up freight, cash and service flows, optimizing traffic and significantly reducing the costs of planning and providing them.

The ability to implement electronic carriage documents is provided for by section #10 of article #6 and section #14 of article #7 of the Agreement on International Goods Transport by Rail.

Informational support for freight traffic in the systems operated by railway administrations is provided in accordance with conventions on EDF as listed in the UN/EDIFACT international standard upon receipt of goods for delivery with subsequent communication of relevant information to border stations for advance notification and processing of documents via Infonet-21 and HERMES data transmission networks, as well as the Internet.

Identifiable authorship, integrity and legal relevance of electronic documents (ED) are ensured by digital signature (DS) technologies.

The goal of using a legally binding e-document flow (EDF) is to organise an efficient railway freight process by using information and communication technologies.

The primary tasks of practical implementation of a legally binding EDF are:

- developing the mechanisms for validating the legal relevance of an electronically signed ED and for ensuring trust in the certificates issued in different jurisdictions;
- organizing interaction between specialized hardware and software used by involved parties operating in different jurisdictions and using potentially incompatible means of encryption;
- creating the technical conditions for transfer, processing and validation of electronically signed EDs.

Resolving the aforementioned issues requires use of secure elements of trust that would enable adequate levels of data exchange security and the legal relevance of documents transmitted. These supposed elements of trust existing between the data exchange parties are inadequately supported by the current information management systems, so they usually require a trusted third party (TTP) to mediate the secure data exchange.

TTP services are described in the ITU-T X.842 “Information technology – Security techniques – Guidelines for use and management of trusted third party services” international recommendation. TTP’s primary functions are validation of an DS created in a foreign jurisdiction and encryption standards and its legal approval from the standpoint of and in accordance with the ED receiver’s jurisdiction.

In order to take advantage of the trusted e-document exchange, parties involved in cross-border cooperation (Railway Administrations) must be connected (or provide the means of connection) to a trust infrastructure Access Points (*fig. 1*).

Access Points may be arranged either on the premises of a Railway Administration in accordance with the requirements listed in this document, or with involvement of independent market agents (trusted service providers). An Access Point enables trusted exchange to be established between the Railway Administration connected to it and a Railway Administrations connected to a different Access Point. An Access Point must be operated by a local company under the same jurisdiction as the Railway Administration connected to it.

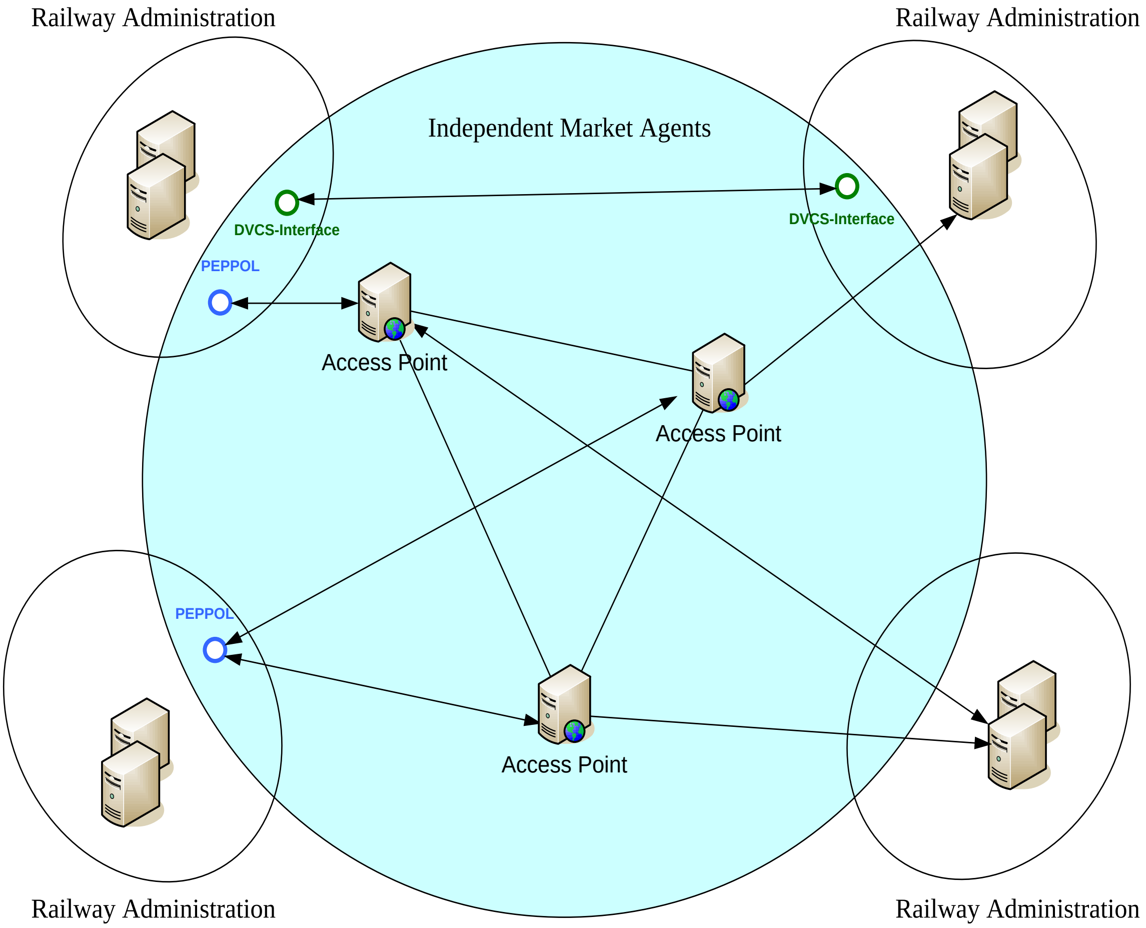

Fig. 1. Interaction between public key infrastructures.

2. Technical Specifications

2.1. ITU-T X.842 “Information technology – Security techniques – Guidelines for use and management of trusted third party services”. [1]

This recommendation includes instructions for application and management of trusted third party (TTP) services, precise definitions of their responsibilities and the services provided, their descriptions and purposes, as well as the roles and responsibilities of third parties and their customers. The document is intended primarily for systems administrators, developers, TTP staff and their customers so that correct TTP services may be chosen and used.

The guidelines determine the major categories of TTP services, such as time-stamping, non-repudiation, key and certificate management and electronic notary public services.

List of primary TTP services provided as per the X.842 international guidelines:

1. Data authenticity check and validation services (as per RFC 3029. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS)).
2. Certificate management.
3. Certificate status check (as per RFC 2560. Online Certificate Status Protocol (OCSP)).
4. Time-stamp creation (as per RFC 3161. Time-Stamp Protocol).
5. Identification and authentication.
6. Electronic notary public.
7. Access control.
8. Electronic filing.
9. Non-repudiation.
10. Directory.
11. Personalization.
12. Key management.
13. In-line translation.
14. Recovery.
15. Incident reporting and alert management.

X.842 specifies more than 30 possible types of service in total.

2.2. PKCS #1 “RSA Cryptography Standard”, v2.1. [2]

Public Key Cryptography Standards are specifications devised by RSA Laboratories in cooperation with a consortium of international developers of cryptography systems for the purpose of developing public-key encryption.

PKCS #1 is a standard that determines the basic working principles of public-key encryption based on the RSA (Rivest, Shamir, Adleman) cryptosystem.

2.3. RFC 2560:1999, RFC 6960 “Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP”. [3]

Online Certificate Status Protocol is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate in real-time.

OCSP offers the capability of obtaining digital certificate status without having to access the client-side list of revoked certificates. Using OCSP minimizes performance overheads of processes with an operating logic that dictate the need to obtain certificate status via client-side software.

OCSP operates on a “request/response” principle. OCSP client generates an OCSP request and sends it to a server. The OCSP server receives the request, obtains the status of the certificate in question, generates an OCSP response and sends it back to the client.

OCSP was first published as RFC 2560 in 1999; the current version is defined in RFC 6960, published in June 2013. [4]

2.4. RFC 2315 “PKCS #7: Cryptographic Message Syntax Version 1.5”; [5] RFC 2630, RFC 5652 “Cryptographic Message Syntax” (CMS). [6]

Cryptographic Message Syntax describes the structure of cryptographically protected messages carrying encrypted data and the information required for its correct decryption or use. Such information may include, e.g., encrypted data, hashing and signature generation algorithm information, signature time-stamp, public key certificate, certificate chain, etc.

Besides electronic signatures, CMS supports encryption, hashing and computation of message authentication code (MAC), including those specified by Russian algorithms (RFC 4490), as well as multiple encapsulation (i.e., a CMS-based message may be encapsulated inside another CMS-based message).

CMS was first published as RFC 2315 “PKCS #7: Cryptographic Message Syntax Version 1.5” in March, 1998. Several revisions later (such as RFC 2630), RFC 5652 “Cryptographic Message Syntax (CMS)” [7] was accepted in September 2009 as an IETF standard. This is the most recent version and the one currently used.

2.5. RFC 2510 [8], RFC 4210 “Internet X.509 Public Key Infrastructure. Certificate Management Protocols” (CMP). [9]

Certificate Management Protocol is used for requests for obtaining and processing X.509 digital certificates. It defines operations with X.509 certificates, such as a signing request, signed certificate receipt and others. It also determines data transaction methods (such as HTTPS) that may be employed for certificate requests over a public network.

The most recent version of the protocol is described in RFC 6712. [10]

2.6. RFC 5246 “The Transport Layer Security (TLS) Protocol,” v1.2. [11]

Transport Layer Security is a cryptographic protocol used for secure data transfer over the Internet. TLS uses asymmetric cypher for authentication, a symmetric cypher for communications privacy and MACs to ensure message integrity.

The main purpose of TLS is to ensure security and integrity of data transmitted during a communications session between two applications. The protocol consists of two layers: the record layer and the handshake layer.

TLS’s record layer is used for encapsulating objects such as higher-level protocols. One such object is the handshake layer of TLS, which enables a server and a client to authenticate each other, exchange cypher spec information and keys before the application sends or receives the first byte of actual data. The handshake sub-protocol of TLS ensures a secure connection with three basic properties:

- The parties’ identity may be established using an asymmetric cypher (RSA, DSS, etc.). This authentication may be made optional, but only for one of the two parties.
- Exchange of a shared secret key is secure: even if an attacker manages to intercept the data, they would be unable to decipher the key.
- The handshake itself is secure: an attacker is unable to modify the established secure connection without alerting both parties to their presence.

2.7. RFC 4634 “US Secure Hash Algorithms” (SHA and HMAC-SHA). [12]

Secure Hash Algorithm is a family of cryptographic hash functions. They transform the initial data set of arbitrary length into a fixed length bit string, which is called the hash, hash sum or hash code.

The hash functions applied by the algorithm share the basic principle with data compression functions. The input message is divided into 512-bit-long blocks and a hash function is applied to them sequentially. The function takes the data in the current data block together with the fixed-length hash sum computed from the previous block as the input and computes a new hash sum as the output until there are no blocks left. The final block’s hash sum output is the resulting hash sum of the entire message.

HMAC (hash-based message authentication code) is a message authentication code created using a hash function.

Message integrity validation mechanisms based on a secret key are usually called message authentication code (MAC). It is typically used by parties engaging in secure data transmission where they exchange the secret keys needed to validate the transmitted data. This behavior is determined by MAC. A validation mechanism that uses cryptographic hash functions in addition to a secret key is called HMAC.

2.8. RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. [13]

Certificate Revocation Lists are a method for validating a digital certificate before the date specified in the *NotAfter* field of the certificate. Lists are usually issued by the same certificate authorities who issued the certificates listed therein. CRLs may be obtained by various means, such as LDAP, HTTP or FTP protocols. The format of CRLs (CRL v2, the current version, in particular) is defined in RFC 5280 and subsequently updated in RFC 6818. [14]

3. Specifications public key infrastructure interwork interfaces are based upon

3.1. RFC 3029 “Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols”. [15]

This specification allows the implementation of a one-off or subscription-based service for data validation and certification, certificate validation and, optionally, time-stamped confirmation of data transmission.

The full range of DVCS services is defined as follows:

1. Certification of possession of data.
2. Certification of claim of possession of data.
3. Validation of digitally signed documents.
4. Validation of public key certificates.

A successful run of any of the functions will produce a DVC message from the TTP.

3.2. OASIS DSS (OASIS Digital Signature Service).

This specification determines the XML interface for interaction between digital signatures and web services or other applications.

The implementation scheme is presented in [16].

3.3. XKMS v2.0 (XML Key Management Specification).

This standard’s specifications determine the technology for using a public key infrastructure for XML encryption. In particular, a protocol for distribution and registration of public keys that is compatible with W3C XML Digital Signature and XML Encoding standards is defined. XKMS specifications introduce two services: XML Key Information Service and XML Key Registration.

XML Key Information Service Specification (X-KISS) is a protocol to support delegation by an application to a service of the processing of key information associated with an XML signature, XML encryption, or other use of the XML Signature <*ds:KeyInfo*> element.

XML Key Registration Service Specification (X-KRSS) is a protocol to support registration of a key pair by a key pair holder, with the intent that the key pair subsequently be usable in conjunction with the X-KISS or a PKI such as X.509 PKIX.

The primary purpose of using XKMS is to offload the effort of traditional PKI implementation from the client on to an external service.

The description of an XKMS standard implementation is presented in [17].

3.4. ETSI TS 102 231 “Electronic Signatures and Infrastructures (ESI). v3.1.2 Provision of harmonized Trust-service status information”, Annex B (normative): Implementation in XML.

Presents and defines the format of Trust-service Status List (TSL), which lists accredited certificate authorities.

Besides the certificates of the accredited certificate authority representatives, the list may contain descriptions and links to other services offered by the accredited certificate authorities, such as time-stamp service (TSP), online certificate status validation (OCSP), etc.

Use of TSLs should help the user answer the following questions:

- whether a certificate authority offers a secure service;
- whether the service matches the scheme criteria at the time of its delivery (or the time of a successful data transaction based on the service).

The TSL structure is described in [18].

4. Requirements for mutual electronic signature acknowledgement software for implementing cross-border information interchange

4.1. General requirements

4.1.1. TTP Access Point should offer a set of web services matching the application scheme and ensuring the functioning of TTP services: DS validation and/or signature certificate validation.

4.1.2. There should be a way to validate DS in accordance with one of the following international recommendations (depending on the application scheme):

- RFC 3029 “Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols”: Validation of Digitally Signed Documents (DVCS);
- Digital Signature Service Core Protocols, Elements and Bindings Version 1.0 OASIS Standard (OASIS DSS).

4.1.3. Depending on the application scheme, it should be possible to validate a signature certificate as per the W3C recommendations in XML Key Management Specification (XKMS 2.0).

4.1.4. The trust-service status list (TSL) and certificate authority list should be made available as per ETSI TS 102 231.

4.1.5. TTP Access Point should implement one or more of the following software components, depending on the application scheme:

4.1.5.1. DVCS server.

4.1.5.2. DSS server.

4.1.5.3. XKMS server.

4.1.5.4. Software modules that generate and process the TSL (TSL library).

4.1.5.5. DVCS client.

4.1.5.6. DSS client.

4.1.5.7. XKMS client.

4.1.6. The hardware and software components of TTP services should ensure 24/7/365 operation of the Access Point with specified performance (depending on the volume of data submitted for validation).

4.1.7. The Access Point should be deployed on the premises of an organization holding the necessary information security licenses and certificates issued by the appropriate authority of the host country.

4.1.8. Facilities used by the organization running the Access Point should be protected against unauthorized access and be equipped with continuous power supply and air conditioning systems.

4.1.9. TTP Access Point should maintain a log of confirmations sent and received by the cross-border cooperation parties.

4.2. Requirements on DS validation web service implementation

4.2.1. DS validation should be implemented using appropriate data encryption tools and it should consist of the following steps:

4.2.1.1. Signature format validation.

4.2.1.2. Cryptographic validation of the DS.

4.2.1.3. Validation of the public key certificate revocation status at the time of signing.

4.2.1.4. Validation of the certificate issuer’s root certificate presence in the TSL.

If the validation procedure fails on any of the four steps above, the signature is considered invalid and the final validation result is considered negative.

4.2.1.5. Generation of an DS validation receipt.

4.2.2. DVCS server requirements.

4.2.2.1. A DVCS server should offer services in accordance with the protocol defined in RFC 3029 as Validation of Digitally Signed Document (*vsd*).

4.2.2.2. A DVCS server should support the capability of forming requests and receiving responses within the scope of the same HTTP session (i.e., operate in synchronous mode).

4.2.2.3. A DVCS server should process requests made with *Content-Type: application/dvcs*, received by HTTP or HTTPS protocols.

4.2.2.4. A DVCS server should be able to authenticate users connecting by via the TLS protocol using corresponding cryptography standards.

4.2.2.5. The capability should be provided of using different certificates for signing confirmations and establishing TLS connections.

4.2.2.6. All the requests received and responses generated should be encapsulated in PKCS #7 *signedData* structure.

4.2.2.7. A DVCS server should validate all the signatures attached to the signed document for correct cryptography, as well as the revocation status of all the public key certificates used to validate these signatures.

4.2.2.8. When validating certificate revocation status, a DVCS server should rely either on the appropriate CRLs or the present status information received from the certificate authorities (e.g., from an OCSP service).

4.2.2.9. *vsd* requests should be generated as per RFC 3029 and contain the following attributes:

- a unique *vsd* request ID (GUID);
- *vsd* request generation date and time (or a time-stamp);
- a signed ED in a format described in #5.6.1 below;
- DS of the *vsd* request based on the user's signature key.

4.2.2.10. Upon validation of an ED received in return for a user's *vsd* request, a DVCS server should generate a *vsd* confirmation message conforming to the requirements listed in RFC 3029 and containing the validation results of the ED specified in the *vsd* request (whether the ED signature is valid or invalid, with an appropriate error code as per RFC 3029).

4.2.2.11. *vsd* confirmation messages should contain:

- a unique *vsd* confirmation ID (GUID);
- *vsd* confirmation generation date and time (or a time-stamp);
- ID of the *vsd* request that prompted the confirmation message;
- signed ED returned in response to the *vsd* request;
- validation of ED signature at the time of signing (valid or invalid);
- DS of the vsd confirmation message signed using the DVCS server's signature key.

4.2.2.12. A DVCS server should produce a return code of the ED signature validation result in the *status* field of the *PKIStatusInfo* structure of the *vsd* confirmation message, conforming to the requirements listed in RFC 2510 (CMP).

4.2.3. DSS server requirements.

4.2.3.1. A DSS server should provide a signature validation service (using Verifying Protocol) conforming to the Digital Signature Service Core Protocols, Elements and Bindings Version 1.0 (DSS) standard defined in OASIS Consortium's recommendations.

4.2.3.2. A DSS server should support the capability to form requests and receive responses within the scope of the same HTTP session (i.e. operate in a synchronous mode).

4.2.3.3. A DSS server should process requests made with *Content-Type: application/xml*, received by HTTP or HTTPS protocols.

4.2.3.4. A DSS server should be able to authenticate users connecting by the TLS protocol and using Russian cryptography standards.

4.2.3.5. The capability of using different certificates for signing confirmations and establishing TLS connections should be provided.

4.2.3.6. All the requests received and responses (confirmation messages) generated should be presented as signed XML documents.

4.2.3.7. A DSS server should validate all the signatures attached to the signed document using all the available information about the public keys and revocation statuses of the certificates used to sign it.

4.2.3.8. A DSS server should validate all the signatures attached to the signed document for correct cryptography, as well as the revocation status of all the public key certificates used to validate these signatures.

4.2.3.9. When validating a certificate revocation status, a DSS server should rely either on the appropriate CRLs or the present status information received from certificate authorities (e.g., from an OCSP service).

4.2.3.10. A DSS server should only process signature validation requests containing a single <*ds:Signature*> field.

4.2.3.11. A DSS request should be presented as a signed XML document with a *xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"* scheme and contain the following:

- a unique DSS request ID (GUID);
- a signed ED;
- an unsigned ED (optionally, if its signature is transmitted separately);
- DS of the DSS confirmation message signed using the DSS server’s signature key (using the *xmlns:ds=http://www.w3.org/2000/09/xmldsig#* scheme).

4.2.3.12. Upon validating an DS received in a DSS request, a DSS server should generate a confirmation message presented as a signed XML document (using the *xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"* scheme) and containing the following data:

- a unique DSS confirmation message ID (GUID);
- validation status (*ResultMajor*, *ResultMinor*);

- an DS of the DSS confirmation message signed using the DSS server's signature key (using the *xmlns:ds=http://www.w3.org/2000/09/xmldsig#* scheme).

4.3. Requirements on public key certificate validation web service implementation

4.3.1. PKC validation should be implemented using appropriate data encryption tools and should consist of the following steps:

4.3.1.1. Generation of a certificate trust chain.

4.3.1.2. Building of a certificate trust chain.

4.3.1.3. Validation of the certificate issuer's root certificate presence in the TSL.

If the validation procedure fails at any of the two steps above, the signature is considered invalid and the final validation result is considered negative.

4.3.1.4. Generation of an DS validation receipt.

4.3.2. XKMS server requirements.

4.3.2.1. An XKMS server should provide a certificate validation service (XKISS: Validate Service).

4.3.2.2. An XKMS server should support the capability of forming requests and receiving responses within the scope of the same HTTP session (i.e., operate in synchronous mode).

4.3.2.3. An XKMS server should process requests made with *Content-Type: application/x-xkms+xml,* received by HTTP or HTTPS protocols.

4.3.2.4. An XKMS server should be able to authenticate users connecting by the TLS protocol using accepted cryptography standards.

4.3.2.5. The capability of using different certificates for signing confirmations and establishing TLS connections should be provided.

4.3.2.6. All the requests received and responses (confirmation messages) generated should be presented as signed XML documents.

4.3.2.7. When validating a certificate revocation status, an XKMS server should rely either on the appropriate CRLs or the present status information received from certificate authorities (e.g., from an OCSP service).

4.3.2.8. An XKMS request should be presented as a signed XML document with a *xmlns="http://www.w3.org/2002/03/xkms#"* scheme and contain the following:

- a unique XKMS request ID (GUID);
- DS certificate;
- an DS of the DSS confirmation message signed using the DSS server’s signature key (using the *xmlns:ds=http://www.w3.org/2000/09/xmldsig#* scheme).

4.3.2.9. Upon validating an DS received in a DSS request, an XKMS server should generate a confirmation message presented as a signed XML document (using the *xmlns="http://www.w3.org/2002/03/xkms#"* scheme) and containing the following data:

- a unique response ID (GUID);
- response status (*ResultMajor*);
- certificate validation status;
- an DS of the XKMS confirmation message signed using the XKMS server’s signature key (using the *xmlns:ds=http://www.w3.org/2000/09/xmldsig#* scheme).

4.4. Trust-service Status List interaction requirements.

4.4.1. A TSL generation and validation tool should be able to generate a TSL containing the following data:

4.4.1.1. TCA certificate list, including their qualification statuses (qualified, unqualified).

4.4.2. A root certificate presence validation software interface should be developed for the TSL.

4.4.3. A TSL validation should consist of the following checks:

4.4.3.1. Validation of the TSL DS using the *xmlns:ds=http://www.w3.org/2000/09/xmldsig#* scheme.

4.4.3.2. Validation of the *xmlns:tsl="http://uri.etsi.org/02231/v2#"* scheme conformity of the TSL.

4.4.4. A graphical representation of the TSL should be provided and contain the following:

4.4.4.1. TSL validity time span;

4.4.4.2. Name of the TSL;

4.4.4.3. Ordinal number of the TSL;

4.4.4.4. A list of trusted root certificates specifying the distinguished name (DN), serial number and validity time span of the certificate and the associated services.

4.5. Requirements for a software client to access DS and certificate validation services

4.5.1. DVCS client requirements.

4.5.1.1. Generation of *vsd* signature validation requests conforming to the specifications listed in RFC 3029 and containing the following data:

- a unique *vsd* request ID (GUID);
- *vsd* request generation time and date (or a time-stamp);
- a signed ED in a format described in #5.6.1 below.

4.5.1.2. Capability of signing a *vsd* request using a client certificate.

4.5.1.3. Capability of saving a *vsd* request.

4.5.1.4. Sending *vsd* requests to specified servers by HTTPS with *Content-Type: application/dvcs*.

4.5.1.5. Capability of receiving and loading a *vsd* response.

4.5.1.6. Capability of validating a *vsd* response.

4.5.1.7. Capability of receiving DS validation status in a *vsd* response.

4.5.1.8. Capability of saving a *vsd* response as a file.

4.5.1.9. Capability of representing a *vsd* response visually.

4.5.2. DSS client requirements.

4.5.2.1. Generation of signature validation DSS requests conforming to the OASIS DSS specifications, using the *xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"* scheme and containing the following data:

- a unique DSS request ID (GUID)
- a signed ED;
- an unsigned ED;
- an unsigned ED (optionally, if its signature being transmitted separately);
- DS of the DSS confirmation message signed using the DSS server's signature key (using the *xmlns:ds=http://www.w3.org/2000/09/xmldsig#* scheme).

4.5.2.2. Capability of signing a DSS request using a client certificate.

4.5.2.3. Capability of saving a DSS request as a file.

4.5.2.4. Sending DSS requests to specified servers by HTTPS with *Content-Type: application/xml*.

4.5.2.5. Capability of receiving and loading a DSS response.

4.5.2.6. Capability of validating a DSS response.

4.5.2.7. Capability of receiving DS validation status in a DSS response.

4.5.2.8. Capability of saving a DSS response as a file.

4.5.2.9. Capability of representing a DSS response visually.

4.5.3. XKMS client requirements.

4.5.3.1. Generation of signature validation XKMS requests conforming to the XKMS v2.0 specifications, using the *xmlns="http://www.w3.org/2002/03/xkms#"* scheme and containing the following data:

- a unique XKMS request ID (GUID)
- one or more signature certificates;
- DS of the DSS confirmation message signed using the DSS server's signature key (using the *xmlns:ds=http://www.w3.org/2000/09/xmldsig#* scheme).

4.5.3.2. Capability of signing an XKMS request using a client certificate.

4.5.3.3. Capability of saving an XKMS request as a file.

4.5.3.4. Sending XKMS requests to specified servers by HTTPS with *Content-Type: application/x-xkms+xml*.

4.5.3.5. Capability of receiving and loading an XKMS response.

4.5.3.6. Capability of validating an XKMS response.

4.5.3.7. Capability of receiving DS validation status in an XKMS response.

4.5.3.8. Capability of saving an XKMS response as a file.

4.5.3.9. Capability of representing an XKMS response visually.

4.6. General software requirements

4.6.1. Use of a single DS format containing a verifiable time-stamp (as per RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol – TSP") and a verifiable signature certificate revocation status at the time of signing (as per RFC 2560 "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP") is recommended. The format of electronic messages should conform to the *SignedData* format as defined by the PKCS #7 standard and conforming to the requirements of RFC 2630 (CMS).

4.6.1.1. The electronic signatures of documents should be based on the hash sum of the document's content, computed as a detached signature.

4.6.1.2. Implementation of the hash function and the electronic signature should be compatible with the formats accepted by the relevant EDM systems.

4.6.1.3. An electronic message should contain the signature certificate.

4.6.1.4. The time-stamp should be contained in an unsignable attribute of the message, with OID equal to <*1.2.840.113549.1.9.16.2.14*>.

4.6.1.5. An OCSP response should be contained in an encrypted bit string in an unsignable attribute of the message, with OID equal to <*1.2.840.113549.1.9.16.2.22*>.

4.6.2. DS and signature certificate validation services should maintain request logs and confirmation message logs containing all validation instances and results.

5. Recommendations for the TTP interaction management functionality of a software module to be embedded in e-document management systems operated by parties involved in cross-border cooperation

5.1. The following functions are to be implemented in the software module:

5.1.1. Extraction of an ED signed by a foreign electronic signature out of the EDMS;

5.1.2. DS type identification;

5.1.3. Formation of a request towards a TTP for signature validation;

5.1.4. Reception of either a response from the TTP (in the form of a confirmation message) or the document in question, electronically signed by the TTP.

5.2. The software module should provide the following software gateway features for setting up unified TTP access points for processing e-documents signed by foreign electronic signatures:

5.2.1. Basic DS validation procedures (see #4.2.1 above).

5.2.2. Receiving confirmation messages from the TTP validating an DS.

5.2.3. Sending a validation request for an DS made under a foreign jurisdiction and re-signing a document with the TTP’s own DS.

5.2.4. Sending an ED to a TTP for it to be signed, with involvement of a designated cryptographic service provider.

5.2.5. Flexibility with regard to adding new electronic signature services.

5.2.6. Working in synchronous and asynchronous modes.

5.2.7. Loading up-to-date TSL and COC lists for signature validation.

5.2.8. Providing secure access to TTP services via the TLS protocol with use of public key certificates and according to the designated privileges (user, administrator).

5.2.9. Fully logging the validation procedures.

5.2.10. Gathering performance data.

5.3. Software module components:

5.3.1. A server component integrated into the EDMS and responsible for discerning the incoming documents signed for a foreign DS.

The server component fulfils the following functions:

- Generation of ED signatures in a format compatible with the EDMS.
- Recognition of documents containing foreign signatures and submission of requests for their validation to a TTP by a relevant

protocol (OASIS, DSS, XKMS, RFC 3029), depending on the type of signature and use policies.

- Interaction with low-level components of an employed cryptographic service provider (such as CryptoPro CSP) and DS validation APIs.
- Validation and analysis of confirmation messages received in response to document validation requests submitted to a TTP.
- Relaying the validation services' confirmation messages to an automated access management system for potential subsequent use in resolving disputes.

5.3.2. A client component providing the EDMS user with electronic documents addressed to them, signed with a foreign DS and confirmed valid by a TTP. An electronic document signed with a foreign signature is cleared for further EDMS processing by the receiving party if its validation returns a positive result. The client component should deliver the document and inform the EDMS user that is the ED recipient of the document's validity. The message should be signed by the appropriate certificate.

Basic functionality carried out by the client component:

- Signature certificate validation with use of a Trust-service Status List (TSL) in a format conforming to the ETSI TS 102 231 "Electronic Signatures and Infrastructures (ESI). Provision of harmonized Trust-service status information" specification.
- DS validation based on the document in question and its signature.
- DS validation based on the hash sum of the document and its signature.
- Time-stamp validation.

5.3.2.1. The client component provides software interfaces to a certificate validation service based on the XKMS v2.0 (XML Key Management Specification) and ensuring the following functionality:

- Generation of public key certificate validation requests.
- Sending of certificate validation XKMS requests to a TTP service over a secure connection in accordance with configured policies.
- Reception of XKMS confirmation messages containing validation results.
- Analysis of the XKMS confirmation messages and DS validation of TTP's certificate validation confirmation messages.

5.3.2.2. The client component provides a software interface to a Trusted Third Party's DS validation based on the OASIS DSS (OASIS Digital Signature Service) specification, ensuring the following functionality:

- Generation of DS validation requests based on the document in question and its signature.
- Generation of DS validation requests based on the hash sum of the document and its signature.
- Sending of DSS requests to a TTP validation service over a secure connection in accordance with configured policies.
- Reception of DSS confirmation messages containing validation results of all of the electronic signatures contained in the DSS request sent to the TTP.
- Analysis of the DSS confirmation messages and DS validation of TTP's DS validation confirmation messages.

5.3.2.3. The client component provides software interfaces to an electronic signature validation service based on the X.842 — RFC 3029 "Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols" specification and ensuring the following functionality:

- Generation of DS validation requests based on the document in question and its signature.
- Generation of DS validation requests based on the hash sum of the document and its signature.
- Sending of *vsd* requests to a TTP validation service over a secure connection in accordance with configured policies.
- Reception of *vsd* confirmation messages containing validation results of all of the electronic signatures contained in the *vsd* request sent to the TTP.
- Analysis of the *vsd* confirmation messages and DS validation of TTP's DS validation confirmation messages.

5.4. Use example of a software module embedded in an e-document management system.

Let us examine how such a software module was used in the informational and technological flow between an EDMS used for freight management at JSC "RZD" (ETRAN Automated System) with a TTP computer appliance complex located at JSC NIIAS certification authority. The primary objective of such interaction was the ability to process e-documents signed with foreign DS without any further input from the user.

A model of a computer appliance complex ensuring the ability to accept electronic signatures used in cross-border EDF was developed (OOO CRYPTOPRO's cryptographic service provider and software was used for the purpose). The model included an automated access management system (AAMS) capable of establishing a connection with ETRAN AS; a client component of the software module was installed on the AAMS enabling it to interact with the TTP services provided by JSC NIIAS CA. ETRAN AS was adapted for use with the AAMS and TTP service interaction with the AAMS was also organized.

An HP Proliant DL380R07 server was used as the hardware platform for the software module's operation. The server was powered by a 2.4 GHz Intel CPU and 4 GB of RAM.

The software platform was chosen to be either Microsoft Windows Server 2003 (x86) with SP2 (or newer), or Microsoft Windows Server 2008 (x86 or x64) with SP2 (or newer), or Microsoft Windows Server 2008 R2 with SP1 (or newer).

The following software was installed on the server:

- cryptographic service (for electronically signed document validation using the necessary encryption algorithms, as well as for generation of confirmation messages);
- a TSP client;
- an OCSP client;
- Microsoft SQL Server 2008 R2 (may be run on a separate server).

The model's performance was assessed on a testing ground jointly operated by Russian and Belarusian Railways, where a twin TTP concept proposed by the Belarusians was suggested and implemented in accordance with the international recommendations and specifications listed in ITU-T X.842 (see below in #6.3.1).

A flowchart of the model's operation is presented on figure 3.

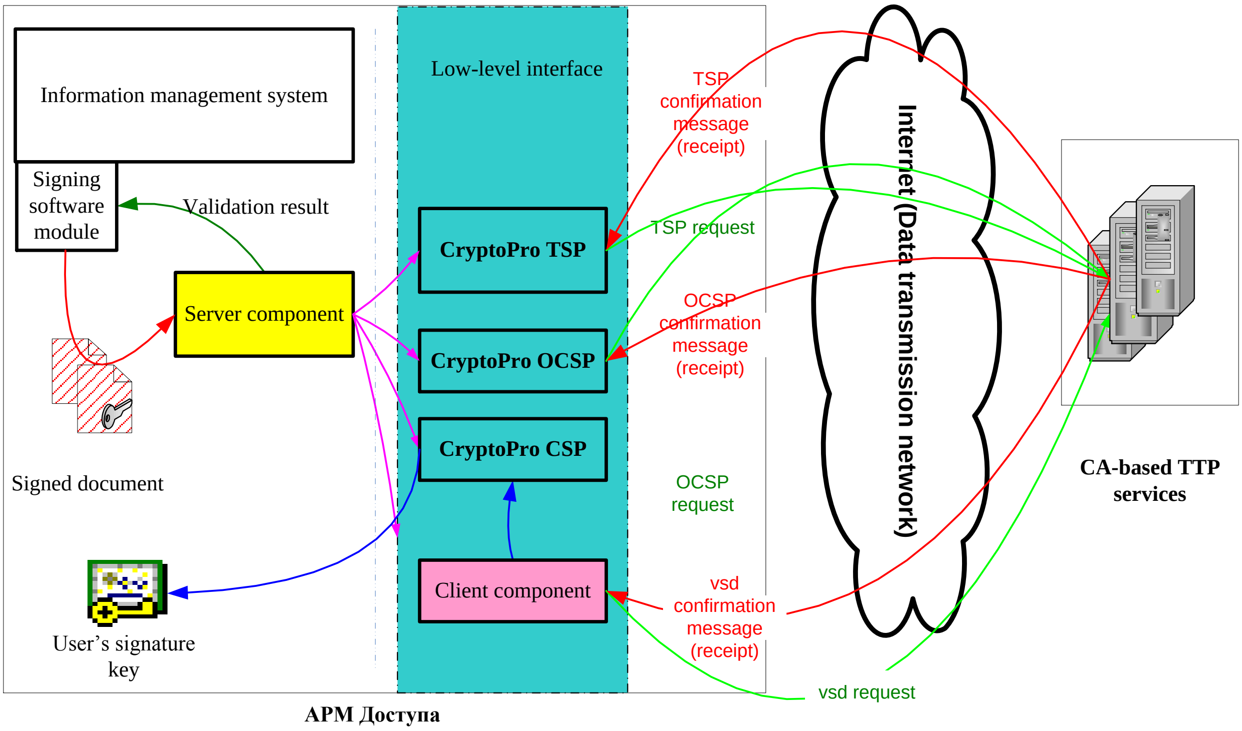

Fig.3 Operation flowchart

5.5. Recommendations for setting up cross-border interaction with foreign partners by the means of an EDI system.

The typical interaction scheme using an EDI system and TTP services is presented in fig. 4 and provides for transparent use of the TTP services without involvement of the main functionality of the EDI systems operated by the interaction parties.

For proper operation, the following EDI system queues must be allocated for every participant:

1. Draft document queue: unsigned documents in IFTMIN format prepared by the sender's automated system, as well as signed documents from the sender.
2. Processed document queue: unsealed IFTMIN documents (those successfully validated).

5.5.1. Recommendations for signing documents to be exported.

It is recommended that the signatures and dispatch of export documents are to be based on freighters, freight clerks or other duty-holders' previously generated signatures. It is also recommended to appoint a member of staff responsible for signing cross-border documents and overseeing their automatic signing (using a server-side signature with all the necessary security measures for key information access and storage).

The recommended TTP interaction module operation algorithm is as follows (the execution sequence of the steps is denoted by numerals in **white** circles).

1. The TTP interaction software module reads the incoming IFTMIN document queue, loads and checks them in accordance with their IFTMIN GUID (only IFTMIN documents are loaded from the incoming document queue).
2. The TTP interaction software module passes the incoming IFTMIN documents to an automatic signing software module to be signed with the private key of the duty holder responsible for overseeing the signing of the sender's cross-border documents.

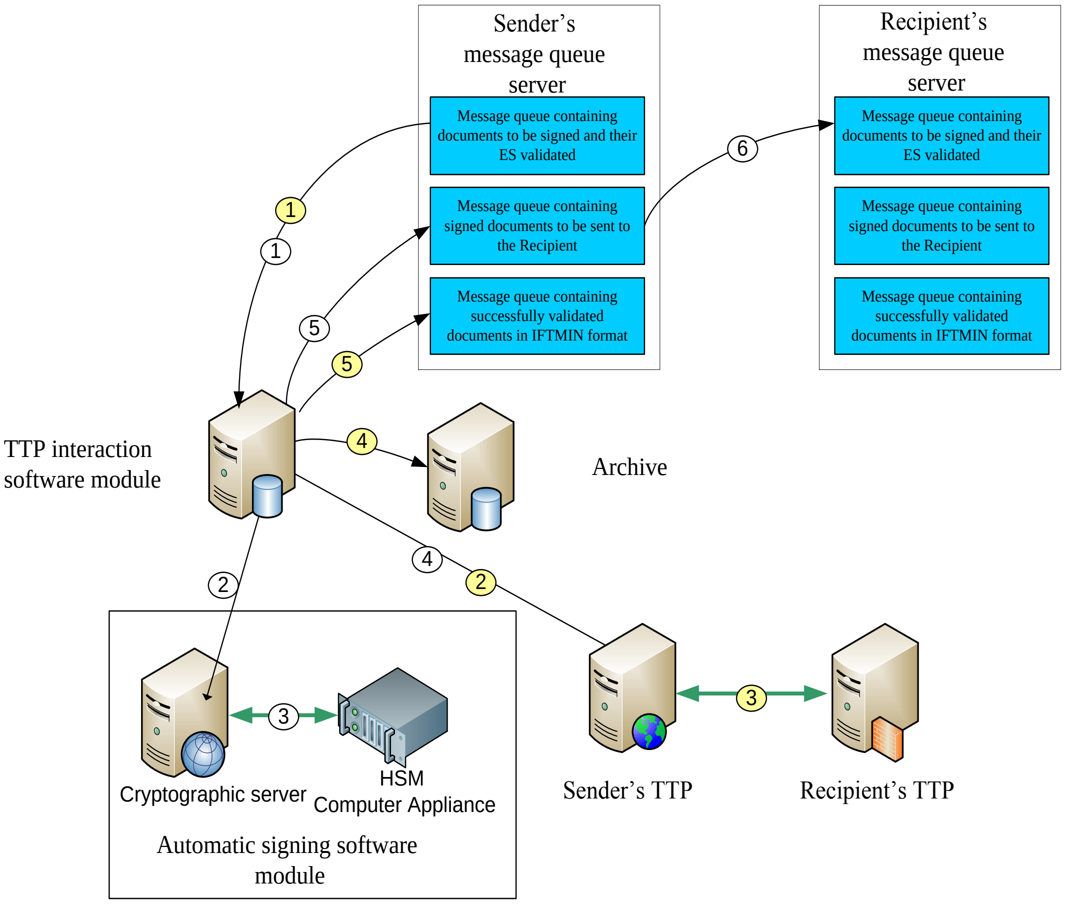
Sender's message queue server
Message queue containing documents to be signed and their ES validated
Message queue containing signed documents to be sent to the Recipient
Message queue containing successfully validated documents in IFTMIN format
Recipient's message queue server
Message queue containing documents to be signed and their ES validated
Message queue containing signed documents to be sent to the Recipient
Message queue containing successfully validated documents in IFTMIN format
1
1
5
5
6
TTP interaction software module
4
Archive
2
4
2
3
3
Cryptographic server
HSM Computer Appliance
Automatic signing software module
Sender's TTP
Recipient's TTP

Fig. 4. Use of the TTP interaction software module in a data exchange between RZD and its Partner.

3. The automatic signing software module signs the documents with the private key of the duty holder. The signature is generated in a format defined in PKCS #7 and integrated with the data.
   Addition of time-stamps and up-to-date certificate revocation statuses is recommended when generating an DS.
4. The data block containing the signature is returned to the TTP interaction software module and, if necessary (depending on the adopted TTP interaction scheme), is sent to the TTP to collect further signature validity proofs (see #6.3.3 below as an example of such interaction used between Russian and Kazakh Railways).
5. The TTP interaction software module passes the data block to the outbox MQ queue of the corresponding IFTMIN document recipient.
6. The document is sent to the recipient's inbox queue.

5.5.2. Recommendations for signature validation during document import.

The recommended TTP interaction module operation algorithm is as follows (the execution sequence of the steps is denoted by numerals in **yellow** circles).

1. The TTP interaction software module reads the incoming signed document queue, loads and checks them in accordance with their IFTMIN GUID.

2. Depending on the signature type, the TTP interaction software module forms a corresponding request to JSC "RZD"'s appointed TTP, signed using JSC "RZD"'s key to confirm the request signature's legitimacy.

3. If necessary (such as in the absence of necessary legitimacy confirmation on its side, interaction between Russian and Belarusian Railways described below in #6.3.1), JSC "RZD"'s TTP forms its own request based on the incoming one and directs it to the Partner's TTP. The Partner's TTP processes the request and sends a response signed using its key based on the RSA algorithm back to JSC "RZD"'s TTP.

4. On the basis of the Partner's TTP's response and confirmation message, JSC "RZD"'s TTP generates its own confirmation message containing validation results and signs it using its key with the help of the automatic signing software module.

5. The TTP interaction software module archives the received confirmation message and the validated IFTMIN document.

6. If a positive signature validation response is received, the TTP interaction software module passes the IFTMIN document to the outbox queue in EDIFACT format with the other successfully validated documents.

6. Cross-border cooperation parties' public key infrastructure trust models and architecture

6.1. TTP services.

TTP performs services listed in Table 1.

Table 1: TTP Services.

Service subsystem	Port	Service description
Public web server	80	HTML-based interface that provides public information about the service performed
TTP service access web interface	443 (TLS with client authentication) and/or 80	HTML-based interface that handles users' requests and displays receipts

The services and ports listed in the table is a reference for external security tool configuration (such as firewalls and packet filters).

6.2. The TTP service is modular and contains the following subsystems:

6.2.1. HTTP Access control module.

6.2.2. Web servers that serve or transmit information, or provide a web-based GUI for other services.

6.2.2.1. A public TTP service web server.

6.2.2.2. A web server to support users' service request and receipt handling.

6.2.2.3. A web server to render a graphical interface for TTP service users' profile pages.

6.2.3. Service repository.

6.2.4. Data encryption tools.

6.2.5. Tech support module.

6.2.6. Fiscal subsystem.

6.2.7. Service administrator subscriber point.

6.2.8. Administrator console.

6.2.9. Command line processor for TTP service user software.

Data transmission for the needs of DVCS and OCSP protocols as well as administration is carried out both ways by the means of the HTTP protocol encapsulated into TLS. Web servers serve as the access subjects (resources to connect to). Access control is executed by the inherent security properties of TLS and their support by the designated HTTP access control module.

Based on the above, the interface for secure access and interaction of users with TTP services contains the following features:

- data encryption tools;
- HTTP and HTTPS protocols;
- TLS protocol ensuring secured data transmission;
- OCSP protocol;
- TSP protocol;
- DVCS protocol;
- web servers;
- data visualization (web browsers);
- text markup (HTML);
- information to be displayed (web sites and pages);
- web applications and a command prompt carrying out dialogues, interaction, and transactions between users and web servers, as well as providing feedback to the users;
- service administrator subscriber point and administrator console carrying out TTP service administration tasks;
- TTP service procedures guide and user manuals.

6.3. Cross-border cooperation parties’ public key infrastructure trust models.

As of today, practical experience regarding the implementation of cross-border electronic signing with the use of TTP services has been collected; in particular this includes paperless freight technology conducted with the use of legally binding electronic documents between RZD and Belarusian, Ukrainian, Kazakh Railways.

Elaborated below are the trust models used in the listed cross-border interaction scenarios.

6.3.1. Cross-border legally binding e-document flow between RZD and BCh.

Cross-border EDF between JSC “RZD” and Belarusian Railway is carried out in the framework established by the Agreement on Private Freight Car Transportation Service Between Russian Federation and the Republic of Belarus, Conducted via Paperless Technology Using Electronic Document Flow

(Addendum #5 to the Agreement Between JSC "RZD" and Belarusian Railway State Union on Electronic Data Exchange Taking Place in International Freight Transportation #520 made on the 28th of July, 2004).

The proposed technical solution assumes that both the data exchange parties interact only with the TTP located in their own domain, conforming to the home jurisdiction's legislative requirements and the TTP interaction agreement's requirements. The DS itself is validated in the domain of the issuer's signature certificate's origin; the other party accepts it without further validation taking place on its end. The trust towards it on the receiving end is predicated on the confirmation message from its local TTP resulting from validating the DS of the issuer's TTP who validated the initial document. TLS protocol with user authentication based on certificates encrypted with the RSA encryption algorithm was used to establish a trusted connection between the parties.

At the same time, data exchange between the two TTPs (requests and responses) is conducted using electronic signatures made using the RSA encryption algorithm and the SHA-1 hashing algorithm, whereas the exchange between a TTP and its customer's information management system is done using state-approved encryption algorithms specified by the local jurisdiction.

The mechanics of data exchange between Russian Railways' and Belarusian Railways' information management systems is described in Fig. 5 and contains the following steps.

1. An electronic waybill for cross-border carriage is prepared and electronically signed in ETRAN AS at the station of origin.
2. Upon generation of the electronically signed waybill, the carriage details, including the electronic data exchange marker, are passed on to the EDI system.

General overview of the cross-border exchange of electronically signed documents between the JSC “RZD” and Belarusian Railways information management systems

Direction: from JSC “RZD” towards BCh

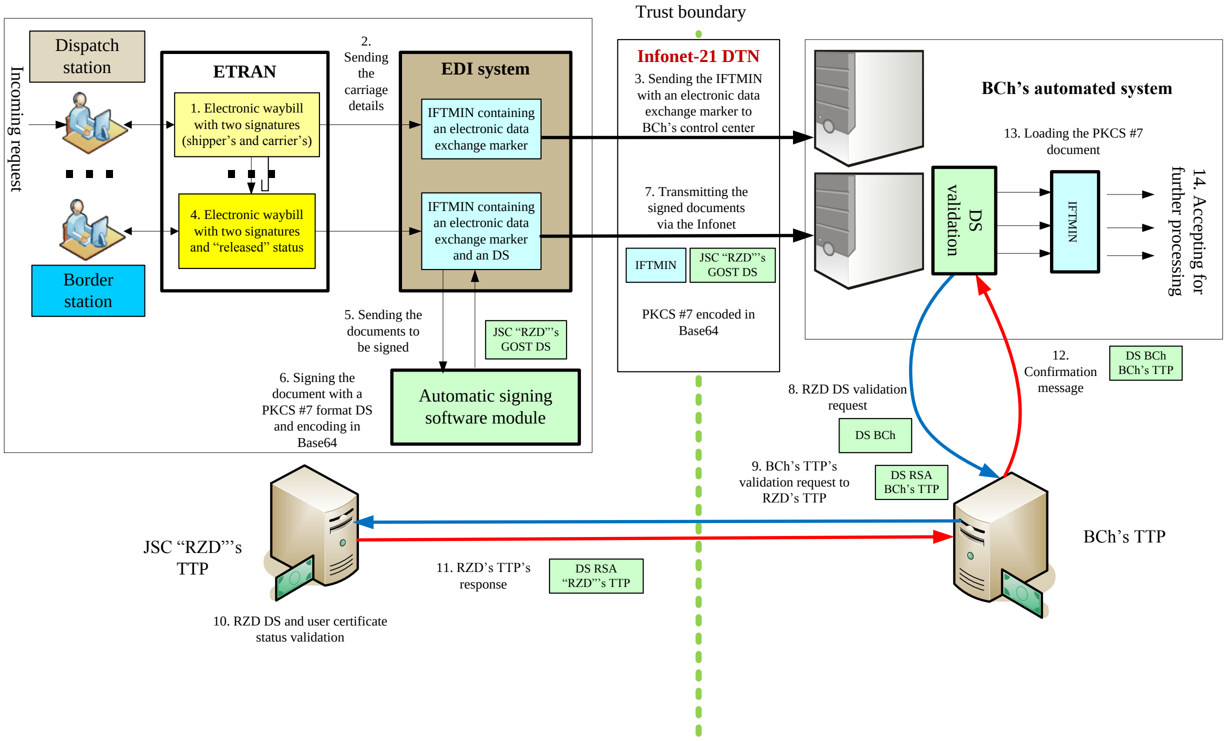
Trust boundary
Incoming request
Dispatch station
Border station
ETRAN
1. Electronic waybill with two signatures (shipper’s and carrier’s)
4. Electronic waybill with two signatures and “released” status
2. Sending the carriage details
EDI system
IFTMIN containing an electronic data exchange marker
IFTMIN containing an electronic data exchange marker and an DS
5. Sending the documents to be signed
JSC “RZD”’s GOST DS
6. Signing the document with a PKCS #7 format DS and encoding in Base64
Automatic signing software module
Infonet-21 DTN
3. Sending the IFTMIN with an electronic data exchange marker to BCh’s control center
7. Transmitting the signed documents via the Infonet
IFTMIN
JSC “RZD”’s GOST DS
PKCS #7 encoded in Base64
BCh’s automated system
13. Loading the PKCS #7 document
DS validation
IFTMIN
14. Accepting for further processing
12. Confirmation message
DS BCh BCh’s TTP
8. RZD DS validation request
DS BCh
9. BCh’s TTP’s validation request to RZD’s TTP
DS RSA BCh’s TTP
BCh’s TTP
JSC “RZD”’s TTP
11. RZD’s TTP’s response
DS RSA “RZD”’s TTP
10. RZD DS and user certificate status validation

Fig. 5. General overview of the cross-border exchange of electronically signed documents between Russian Railways’ and Belarusian Railways’ information management systems (starting from the Russian side).

3. At a border station, upon concluding the necessary technical procedures pertaining to the station’s operation, the information from the waybill is released and passed from ETRAN AS to the EDI system with the electronic data exchange marker and the “released” status.
4. Upon receiving the electronic waybill with the “released” status and the electronic data exchange marker, the EDI system generates and sends an IFTMIN message to be automatically signed with an DS based on RZD’s duty holder’s certificate.
5. The IFTMIN format text document is signed using the key intended for cross-border document signing. The signature is generated in PKCS #7 format and packed together with the rest of the data. The signature must contain a time-stamp.
6. The document is then transported through the transport subsystem of the EDI system using EDIFACT to BCh’s automated system via the InfoNet-21 DTN.

7. BCh’s AS generates an RZD signature validation request, signs it with a BCh staff member’s key, and passes it on to BCh’s TTP for validation.
8. Based on the BCh staff member’s request, BCh’s TTP generates its own RZD signature validation request, signs it with an RSA-based key, and sends it to RZD’s TTP.
9. RZD’s TTP validates the received signature and the authenticity of the RZD staff member’s certificate.
10. RZD’s TTP sends a confirmation message containing validation results and signed with an RSA key back to BCh’s TTP.
11. Based on the confirmation received from RZD’s TTP, BCh’s TTP generates a confirmation message for the BCh staff member, signed by BCh’s TTP with the use of an encryption algorithm approved by the state of the Republic of Belarus.
12. BCh’s AS extracts the data from the PKCS #7 document in the IFTMIN format and passes it on to the recipient for further processing.
13. The recipient, being a BCh AS user, receives the document for further processing in accordance with the accepted procedures.

The mechanics of data exchange between Belarusian Railways’ and Russian Railways’ information management systems is described in Fig. 6 and contains the following steps.

1. BCh’s AS generates a request for cross-border interaction.
2. The request is transformed into an IFTMIN message (the UN/EDIFACT format).
3. The resulting UN/EDIFACT format text document is signed by the BCh duty holder responsible for cross-border document signing, using their key. The signature is generated in a the PKCS #7 format together with the rest of the data. The signature must contain a time-stamp.
4. The document is passed via the Infonet on to RZD’s AS with the help of the EDI system.
5. The document ends up in a TTP interaction software module (described in #6 above) which generates a BCh signature validation request, signs it with an RZD staff member’s key and passes in on to RZD’s TTP.

General overview of the cross-border exchange of electronically signed documents between the JSC “RZD” and Belarusian Railways information management systems

Direction: from BCh towards JSC “RZD”

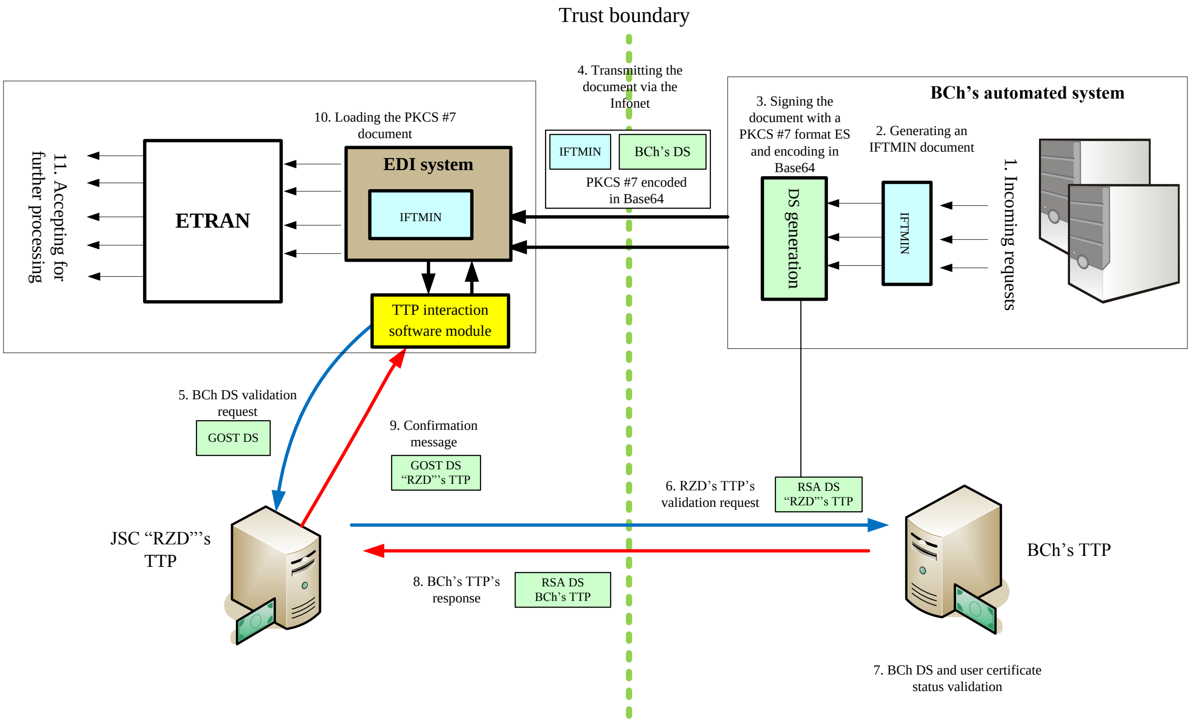
Trust boundary
4. Transmitting the document via the Infonet
IFTMIN
BCh’s DS
PKCS #7 encoded in Base64
BCh’s automated system
3. Signing the document with a PKCS #7 format ES and encoding in Base64
2. Generating an IFTMIN document
1. Incoming requests
DS generation
IFTMIN
10. Loading the PKCS #7 document
EDI system
IFTMIN
ETRAN
11. Accepting for further processing
TTP interaction software module
5. BCh DS validation request
GOST DS
9. Confirmation message
GOST DS “RZD”’s TTP
6. RZD’s TTP’s validation request
RSA DS “RZD”’s TTP
JSC “RZD”’s TTP
BCh’s TTP
8. BCh’s TTP’s response
RSA DS BCh’s TTP
7. BCh DS and user certificate status validation

Fig. 6. General overview of the cross-border exchange of electronically signed documents between Russian Railways’ and Belarusian Railways’ information management systems (starting from the Belarusian side).

6. Based on the RZD staff member’s request, RZD’s TTP generates its own BCh signature validation request, signs it with an RSA-based key, and sends it to BCh’s TTP.
7. BCh’s TTP validates the received signature and the authenticity of the BCh staff member’s certificate.
8. BCh’s TTP sends a confirmation message containing validation results and signed with an RSA key back to RZD’s TTP.
9. Based on the confirmation received from BCh’s TTP, RZD’s TTP generates a confirmation message for the RZD staff member, signed by RZD’s TTP’s certificate with the use of Russian encryption algorithms.
10. The TTP interaction software module extracts the data from the PKCS #7 document in the IFTMIN format and passes it on to the recipient for further processing.
11. The recipient, being an ETRAN AS user, receives the document for further processing in accordance with the accepted procedures.

6.3.2. Cross-border legally binding e-document flow between RZD and UZ.

In accordance with the Agreement on Private Empty Freight Car Transportation Service between Ukraine and the Russian Federation, Conducted via Paperless Technology Using Electronic Document Flow signed on the 21st of January, 2013, empty freight car transportation services are carried out between JSC "RZD" and UZ with the use of electronic waybills.

During the interaction with UZ, much like with BCh, AIGTR waybills are transmitted in the form of UN/EDIFACT electronic documents (IFTMIN messages) via the circuits of InfoNet-21 data transmission network.

In contrast with the Belarusian interaction scheme, DS validation during the interaction with UZ doesn't require the use of TTP services and is based on the interaction of Trusted Certificate Authorities (TCAs) from each side and the exchange of state-approved encryption algorithms and electronic signature tools.

The DS used in the domestic information management systems of either party (e.g. by its carriers and goods agents) isn't passed on across the border. In order to arrange for cross-border cooperation, the sending party generates an IFTMIN message containing the electronic data exchange marker and signed using their DS key intended for cross-border interaction, as well as the DS key provided by the cooperating party. The IFTMIN message is passed through the EDI system together with the electronic signatures it is signed with.

Trust in the received document is predicated on validation of the two signatures the IFTMIN message delivered to the recipient is signed with. The validation also includes sending of a certificate revocation status validation request to the sending party's TCA.

The successful validation result of both of the DSs enables the receiving party's TCA to generate a confirmation message for the document's recipient, confirming that the document may be cleared for further processing.

The interaction mechanics between Russia and Ukraine is explored in further detail below (see also Fig. 7).

The preliminary step (step 0) preceding the electronic carriage document exchange is the exchange of DS tools, public keys, and the parties' TCA' certificates.

General overview of the cross-border exchange of electronically signed documents between the JSC "RZD" and Ukrainian Railways information management systems

Direction: from Russia towards Ukraine

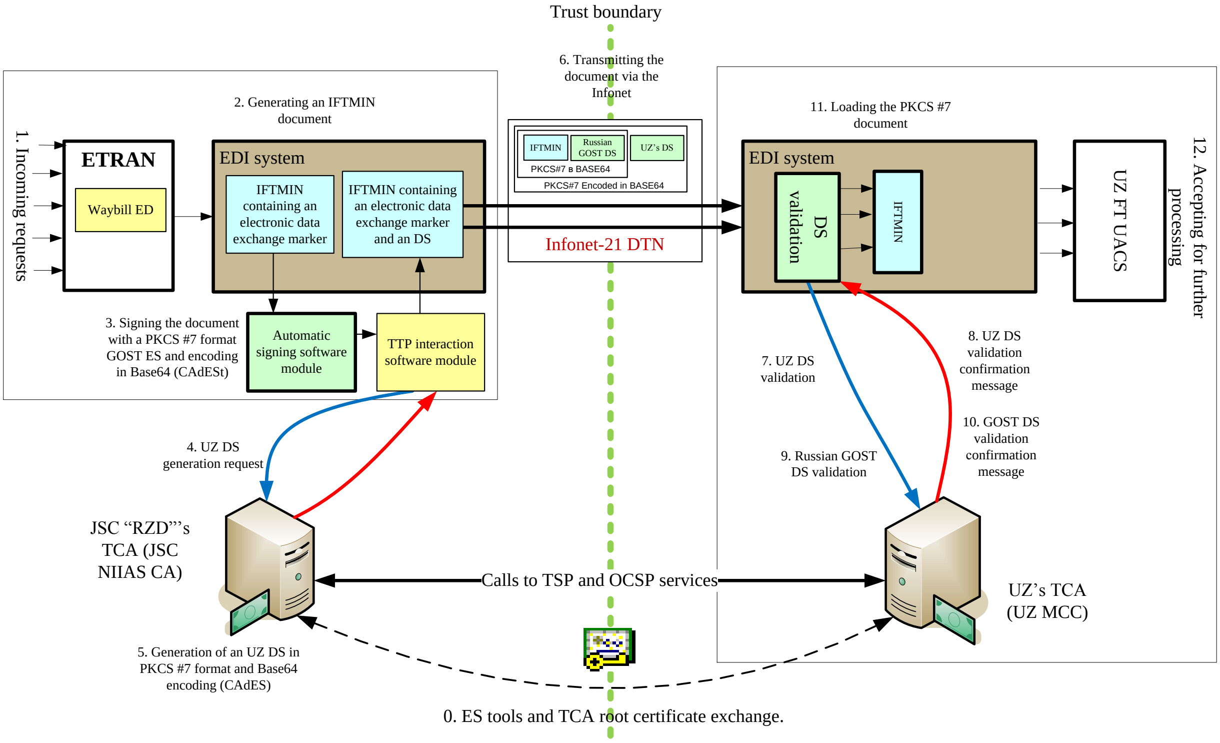
Trust boundary
6. Transmitting the document via the Infonet
2. Generating an IFTMIN document
11. Loading the PKCS #7 document
1. Incoming requests
ETRAN
Waybill ED
EDI system
IFTMIN containing an electronic data exchange marker
IFTMIN containing an electronic data exchange marker and an DS
IFTMIN
Russian GOST DS
UZ's DS
PKCS#7 в BASE64
PKCS#7 Encoded in BASE64
Infonet-21 DTN
EDI system
DS validation
IFTMIN
UZ FT UACS
12. Accepting for further processing
3. Signing the document with a PKCS #7 format GOST ES and encoding in Base64 (CAdESt)
Automatic signing software module
TTP interaction software module
7. UZ DS validation
8. UZ DS validation confirmation message
10. GOST DS validation confirmation message
9. Russian GOST DS validation
4. UZ DS generation request
JSC "RZD"'s TCA (JSC NIIAS CA)
Calls to TSP and OCSP services
UZ's TCA (UZ MCC)
5. Generation of an UZ DS in PKCS #7 format and Base64 encoding (CAdES)
0. ES tools and TCA root certificate exchange.

Fig. 7. General overview of the cross-border exchange of electronically signed documents between Russian Railways' and Ukrainian Railways' information management systems (starting from the Russian side).

1. An electronic waybill for cross-border carriage is prepared in ETRAN AS based on the incoming carriage requests.
2. The EDI system generates an IFTMIN message (a railroad waybill) with an electronic data exchange marker.
3. The EDI system then sends the message to be automatically signed with an DS based on RZD's key intended for cross-border document signing. The signature is generated in PKCS #7 format and packed together with the rest of the data and a time-stamp in CAdES format.
4. The TTP interaction software module sends a request to RZD's TCA to generate an DS based on the public key provided by UZ.
5. RZD's TCA generates an DS based on the key provided by UZ in PKCS #7 format and encoded in BASE-64 (CAdES), then returns the signed document to the EDI system.
6. The document is then transported through the transport subsystem of the EDI system using EDIFACT to UZ's automated system via the InfoNet-21 DTN.

7. UZ’s AS generates a validation request for the UZ signature attached to the document and sends it to their TCA.
8. UZ’s TCA validates the UZ DS and sends a confirmation message with the result to UZ’s AS.
9. Similarly, UZ’s AS generates and sends an RZD DS validation request.
10. Based on the RZD DS validation results, UZ’s TCA generates a confirmation message for the UZ AS user, signed with UZ’s TCA’s certificate.
12. UZ’s AS extracts the data from the PKCS #7 document in the IFTMIN format and passes it on to the recipient for further processing.
11. The recipient, being an UZ AS user, receives the document for further processing in accordance with the accepted procedures.

Figure 8 below describes the interaction mechanics between Ukraine and Russia from the Ukrainian side. The preliminary step (step 0) preceding the electronic carriage document exchange is the exchange of DS tools, public keys, and the parties’ TCA’ certificates.

General overview of the cross-border exchange of electronically signed documents between the JSC “RZD” and Ukrainian Railways information management systems

Direction: from Ukraine towards Russia

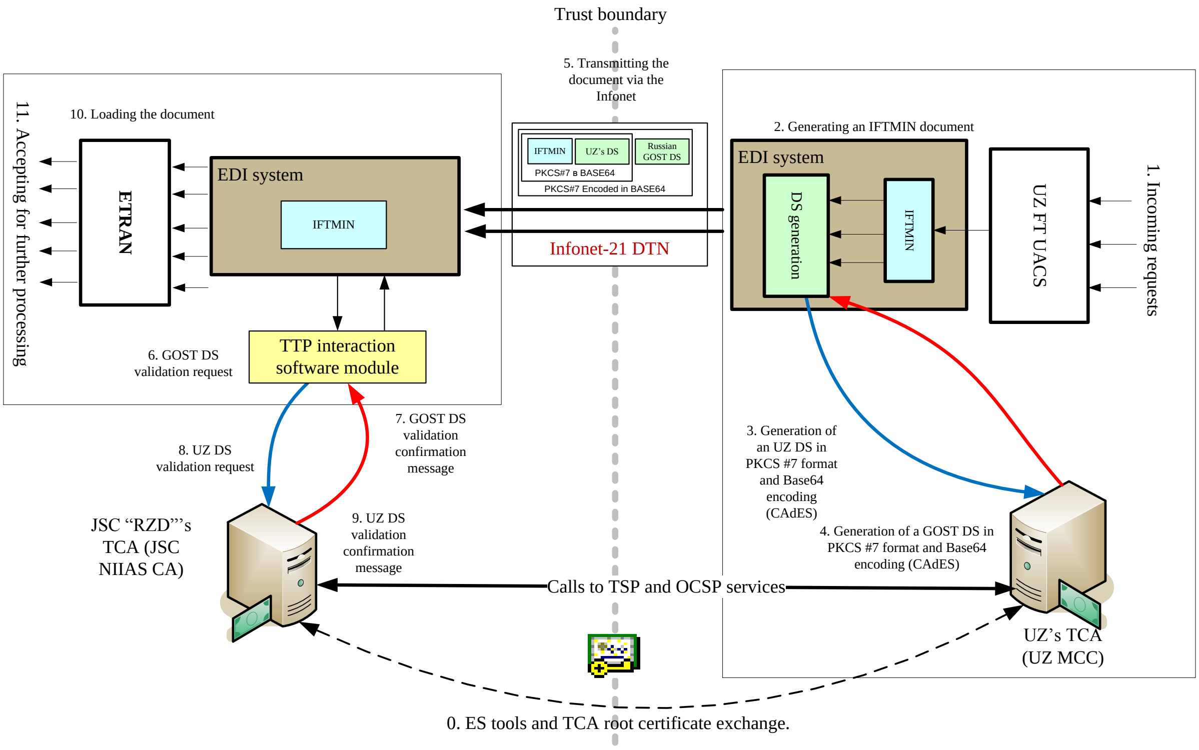
Trust boundary
5. Transmitting the document via the Infonet
IFTMIN
UZ’s DS
Russian GOST DS
PKCS#7 в BASE64
PKCS#7 Encoded in BASE64
Infonet-21 DTN
11. Accepting for further processing
10. Loading the document
ETRAN
EDI system
IFTMIN
6. GOST DS validation request
TTP interaction software module
2. Generating an IFTMIN document
EDI system
DS generation
IFTMIN
UZ FT UACS
1. Incoming requests
8. UZ DS validation request
7. GOST DS validation confirmation message
3. Generation of an UZ DS in PKCS #7 format and Base64 encoding (CAdES)
4. Generation of a GOST DS in PKCS #7 format and Base64 encoding (CAdES)
JSC “RZD”’s TCA (JSC NIIAS CA)
9. UZ DS validation confirmation message
Calls to TSP and OCSP services
UZ’s TCA (UZ MCC)
0. ES tools and TCA root certificate exchange.

Fig. 8. General overview of the cross-border exchange of electronically signed documents between Russian Railways’ and Ukrainian Railways’ information management systems (starting from the Ukrainian side).

1. An electronic waybill for cross-border carriage is prepared in UZ's AS.
2. The EDI system generates an IFTMIN message (a railroad waybill) with an electronic data exchange marker.
3. The EDI system then sends the message to UZ's MDC TCA to be automatically signed with an DS based on UZ's key intended for cross-border document signing. The signature is generated in PKCS #7 format and packed together with the rest of the data and a time-stamp in CAdES format.
4. Similarly, a request is sent to generate an DS based on a Russian encryption algorithm (conforming to GOST).
5. The document is then transported through the transport subsystem of the EDI system using EDIFACT to RZD's EDI system via the InfoNet-21 DTN.
6. RZD's EDI system generates a validation request for the GOST signature attached to the document and sends it to their TCA.
7. RZD's TCA validates the GOST DS and sends a confirmation message with the result to RZD's EDI system.
8. Similarly, RZD's EDI system generates and sends an UZ DS validation request.
9. Based on the UZ DS validation results, RZD's TCA generates a confirmation message for the RZD user, signed with RZD's TCA's certificate.
10. RZD's EDI system extracts the data from the PKCS #7 document in the IFTMIN format and passes it on to the recipient via ETRAN AS for further processing.
11. The recipient, being an ETRAN AS user, receives the document for further processing in accordance with the accepted procedures.

6.3.3. Cross-border legally binding e-document flow between RZD and KTZ.

The proposed technical solution assumes that both the data exchange parties interact only with the TTP located in their own domain, conforming to the home jurisdiction's legislative requirements and the TTP interaction agreement's requirements. The DS itself is validated in the domain of the issuer's signature certificate's origin; the other party accepts it without further validation taking place on its end. The trust towards the document on the receiving end is predicated on the confirmation message from its local TTP resulting from validating the DS of the issuer's TTP who validated the initial document.

At the same time, data exchange between the two TTPs (requests and responses) is conducted using electronic signatures made using the RSA encryption algorithm and the SHA-1 hashing algorithm, whereas the exchange between a TTP and its customer's information management system is done using state-approved encryption algorithms specified by the local jurisdiction.

The distinguishing trait of this interaction scheme is the lack of a direct interaction between the two parties' TTPs. Sending party's TTP's confirmation messages are generated at the moment of being signed on the sender's end rather than at the moment of validation on the receiver's end. The corresponding confirmation is attached to the document being transmitted and is sent to the receiving party.

The interaction mechanics between Russia and Ukraine is explored in further detail below (see also Fig. 9).

General overview of the cross-border exchange of electronically signed documents between the JSC "RZD" and AO NK KTZ information management systems

Direction: from Russia towards Kazakhstan

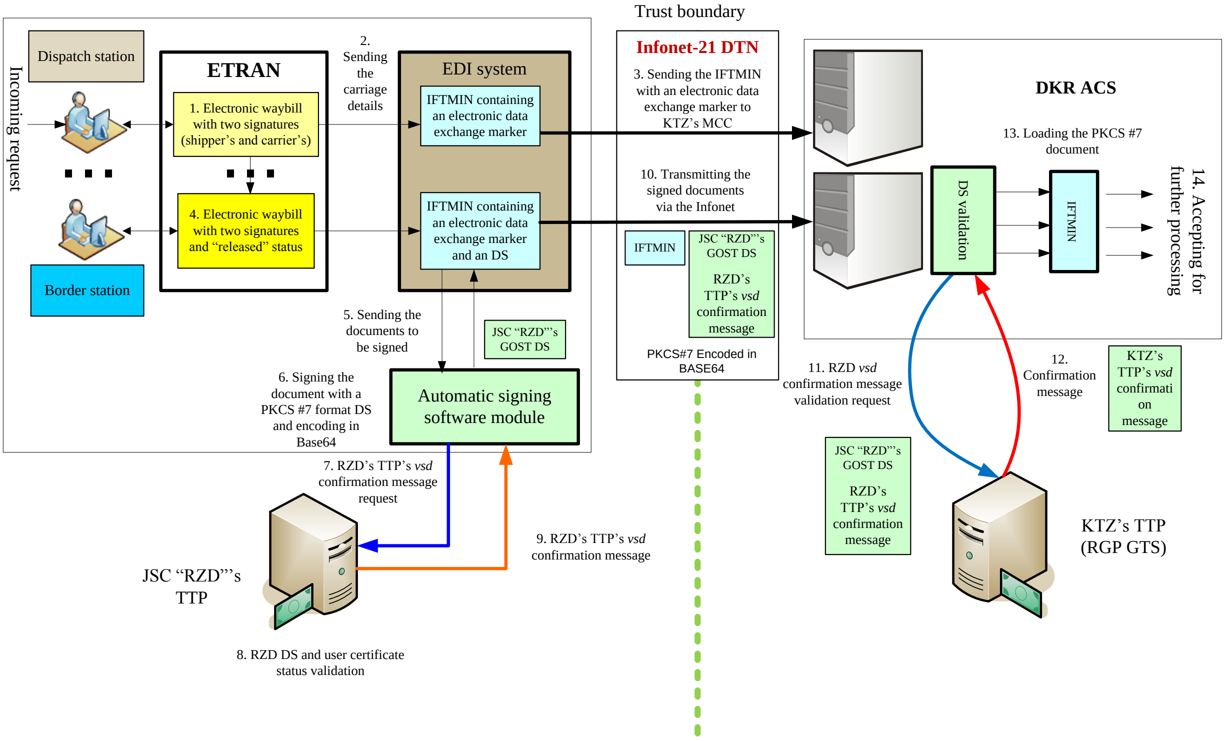
Trust boundary
Dispatch station
Incoming request
Border station
ETRAN
1. Electronic waybill with two signatures (shipper's and carrier's)
4. Electronic waybill with two signatures and "released" status
2. Sending the carriage details
EDI system
IFTMIN containing an electronic data exchange marker
IFTMIN containing an electronic data exchange marker and an DS
5. Sending the documents to be signed
JSC "RZD"'s GOST DS
6. Signing the document with a PKCS #7 format DS and encoding in Base64
Automatic signing software module
7. RZD's TTP's *vsd* confirmation message request
JSC "RZD"'s TTP
8. RZD DS and user certificate status validation
9. RZD's TTP's *vsd* confirmation message
Infonet-21 DTN
3. Sending the IFTMIN with an electronic data exchange marker to KTZ's MCC
10. Transmitting the signed documents via the Infonet
IFTMIN
JSC "RZD"'s GOST DS
RZD's TTP's *vsd* confirmation message
PKCS#7 Encoded in BASE64
DKR ACS
13. Loading the PKCS #7 document
DS validation
IFTMIN
14. Accepting for further processing
11. RZD *vsd* confirmation message validation request
12. Confirmation message
KTZ's TTP's *vsd* confirmati on message
JSC "RZD"'s GOST DS
RZD's TTP's *vsd* confirmation message
KTZ's TTP (RGP GTS)

Fig. 9. General overview of the cross-border exchange of electronically signed documents between Russian Railways' and Kazakh Railways' information management systems (starting from the Russian side).

1. An electronic waybill for cross-border carriage is prepared in ETRAN AS based on the incoming carriage requests.

2. Upon generation of the electronically signed waybill, the carriage details, including the electronic data exchange marker, are passed on to the EDI system.
3. The EDI system generates an IFTMIN message (a railroad waybill) with an electronic data exchange marker and sends it to the border station; the message is transmitted by the accepted means and in accordance with the EDP agreement at KTZ’s MDC upon processing of the carriage document at the station handling acceptance for carriage of the goods in question (carriage information).
4. At a border station, upon concluding the necessary technical procedures pertaining to the station’s operation, the information from the waybill is released and passed from ETRAN AS to the EDI system with the electronic data exchange marker and the “released” status.
5. Upon receiving the electronic waybill with the “released” status and the electronic data exchange marker, the EDI system generates and sends an IFTMIN message to be automatically signed with an DS based on RZD’s duty holder’s certificate.
6. The IFTMIN format text document is signed using the key intended for cross-border document signing. The signature is generated in PKCS #7 format and packed together with the rest of the data. The signature must contain a time-stamp.
7. The automatic signing software module sends an RZD DS validation confirmation message generation request to RZD’s TTP.
8. RZD’s TTP validates the signature attached to the document and generates a *vsd* confirmation message containing validation results and signed with an RSA key.
9. The *vsd* confirmation message is attached to the ED and put into an unsignable attribute of the DS.
10. The document is then transported through the transport subsystem of the EDI system using EDIFACT to KTZ’s automated system (DKR ACS) via the InfoNet-21 DTN.
11. KTZ’s AS extracts the RSA-signed RZD DS validation *vsd* confirmation message from the ED, and sends a validation request to KTZ’s TTP.
12. KTZ’s TTP validates the DS confirmation message issued by RZD’s TTP and sends a confirmation message containing validation results back to DKR ACS.
13. DRK ACS extracts the data from the PKCS #7 document in the IFTMIN format and passes it on to the recipient for further processing.

14. The recipient, being a DRK ACS user, receives the document for further processing in accordance with the accepted procedures.

General overview of the cross-border exchange of electronically signed documents between the JSC "RZD" and Belarusian Railways information management systems.

Direction: from Kazakhstan towards Russia

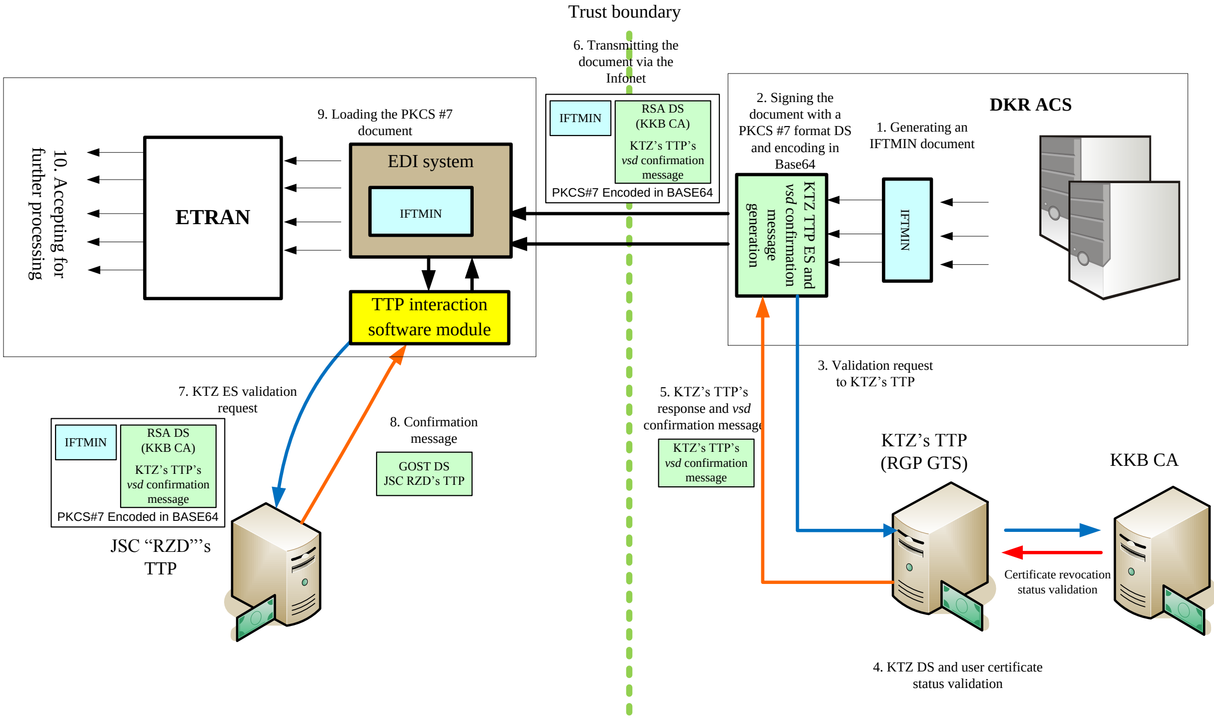
Trust boundary
6. Transmitting the document via the Infonet
IFTMIN
RSA DS (KKB CA)
KTZ's TTP's *vsd* confirmation message
PKCS#7 Encoded in BASE64
2. Signing the document with a PKCS #7 format DS and encoding in Base64
1. Generating an IFTMIN document
DKR ACS
KTZ TTP ES and *vsd* confirmation message generation
IFTMIN
9. Loading the PKCS #7 document
EDI system
IFTMIN
ETRAN
10. Accepting for further processing
TTP interaction software module
7. KTZ ES validation request
IFTMIN
RSA DS (KKB CA)
KTZ's TTP's *vsd* confirmation message
PKCS#7 Encoded in BASE64
JSC "RZD"'s TTP
8. Confirmation message
GOST DS JSC RZD's TTP
5. KTZ's TTP's response and *vsd* confirmation message
KTZ's TTP's *vsd* confirmation message
3. Validation request to KTZ's TTP
KTZ's TTP (RGP GTS)
KKB CA
Certificate revocation status validation
4. KTZ DS and user certificate status validation

Fig. 10. General overview of the cross-border exchange of electronically signed documents between Russian Railways' and Kazakh Railways' information management systems (starting from the Kazakh side).

Figure 9 describes the interaction mechanics between Kazakhstan and Russia from the Kazakh side.

1. The EDI system generates an IFTMIN message (a railroad waybill) with an electronic data exchange marker.
2. The IFTMIN message is signed in DKR ACS using the KTZ AS duty holder's key.
3. DKR ACS then generates and sends the signed IFTMIN message to KTZ's TTP for DS validation.
4. KTZ's TTP validates the ED signature and generates a confirmation message containing validation results and signed with an RSA key.
5. The *vsd* confirmation message signed by the RSA key of KTZ's TTP is attached to the ED and put into an unsignable attribute of the DS.

6. The signed document containing the confirmation message is then transported through the transport subsystem of the EDI system using EDIFACT to RZD’s EDI system via the InfoNet-21 DTN.
7. RZD’s EDI system sends an DS validation request to RZD’s TTP.
8. RZD’s TTP extracts the RSA-signed KTZ DS validation confirmation message from the ED, validates its DS, and sends an DS confirmation message to RZD’s EDI system.
9. RZD’s EDI system extracts the data from the PKCS #7 document in the IFTMIN format and passes it on to the recipient via ETRAN AS for further processing.
10. The recipient, being an ETRAN AS user, receives the document for further processing in accordance with the accepted procedures.

7. Requirements for trust infrastructure nodes – TTP complexes

7.1. Legal aspects of cross-border interfaces according to the requirements of local laws (of the country of residence of the TTP).

There are numerous constrains for e-documents management in international railway transportation. The main factor is the incompatibility of the EDS systems of OSJD member states due to differences in the applied standards, protocols and technical specifications. As a result, a digital signature applied using certified facilities of one member state may not be validated and accepted using the certified DS facilities of another state.

Thus, in order to organise a data exchange between the railways of OSJD member states using EDS, solutions to the following problems are required:

- A mechanism for recognising the legal value of documents signed using EDS must be created; the credibility of certificates issued in different legal environments must be ensured; respective legal and regulatory documents need to be signed between the interacting parties.
- Interaction needs to be organised between specialised software and hardware developed by parties operating in different legal environments in order to assure the exclusivity of legitimately used cryptographic algorithms;
- The technical conditions for transferring, processing and checking e-documents signed using EDS need to be provided.

In order for an international document to be recognised and accepted in all countries participating in e-document management, this document needs to bear signatures based on cryptographic algorithms recognised in the respective countries. Hence, each participant of e-document management needs to have two EDSs, so that e-documents can be recognised both within the home country and abroad.

In addition, in Russian and the CIS countries, the legal relevance and applicability of EDS for certifying documents and transactions are defined by the laws, regulations and agreements between the individual parties.

Therefore, organising legally valid cross-border digital interfaces does not seem possible without an exchange of cryptographic algorithms (or the selection of a uniform data exchange algorithm). Nor would it be possible without relevant agreements and contracts being executed, both at the government level and at the level of interaction among business entities.

7.2. Recommendations for selecting optimal variant for organising cross-border e-document flow.

We offer the creation of cross-border e-document flow based on the compilation of bilateral data exchange agreements between various countries, an analysis and summary of the legal aspects of the cross-border use of EDS from the point of view of the laws of Poland and EurAsEC, CIS practices and e-commerce practices.

Let us briefly define the subjects and levels of legal relations, as well as the principles of legal acts supporting the rights and responsibilities of each party to this process. First, an e-document or an aggregation of such documents is the subject of legal relations. Second, legal regulation focuses on the relations between the participants in cross-border exchanges.

These relations are as follows: provisional entities A and B (each operating within its own jurisdiction) enter into relations pertaining to the exchange of legally effective documents. Entity A transfers its e-document via an interface with its counterparty (Partner) B. During this process, each of its participants (A and B) interacts with its own TTP (TTP A and TTP B).

The TTP has three objectives:

1. To receive correspondence from Client A, enter it into the in-coming e-documents register for cross-border transmission; check that the validity of its electronic signature has been confirmed as of the moment of its transmission via the communications system to the jurisdiction of the country of Client B.
2. To confirm the validity of Signature A to the other TTP (TTP B) by way of an electronic apostille stamp comprising the details of TTP A, as well as the date and time of its generation, certified by the signature of a TTP A official, and transmit it via network to the address of TTP B.

3. To inform Client A about operations with its ED by sending confirmation (receipt) in the event that the contract provides for it.

The TTPs of participants A and B (TTP A and TTP B) shall accept electronic documents (messages), record their receipt and check and validate the electronic signature (apostille) in their registers.

7.3. Defining the list of organisational and legal documents for cross-border flows of electronic documents.

The legal framework underpinning cross-border data exchange involves executing the respective agreements. In this case, they should be of two types: agreements between each of the clients (TTP services user) with the respective TTP, and agreements between each TTP and its foreign counterparty (in this case, between TTP A and TTP B).

However, these agreements are not sufficient for full-fledged legal relationship between participants A and B, which may be either legal entities or the public authorities of different countries. International legal acts are required to regulate the procedure of cross-border data exchange.

An international legal act such as an International Convention for Cross-Border Interface Based on Electronic Documents (Messages) and Electronic Signature may provide the broadest information space. Countries participating in the Convention by ratifying it would commit to creating the appropriate infrastructure and legal framework within the context of their national laws. Another document will be required in order to assure the transition from a Convention like this one to specific agreements between operators in partner states – a standard agreement between operators acting in the countries participating in the Convention.

Figure 11 shows interaction and systemic interconnection of legal acts governing services for validating electronic signatures during cross-border data exchanges between entities based in two or more participating countries.

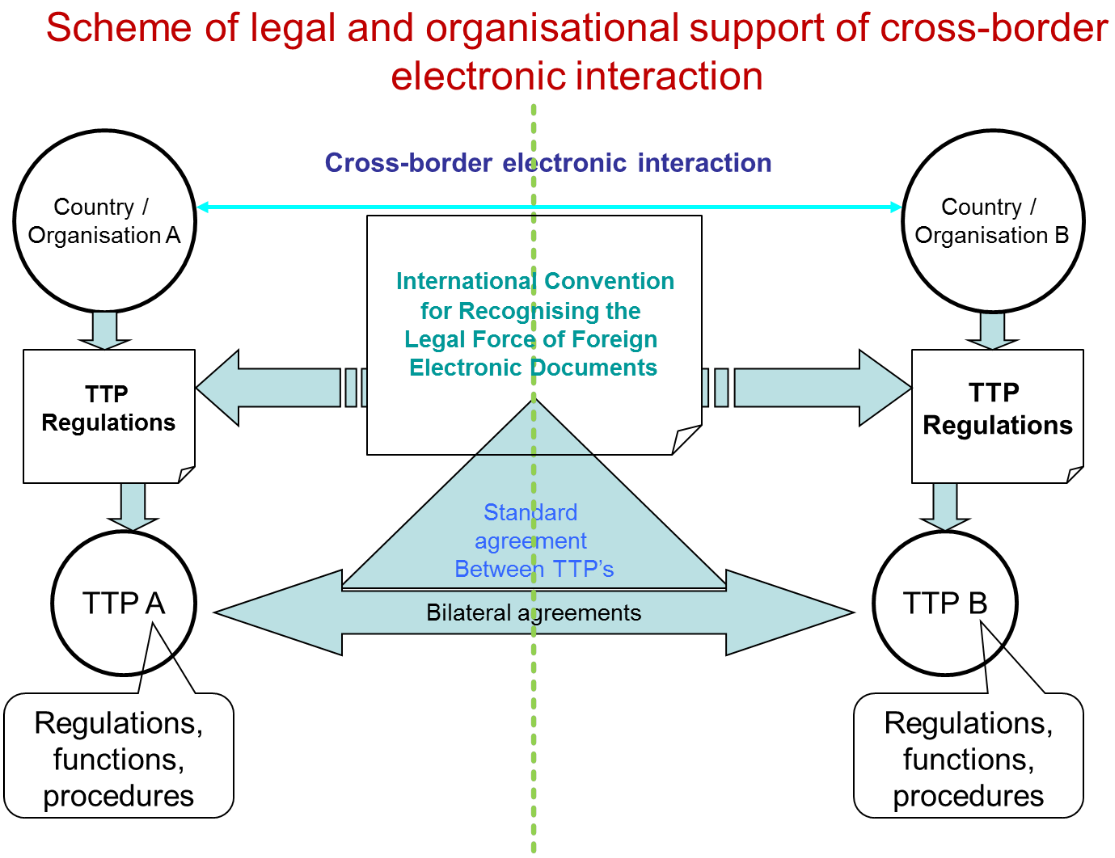
Scheme of legal and organisational support of cross-border electronic interaction
Cross-border electronic interaction
Country / Organisation A
Country / Organisation B
International Convention for Recognising the Legal Force of Foreign Electronic Documents
TTP Regulations
TTP Regulations
Standard agreement Between TTP's
TTP A
TTP B
Bilateral agreements
Regulations, functions, procedures
Regulations, functions, procedures

Fig.11. Scheme of legal and organisational support for cross-border electronic interaction.

The proposed Convention should stipulate for all types of legal documents providing for cross-border data exchange based on electronic digital signatures (EDS). The respective TTP Regulations of each participating country defining the functions, operations and availability of administrative and technical regulations required by national laws should support the documents stipulated by the Convention.

The preparation of the legal framework described above will require a number of issues to be solved. First, the participants should develop a common understanding of the level of the Convention and the procedure for adopting it. We believe there is a need for a body that it authorised to adopt a legal act that will cover the broadest information space. Second, it is important to define the sphere of powers and responsibilities of cross-border trust organisations. Third, it is important to define the scope of the operator's control: only the electronic signature, or the content of the document as well.

In addition, it is important to set the rule that the operator cannot claim ownership rights with respect to registers maintained and circulated across the network by this operator. However, the operator will be responsible for the safekeeping and integrity of such registers, as well as for the confidentiality of data within the network it operates.

It will be important for each country participating in the proposed Convention to decide on the organisation of the TTP service. It should provide for operational interface with their validation centres, confirming the validity of public key certificates at the time the electronic document enters the counterparty's legal environment. The TTP organisation shall be responsible for the reliability and timeliness of data provided to other parties in the cross-border mechanism for a specific recipient in accordance with the terms of the relevant agreement between specific TTP organisations.

The proposed model will allow the specific features of the national laws of participating countries to be aligned with the general requirements for the cross-border exchange of electronic documents (messages).

7.4. Technical and organisational requirements for the operation of TTP complexes.

For the purposes of standardisation, there should be uniform requirements for the interaction of TTPs. This means defining interfaces and interaction formats so that the subjects of one TTP can communicate reliably with the subjects of another TTP. It also means creating interconnected TTP network. Uniform requirements for requesting TTP services, providing data for validation and verifying results should form the basis of the TTP-user interface. With respect to the cryptographic facilities of EDS generation and validation, the level of interconnection between the validation processes carried out by means of EDS validation and TTPs needs to be established. They may either be connected, or remain independent, with priority given to validation by TTPs.

The respective security policy for TTPs needs to be developed, covering all security aspects in relation to TTP management and maintenance. The responsibilities of TTP and TTP services users should be separate and clearly defined. The obligations and responsibilities of TTPs should be compatible with their financial capabilities. Appendix No. 1 provides an example of a standard agreement between TTPs. The standard service agreement shall form the basis for defining the separate responsibilities of TTP and its users.

A necessary condition for the further development of TTP services is the development of a harmonised methodological framework and supporting tools that allow for:

- the readiness and compatibility of different information systems of the interacting parties for cooperating with TPP services to be evaluated;
- the quality and accessibility of TPP services to be evaluated.

References

[1] trict.tomsk.gov.ru/core/download?objectURI=597 [Internet].

[2] http://tools.ietf.org/html/rfc3447 [Internet].

[3] http://tools.ietf.org/html/rfc2560 [Internet].

[4] http://tools.ietf.org/html/rfc6960 [Internet].

[5] http://tools.ietf.org/html/rfc2315 [Internet].

[6] http://tools.ietf.org/html/rfc2630 [Internet].

[7] http://tools.ietf.org/html/rfc5652 [Internet].

[8] http://tools.ietf.org/html/rfc2510 [Internet].

[9] http://tools.ietf.org/html/rfc4210 [Internet].

[10] http://tools.ietf.org/html/rfc6712 [Internet].

[11] http://tools.ietf.org/html/rfc5246 [Internet].

[12] http://www.ietf.org/rfc/rfc4634 [Internet].

[13] http://tools.ietf.org/html/rfc5280 [Internet].

[14] http://tools.ietf.org/html/rfc6818 [Internet].

[15] http://www.rfc-editor.org/rfc/rfc3029.txt [Internet].

[16] http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf [Internet].

[17] http://www.w3.org/TR/xkms2/ [Internet].

[18] http://www.etsi.org/deliver/etsi_ts/102200_102299/102231/03.01.02_60/ts_102231v030102p.pdf [Internet].

Appendix 1

TTP Services Cooperation Agreement
For Organising the Mutual Recognition of Electronic Signatures
During Cross-Border Electronic Document Flow

The Trusted Third Party Service of Open Joint-Stock Company “Russian Railways” represented by ______________________________ acting on the basis of the Regulations (Charter), hereinafter referred to as “TTP A”, and the Trusted Third Party Service of ____ represented by ______________________________ acting on the basis of the Regulations (Charter), hereinafter referred to as “TTP B”, and jointly referred to as “the Parties”, entered into the Agreement hereof with regard to the following:

1. SUBJECT OF AGREEMENT

The subject of the Agreement hereof shall be as follows:

1.1. The procedure for interaction between the Parties and terms of data exchange between the Parties for recognising the legal effect of foreign electronic documents and their signatures during cross-border data exchange.

1.2. The assurance of trust guarantees for electronic documents certified by the Party in the same jurisdiction as the recipient, recognising the legitimacy of using electronic signatures in incoming and/or outgoing electronic documents in accordance with the norms and requirements of the national law of the country in which the Trusted Third Party is resident.

2. TERMS AND DEFINITIONS

For the purposes of this Agreement, the Parties shall use the following terms and definitions:

2.1. Electronic Document Recipient means a person/entity in receipt of a the signed electronic document according to the intent of its Issuer, except for entities acting as a Trusted Third Party or other operators acting as intermediaries with respect to the electronic document in question.

2.2. Electronic Document Issuer means a person/entity, that has drafted/signed and/or sent an electronic document for storage if required (or on behalf of which this has been done), except for entities acting as a Trusted Third Party or other operators acting as intermediaries with respect to the electronic document in question.

2.3. The system of legally effective electronic document management (LEEDM) means the information systems of the Parties that provides for the exchange of electronic documents using EDS and in which actions of the participants shall be regulated by separate agreements and contracts.

2.4. The Trusted Third Party (TTP) service means an organisation empowered in accordance with the national law of the country of residence of each Party or in accordance with an agreement between the Parties to perform validation of electronic signatures in electronic documents at a fixed point of time with respect to the Issuer and/or the Recipient of the respective electronic document.

2.5. Electronic document means a formalised record of data in electronic format certified by an electronic signature and complying with the rules and requirements for documentation established by the Parties.

2.6. Electronic signature means a piece of electronic data paired or associated with another piece of electronic data being signed, used to identify the signatory.

3. RIGHTS AND OBLIGATIONS OF THE PARTIES

3.1. This Agreement shall be gratuitous due to equivalence of rights and responsibilities of the Parties with respect to each other.

3.2. The Parties undertake to comply with the document exchange procedures in accordance to the terms of this Agreement.

3.3. Each Party under this Agreement shall act and do business in accordance with its national laws and within its established powers.

3.4. In terms of standardisation, the requirements for interaction among TTPs shall be uniform, meaning the interface and format of interaction need to support reliable connection between the subjects of one TTP and those of another TTP, as well as support an interconnected TTP network. Uniform requirements regarding requests for TTP services and formats to provide data for validation and to provide validation outcomes shall form the basis of the TTP-user interface.

3.5. The Parties shall have the following rights:

3.5.1. To transmit information about TTP services at the request of the respective authorised entities and organisations entitled to receive such services within the established procedures and effective laws of the Parties.

3.5.2. To suspend data exchange on the terms and conditions set by the technical regulations for performing maintenance checks and preventive maintenance.

3.5.3. To render other services in addition to those listed in Clause 3.6.12 hereof in connection with the organisation of legally binding electronic document management.

3.6. The Parties of this Agreement shall have the following mutual obligations:

3.6.1. To provide mutual guarantees and ensure the trustworthiness of electronic documents in the context of cross-border exchange; assure the legitimacy of the use of electronic signatures and methods of protecting incoming and/or outgoing electronic documents in accordance with the national law of the country of residence of each Party hereto.

3.6.2. To provide, in accordance with the national law of the country of residence of each Party hereto, the other Party (on the terms of mutual exchange) with all the required regulations and software (interfaces) for checking electronic documents received from the other Party and/or validation of their electronic signatures.

3.6.3. To perform automated validation/certification of its own electronic documents and/or their electronic signatures at the requests of other Parties, along with electronic receipts.

3.6.4. To legalise all transit electronic documents and their respective receipts generated by the other Party based on the results of their automated check by way of validating or certifying them in accordance with the requirements of the national law of the Party, where the respective electronic document (message) needs to be used.

3.6.5. To perform an expert evaluation and check of electronic signatures in electronic documents for their authenticity and compliance with the requirements of the national law; issue expert evaluation certificates in accordance with the procedures established by the national law of the Party's country of residence.

3.6.6. When validating/certifying its own electronic documents and/or their electronic signatures, each Party shall generate a respective electronic receipt and transmit it to the other Party in the established way.

3.6.7. Electronic receipts shall contain the following data:

- The electronic signature of the TTP's authorised person, on behalf of which validation/certification of the respective electronic document was performed listing his (her) name, surname and position;
- official details of the TTP Service;
- registration number of the electronic receipt, date and time of its generation.

3.6.8. Each Party hereto shall maintain an updated and secure electronic register (database) for recording all validations/certifications of electronic documents (message) or their electronic signatures and all electronic receipts.

3.6.9. The electronic register shall include the following data:

- the registration number of the electronic receipt;
- the date and time the electronic receipt was generated and the entry registered;
- attributes and details of the validated/certified format and circulation of the electronic document and/or its electronic signature;
- electronic receipt with the electronic signature of TTP's authorised person, on behalf of which the validation/certification procedure was performed with regard to an electronic document – name, surname and position;
- other additional data (e.g., confirmation by the recipient that the electronic document has been received).

3.6.10. Each Party shall maintain an automated record of all its actions and processes in the LEEDM system of the respective Party and of the TTP providing the respective services with step-by-step fixing of date and time;

3.6.11. Each Party shall, at the request of the other Party, perform an expert evaluation of the electronic signatures in electronic documents generated in its jurisdiction and provide the respective expert opinion to the other Party.

3.6.12. Each Party shall, at the request of the other Party, provide evidence of actions performed to deliver services:

- Confirmation of electronic documents sent by the issuer and/or received by the recipient;
- Confirmation that electronic documents have been validated/certified;
- Confirmation that the electronic signature has been validated;
- Confirmation of the results of the expert evaluation (check) of electronic signatures in documents;
- Confirmation that reference copies of electronic documents have been archived and deposited;
- Confirmation of other actions performed in connection with delivering TTP services.

3.6.13. In the process of delivering the services, each Party undertakes to follow security and confidentiality requirements with respect to the information contained in transit documents (messages) in accordance with international recommendations and the effective laws of the respective country.

3.6.14. Each Party hereto shall obtain all the required licenses, certificates and appraisal reports for delivering TTP services in case the effective laws of the respective country so require.

4. PROCEDURES FOR INTERACTION

4.1. The Parties shall independently organise interaction with their LEEDM systems that participate in cross-border data exchange. At the same time, the Parties shall not be responsible for direct interaction between the respective LEEDM systems if the procedure for cross-border data exchange provides for such interaction.

4.2. The Parties agree to recognise the legal force of electronic documents from issuers within the jurisdiction of the counterparty that are generated in compliance with the norms and requirements of the respective national laws, if the electronic document has an electronic receipt of the issuing Party that has been generated in accordance with international recommendations ITU-T X.842 “Information Technology – Security Techniques – Guidelines for the Use and Management of Trusted Third Party services”.

4.3. To organise information interaction, the Parties shall use the following data exchange protocols and unified formats of data presentation:

- RFC 3029. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS);

- RFC 2560. Online Certificate Status Protocol – OCSP;
- RFC 3161. Time-Stamp Protocol (TSP).

4.4. In order to undergo the legalisation procedure, interested users shall forward the respective electronic documents to the Party hereto, in the jurisdiction where they are located, indicating the electronic address of the final recipient.

4.5. The Regulations for Interaction agreed by the Parties (Appendix 1 hereto) shall form the basis for legalising electronic documents and their electronic signatures by the Parties, as well as for the engineering and technology interface of the Parties' TTPs.

4.6. The Parties shall validate or certify the integrity and authenticity of electronic documents and/or the compliance of their electronic signatures with the norms and requirements of the respective national law, unless otherwise stipulated by an international treaty.

4.7. The Parties shall not validate or certify the compliance of the content of electronic documents (messages) with the norms and requirements of the respective national law, unless otherwise stipulated by an international treaty.

4.8. The Parties shall recognise that the data protection facilities used by the Parties provide sufficient security and integrity of electronic documents and allow entities/persons, on behalf of which electronic signatures are used in accordance with the norms and requirements of the national law of each Party's country, to be identified.

5. RESPONSIBILITIES OF THE PARTIES

5.1. The Parties shall be liable for the improper performance of their obligations hereto in accordance with the requirements of the respective national law.

5.2. When transmitting documents (messages) received from third parties, the Parties shall be responsible for the accuracy and timeliness with which the said documents (messages) are processed, the integrity and consistency of the data in the document (message) that has been received and transmitted, and the confidentiality of the information contained within. The Parties shall not be liable for the content of electronic documents (messages), unless otherwise stipulated by an international treaty.

5.3. Each Party shall be liable for the actions of persons/entities authorised by such Party to perform the established procedures or TTP services during the process of legalising and signing electronic documents.

6. SETTLEMENT OF DISPUTES

6.1. The Parties undertake to follow the pre-court settlement procedure for disputes and disagreements arising from this Agreement.

6.2. The issuer or the recipient of electronic documents (hereinafter referred to as “the applicant”) shall have the right to file a claim. Claims to the Party to this Agreement must be filed in the applicant’s country of residence.

6.3. One Party shall submit the claim received from the applicant to the other Party (“the responding Party”) in writing and signed by the authorised representative of the Party submitting the claim. The claim shall contain:

- The applicant’s case;
- A statement of the facts that form the basis for the applicant’s claim, and the evidence confirming such facts with reference to the relevant legislation;
- A list of supporting documents and other materials appended to the claim;
- Any other information that might be required to settle the dispute.

6.4. The responding Party shall review the claim within _______ days of its receipt. Should additional documents be required to review the claim, the responding Party shall request such documents from the Party that submitted the claim. This request shall contain the deadline for submitting such documents. If the documents are not received by the established deadline, the respondent Party shall review the claim based solely on the previously submitted documents.

6.5. The respondent Party shall submit a response to the claim, signed by an authorised representative, to the Party of the applicant. Failure to submit such a response within __________ days of receiving the claim shall be understood as a refusal to satisfy the claim.

6.6. Disputes between the Parties relating to the interpretation and/or application of the provisions hereof shall be resolved, in the first instance, through negotiations and consultations.

6.7. In the event that the Parties fail to settle the dispute through negotiations and consultations within six months of the formal written request for negotiations/consultations to be held being sent by one Party to the other, then, unless another agreement concerning the methods to settle such a dispute exists between the Parties, either of the Parties shall be entitled to file this dispute for litigation to the appropriate court of the country of the railway company against which the claim has been filed.

7. FORCE MAJEURE

7.1. The Parties shall be exempt from liability for partial or complete failure to fulfil their obligations hereunder if such failure is the result of force majeure circumstances that occurred after this Agreement was signed, or as the result of extraordinary events, including: equipment failures and breakdowns; software failures or errors; and defects, failures or breakdowns of communication systems, power supply units, air conditioning and other life-support systems that are necessary for the successful implementation of obligations under this Agreement – if the Parties were not able to foresee or prevent such circumstances.

7.2. In the event that a force majeure circumstance arises, the deadlines for the Parties to fulfil their obligations hereunder shall be shifted proportionately to the period that such circumstances, and their consequences, persist.

7.3. A Party that is unable to fulfil its obligations as the result of a force majeure situation shall notify the other Party immediately about the scale and nature of such situation, when it began and when it finished.

7.4. The Party claiming that a force majeure situation prevented them from fulfilling their obligations hereunder in a timely manner shall be responsible for providing evidence of such circumstances.

7.5. After the force majeure situation has been dealt with, the Parties shall undertake all necessary measures to eliminate the consequences of, and mitigate the damage caused by, the force majeure situation.

8. DURATION OF THE AGREEMENT

8.1. This Agreement shall enter into effect upon its signing by both Parties and shall stay in effect until _______________. The date established by the regulatory documents (instructions) of the Parties as the commencement date for exchanging electronic documents with electronic signatures shall be considered the official starting date.

8.2. The Agreement shall be automatically for twelve (12) months at the end of each calendar year, unless one of the Parties provides the other Party with written notice stating its intent to terminate the Agreement one (1) month prior to the expiration of the period indicated above.

9. TERMINATION OF THE AGREEMENT

9.1. The Parties shall be entitled to unilaterally terminate this Agreement after notifying the other Party in writing ________ days prior to such termination. The Agreement shall be understood as terminated ________ days after the date that such notice was sent.

10. CONFIDENTIALITY

10.1. Information contained in electronic documents shall be understood as confidential, unless the owner of such information states otherwise, and shall not be disclosed to third parties. The Parties undertake to maintain the confidentiality of such information and not disclose it to any third party.

11. MISCELLANEOUS

11.1. Any agreements between the Parties pertaining to relations regulated herein and implying the need to amend this Agreement shall be confirmed in writing by the Parties in the form of supplementary agreements.

11.2. In the event that international or bilateral inter-state treaties or other legal acts regarding the matters regulated by this Agreement are adopted, the respective provisions hereof shall be amended through the execution of a supplementary agreement within 30 days of the day that such legal acts come into force.

11.3. Amendments and supplements hereto may be introduced by way of supplemental agreement between the Parties executed in writing and signed by authorised representatives of the Parties.

12. **SCHEDULED TO THE AGREEMENT** (to be additionally developed by interacting Parties)

Schedule No. 1: Regulations for the Interaction of TTP Services When Using Hardware/Software Systems for Organising the Mutual Recognition of Electronic Signatures during Cross-Border Electronic Document Flow.