Technological aspects of the trust in cross-border paperless exchange

V N Kustov¹ and E S Silanteva²

¹ Informatic and Information Security Department, St. Petersburg state Railways University of Emperor Alexander I, 9 Moskovsky Ave., Saint Petersburg, North-Western Federal district, 190031, Russia
² LLC "NST", 107078, Moscow, Orlikov lane, house 5, building 2, floor 09, room 34, Russia

E-mail: kvnvika@mail.ru, ceo@newspaceoftrade.com

Abstract. To operate high quality expert and decision support systems we need to use data that could be trusted. Given differences in technical, legal, and administrative environments, cross-border paperless exchange poses significant challenges to the data validation. These challenges could be overcome due to the provision of the trust to the technologies used to exchange data across borders. That is why this article discusses trust technologies that allow cross-border data exchange in electronic form. The article provides a brief description of advantages and disadvantages of the three main validation protocols: DVCS, XKMS, and OASIS DSS. As the main form to provide trust in cross-border documents exchange we propose trusted third party (TTP) technology. Hardware and software aspects of the TTP implementation in the form of hardware and software package are described in the article with the examples of successful implementation of cross-border electronic legally significant documents flow implementation.

1. Introduction

1.1. Relevance of the issue

Currently, the concept of trust is inextricably linked with the concepts of validation service and trusted third party (TTP). Let's try to turn to the history of the TTP concept.

The historical roots of the TTP concept come from Byzantium and Ancient Rome, as it was studied in the works of N. P. Lyapidevsky [1]. He described the application of Roman law in the legal practice of Western Europe, and did not forget about the scribes (scribae) of ancient Rome [2], mentioned the era of the Byzantine Empire with its tabillions, the Roman Forum and its tabulary, the ecclesiastical notary, the barbarian tribes, and ended up by describing a notary in Italy.

So, we can see that even in ancient times there were groups of people who were engaged in the professional development of various documents, and provided legal assistance. This activity is gradually structured into a professional, and becomes a public character. Thus, in the Institute of tabellions [2], introduced for the first time in Byzantine society, a class of citizens appeared, endowed with the following rights and duties:

1) Carry out legal activities controlled by the state.
2) Provide legal services to any person who has applied for such assistance.
3) The official document issued by the tabellion had increased evidentiary force, and the legal force of such a document could not be disputed.

Tabellions were engaged in the official registration of the documents they drew up in order to give them legal force and ensure their protection from loss. Only a free Roman citizen with the necessary legal knowledge and skills could be given the opportunity to become a tabellion.

Consequently, we see that the institution of TTP has been used since ancient times as a mediator for resolving conflict situations in the sphere of interaction between citizens and the state and citizens with citizens. The further development of civil society only increased the relevance of the existence of the TTP.

1.2. Current status
In the era of the advent of computer technology and the further development of data transmission methods over communication channels, a new purpose of TTP appears, first formulated in the standard X. 842 ("Recommendations X. 842: Guidelines for the use and management of TTP services", which was developed by the International telecommunications Union) [2].

TTP is defined in this document as "... an organization or its agent that provides one or more security services that is trusted by other entities as a provider of these services". TTP is being used to provide additional services for organizations or individuals seeking to increase the level of reliability and confidentiality of services consumed or provided to ensure secure communication with business partners and the ability to create, transmit and save the necessary confirmations to restore the course of events.

The main TTP services and their purpose (based on Recommendation X. 842) are presented in the table 1.

**Table 1. Basic TTP services (based on Recommendation X. 842).**

| №  | Service name                                      | Purpose of the service                                                                 |
|----|--------------------------------------------------|----------------------------------------------------------------------------------------|
| 1  | Timestamp Service                                | Setting timestamps based on global standards (State service for time, frequency and determination of Earth rotation parameters - SSTF, GLONASS and GPS) |
| 2  | Service for Managing Certificates and E-signature Keys | Ensuring the lifecycle of certificates and e-signature keys                              |
| 3  | Attribution Service                              | Providing information about changes in attributes (for example: passport data, access rights, personal data, property rights) |
| 4  | Identification and Authentication Service         | Verification of IDs (identification) and confirmation of rights (authentication) of the subject |
| 5  | Personalization Service                          | Personalization of the record of the e-signature key as well as the certificate of the e-signature verification key on a personal electronic medium |
| 6  | Access Control Service                           | Granting access only to an authorized user (authorization)                              |
| 7  | Non-rejection service                            | Recording facts and providing evidence of their completion                              |
Broadcast Service
Ensuring TTP-TTP interaction (cross-border interaction)

Archiving Service
Providing long term archival storage of electronic documents

Notary Service
Certification of legal documents based on their legal status, performing an intermediary role in resolving disputes

As for the functions of the notary service, it is necessary to take into account the role of the TTP in disputes, for example, when challenging:

1) Facts of sending and/or delivering an electronic document (e-document).
2) Time of sending and/or delivery of the e-document.
3) Context of the sent/delivered e-document.
4) Authenticity of the e-document and/or its hard copy.
5) Integrity and reliability of the e-document.
6) Identification of the subject who put an e-signature under the e-document.
7) The Authority of the subject who put an e-signature under the e-document.
8) Validity of the subject's authority to use the e-signature verification key certificate.

1.3. Prospects

Among the promising areas of use of services that provide the functionality of TTP and are currently actively developing, more generally, it should be noted:

1) **Service for Building the Trusted Interaction Environment.** The service provides users with a trusted platform, where they can perform legally significant actions, sign e-documents with an e-signature and perform e-signature verification. In the case of a conflict, a user has the opportunity to make a request to an accredited organization that provides this service, and is liable for errors and damages caused by it related to verification of the e-signature.

2) **Long-Term Storage (Archiving) Service.** The service is designed to provide remote secure storage of e-documents with verification of the legitimacy of e-documents at the time of creation of an e-signature.

3) **Secure Interaction Service.** A service at the infrastructure telecommunications level provides a connected resource that is protected using e-signature tools.

4) **Service of Cross-Border Interaction.** The service is designed to ensure cross-border interaction of subscribers located in the zones of different jurisdictions in order to confirm the authenticity of their e-signatures, as well as certificates of e-signature verification keys.

Technology does not stand unaltered, there are more and more new directions and discoveries. In processing and storing e-documents, modern distributed registry technology (blockchain) and related smart contracts technology are becoming increasingly important. Many new national-scale digital platforms are being created on the basis of blockchain [7]. The creation of Digital state in the near future is no longer a dream. The scale of application of TTP services in such a state becomes almost immense.

2. **Comparative evaluation of validation protocols**

Currently, 3 main validation protocols are used in international practice: XML Key Management Specification (XKMS) [11], OASIS Digital Signature Service (DSS) [12], Data Validation and Certification Server (DVCS) [4].

Comparative analysis of XKMS, OASIS DSS, and DVCS protocols is necessary to identify the most effective approaches to implementing processes, technical characteristics and ways to implement validation processes for certificates and signed documents.

In the process of comparative analysis, we will try to pay special attention to how effectively each of the compared protocols will solve the following problems:
• Validation of the electronic-signature (e-signature) under the document;
• Validation of the certificate of the e-signature verification key;
• Provision of the validation process results in the prescribed form (in the form of receipts), that could be used in resolving conflict situations as evidence of certain actions in relation to an e-document or an e-signature at a fixed time.

Based on this, we have determined the following main parameters of the compared protocols, that will be used for comparison:

1) Types of the requests to the service.
2) The transport protocol that is used
3) The type of signature that can be verified.

Interaction of individuals and legal entities with state bodies, interdepartmental interaction in state authorities carried out in accordance with the established procedure. The document presentation format (XML format) is defined, as well as the type of e-signature used (CMS signature or XML signature, depending on the interaction subjects and their information systems). Documents in PDF format signed by the e-signature in PADES format are also widely distributed.

The interaction of state bodies in the framework of the transboundary trust space of the Eurasian economic Union is carried out in the prescribed manner in accordance with international law of the Eurasian economic Union will be identified and clearly defined format for the presentation of documents (XML format) and the format to use electronic signatures (XMLDSig, XADES). Ability to verify the signature without providing the document itself (for example, by hash).

4) Possibility of checking and forming a time stamp.
5) Ability to process two or more e-signatures in one e-document.
6) Speed of processing the request to check the e-signatures.
7) Complexity of implementation.
8) Legal validity of the verification result
9) Applicability of the Protocol to ensure cross-border confidence.

Let's look at the most significant characteristics of the compared protocols.

2.1. XML Key Management Specification
XKMS describes protocols for registering and distributing e-signature verification keys that are used in accordance with the XML signature and XML Encryption standard. XKMS defines two services – XML Key Registration Service Specification (X-KRSS) and XML Key Information Service (X-KISS). XKMS does not require any specific public key infrastructure (for example, X. 509), but it is compatible with such infrastructures.

X-KISS allows the client to delegate tasks required for processing the <ds: KeyInfo> XML signature elements to the XKMS service. The main purpose of the Protocol is to simplify applications that use XML signatures.

X-KRSS provides tools for managing PKI information and registering the owner's public key. The user can use this Protocol to make a request to link the information provided to the public key. The information provided may include the owner's name and other information required for linking.

XKMS is a Protocol that authenticates the applicant and, if the keys are generated directly by the user, the Protocol can confirm ownership of the electronic signature key. The registration service provides the user with the opportunity to transfer the electronic signature key to the user if the keys are created by the registration service.

XKMS can register both DSA and RSA keys and has the ability to connect and use other cryptographic systems, such as elliptic curves and various implementations of the Diffie-Hellman algorithm.

XKMS has features of various types of canonization, which complicates the process of developing a solution based on it.
An XKMS message exchange consists of a sequence of one or two request-response pairs. Messages have a common format that can be supported by different protocols. For interoperability, it is recommended that those implementing XKMS implement SOAP support over HTTP.

It is possible to link with other protocols.

XKMS defines three types of requests:
1) X-KISS Request – a request for location or validation as prescribed by X-KISS;
2) X-KRSS Request - a request to register, reissue, revoke or restore as prescribed by X-KRSS.
3) Composite request - consists of one or more X-KISS or X-KRSS requests.

XKMS supports two process modes – synchronous and asynchronous:
1) Synchronous - the service responds to the request that it has fulfilled its obligation and will not issue any more responses in relation to this request.
2) Asynchronous - the service will not finish responding to the request immediately and will notify you that the request has not yet been met and subsequent responses will be published.

The disadvantages of the protocol are that it:
• requires a large amount of memory to parse large e-document;
• requires additional processing in the form of data containers;
• it slow in operation;
• does not support PDF signatures (ETSI TS 102 778 PADS).

2.2. OASIS Digital Signature Service

OASIS is an organization that develops information standards, promotes industry consensus, and creates global standards in the fields of security, Internet technology, cloud computing, energy, information technology, emergency management, and other areas.

OASIS Digital Signature Services (DSS) is fully ratified as an OASIS specification and consists of:

1. Basic Module.
2. Profiles DSS:
   2.1. XML Timestamp Profile;
   2.2. Signature Gateway Profile;
   2.3. Profile of an Item Instance executed in accordance with German Law;
   2.4. Electronic Printing Profile;
   2.5. Profile of E-Stamp;
   2.6. Abstract Profile for Code-Signing;
   2.7. J2ME Code-Signing Profile;
   2.8. Asynchronous Processing Abstract Profile;
   2.9. Advanced E-Signature Profiles.

The base Module uses DSS profiles to describe the main most commonly used protocols and scenarios.

Signature and verification protocols are mainly used for creating and verifying XML signatures, binary timestamps, XML timestamps and CMS signatures. These protocols can also be used for other types of signatures, such as PGP signatures.

The disadvantages of the Protocol include:
• the fact that it cannot provide a report for each signature in the e-document with multiple signatures;
• it does not support PDF e-signatures (ETSI TS 102 778 PADS).
2.3. Data Validation and Certification Server (DVCS) Protocols
The DVCS protocols are described in the Request for Comments (RFC) 3029. This document provides a detailed description of the DVCS, as well as the protocols for communicating with it. DVCS represents TTP, which can be used as the main element when creating reliable authorship verification services.

RFC3029 defines 4 certification and data verification services:
- Certification of Possession of Data (CPD);
- Certification of Claim of Possession of Data (CCPD);
- Validation of Digitally Signed Document (VSD);
- Validation of Public Key Certificates (VPKC).

The CPD is a data ownership certificate service for confirming that the requester had the data at the specified time, and that this data is submitted to the Data Verification Server.

CCPD also confirms claims of data ownership, but uses only the hash function value, not the data itself.

The VSD service for document instance verification is used when you need to confirm the validity of a document. The service checks electronic signatures in a document using the required certificate data and their status for an instance of this document using signature verification keys. The service also verifies the cryptographic correctness of the electronic signatures in the document and also checks whether to trust the signatories, e.g. checking the certificate chain of documents from the signatories to a trusted point (the CA that issued the certificate and the certificate on the DVCS server or the root CA in a hierarchy).

Certificate validity verification can be performed using both the Certificate Revocation List (CRL) and to-date information, such as the Online Certificate Status Protocol (OCSP), or accessing a trusted directory or other DVCS services. Failure to validate one of the e-signatures does not necessarily cause the entire verification to fail.

A CMS signature can be used as an item instance, as well as a PDF signature, since it is based on a CMS signature.

VPKC is a certificate verification service for item instance verification keys that is used to authenticate and validate one or more certificates at a specified time. When verifying the certificate, the DVCS item instance verification key verifies that the certificate included in the request is a valid certificate and determines its revocation status at the specified time. DVCS checks the entire certificate chain from the publisher to the root certificate authority. External information (CRL, OCSP, DVCS) can also be used for verification.

DVCS uses the standard ASN1-encoding.

The advantage of the DVCS Protocol is that it can encapsulate certificate validity, signature validity, and time stamp verification services in a single message.

The disadvantage is that the verification results cannot be opened with a text editor to view and copy information, and XML signatures cannot be verified.

At the moment, the TTP service of the Eurasian Economic Commission is successfully functioning on the basis of the DVCS Protocol.

2.4. The results of the comparison of characteristics of validation protocols
A comparative analysis of the protocols XKMS, OASIS DSS, DVCS is presented in the table 2. for clarity, each parameter is assigned a rating on a five-point scale, where the value " 1 " - the parameter does not allow you to solve the tasks, and the value " 5 " - the parameter allows you to solve the tasks.
Table 2. Comparative analysis of protocols.

| No | Parameter to compare | XKMS                                      | OASIS DSS                                 | DVCS                                      |
|----|----------------------|-------------------------------------------|-------------------------------------------|-------------------------------------------|
| 1. | Types of requests   | Validation of the XML signature;          | Creation the item instance;              | Certificate possession of data (CPD);     |
|    |                      | Registration of a key pair by the owner of the key pair | Verify the validity of the item instance; | Certificate the possession of data without providing it to the service (CCPD); |
|    |                      |                                          | Provision of a time stamp service        | Verify the validity of the ED signature (VSD); |
|    |                      |                                          |                                           | Verify the validity of the certificate (VPK) [RFC2459] |
|    |                      |                                          |                                           |                                           |
| Estimation | 3 | 4 | 5 |
| 2. | Transport protocol  | SOAP over HTTP                            | SOAP [SOAP];                             | The transport mechanism is optional, including: |
|    |                      |                                          | HTTP POST [RFC 2616];                    |                                          |
|    |                      |                                          | TLS [RFC 2246]                           |                                          |
|    |                      |                                          |                                           |                                          |
| Estimation | 2 | 5 | 5 |
| 3. | Type of signature that can be | XML signature                            | XML signature;                           | CMS signature                            |
|    |                      |                                          |                                           |                                           |
verified

- CMS signature (RFC 3852);
- Binary time stamp (RFC 3161);
- XML time stamp;
- Advanced signature (ETSI TS 101903 (XADES) and ETSI TS 101733 (CADES));
- PGP signature (RFC 2440);

| Evaluation | 3 | 5 | 4 |

4. Ability to verify the signature without providing the document itself (by hash)
   Evaluation | 1 | 5 | 5 |

5. Ability to check and generate a time stamp
   Evaluation | 1 | 5 | 5 |

6. Ability to process two or more signatures in one e-document
   Evaluation | 5 | 4 | 5 |

7. Speed of processing the signature verification request
   - Low, XML format carries a lot of redundant information
   - It is difficult to work with large files

| Evaluation | 3 | 4 | 5 |
Comparative analysis of the protocols shows that XKMS Protocol is the least acceptable for use as a prototype for developing domestic validation service solutions, since it has a number of limitations compared to other protocols, including the inability to check and generate a time stamp, which will

| Evaluation | Average | Average | Minimum |
|------------|---------|---------|---------|
| 8. The complexity of the implementation | 4 | 4 | 5 |
| 9. Legal significance of the validation result | Validation result could be signed by e-signature | Validation result could be signed by e-signature | Validation result could be signed by e-signature |
| 10. Applicability of the Protocol to ensure cross-border trust | Perhaps | Perhaps | Yes |
| 11. Evaluation disadvantages | 4 | 4 | 5 |
| — Requires a large amount of memory to parse large e-documents; | — Cannot provide a report for each signature in the e-document with multiple signatures; | You can't open it with a text editor to view and copy information |
| — Requires additional processing in the form of data containers; | — Does not support PDF signatures (ETSI TS 102 778 PADS) |
| — Slow in operation; | | |
| — Does not support PDF signatures (ETSI TS 102 778 PADS) | | |

Average score: 3.1, 4.5, 4.9
make it impossible to check advanced signatures. In addition, XKMS has lower performance compared to other protocols.

Protocol OASIS DSS can be used to solve the tasks, however, the most effective as a prototype is the DVCS Protocol, due to its simplicity, high performance, regulated content of the verification result, the possibility of building a TTP network both within the national segment and in cross-border interaction. In addition, based on the results of the expert evaluation, we can conclude that the DVCS Protocol has the best characteristics for solving the formulated tasks when comparing them with reasonable parameters.

3. Structure of the Software and Hardware Complex of the E-signature Validation Service

Recommendation X.842 very broadly defined the functions of the TTPs. Most of these services are currently performed by accredited certification authorities. The TTP functions are more narrowly defined in the RFC 3029 standard [4]. In this document, the main function of the TTP is to perform the data validation and certification service in accordance with the DVCS Protocol described in it. To fully perform the functions of the DVCS Protocol, the TTP must implement at least 2 additional services:

1) The time stamp service (TSP – Time-Stamp Protocol) described in RFC 3161 [5].
2) The Service of an online certificate status checking (OCSP), described in RFC 6960 [6].

In recent years, Russia has been actively developing hardware and software complexes (HSC) for validation services. According to the authors, one of the successful options for implementing the DVCS service is "The Litoria DVCS HSC" developed by Gazinformservice LLC. Let's take a closer look at its software and hardware complexes.

3.1. Litoria DVCS Trusted Third Party Services Software package

The Litoria DVCS Trusted Third Party Services (TTPS) software package (SP) [8] verifies the e-signature and the validity of the e-signature verification key certificate. The SP allows the user to create verification requests, analyze such requests, and generate a response containing information about the result of the verification.

The main task of the SP TTPS Litoria DVCS is to provide e-signature validation services for interdepartmental information interaction of information exchange participants in the conditions of ensuring the integrity and reliability of e-documents and their e-signatures.

In order to perform this task, the SP TTPS Litoria DVCS implemented the following functions:

1. Creating all DVCS requests (in accordance with RFC3029):
   - confirm e-signature of document (Validation of Digitally Signed Document – VSD);
   - verification of the validity of the signature key certificate (Validation of Public Key Certificates – VPKC);
   - certificate of possession of information at the specified time and providing it to the service (Certificate of Possession of Data – CPD);
   - certificate the information possession without providing it to the service (by hash) (certificate of Claim of Possession of Data – CCPD).
2. Checking all data contained in the request.
3. Formation:
   - time stamps
   - DVC receipts and their analysis in accordance with the requirements of the RFC 3029 recommendations.
4. Archiving and storage of:
   - user information
   - created DVC receipts with their serial numbers,
   - audit log files on the SP authentication server TTPS Litoria DVCS, containing the type, time and date of the event.
5. Providing a developer with software tools that facilitate creation of client applications such as:
   - SDK-client of the DVCS service – a software component that includes libraries (C++, C#) used for creating applications that use the DVCS service functionality;
   - The TSP service SDK client is a software component that includes libraries (C++, C#) used for creating applications that use time stamps in accordance with the requirements of the RFC3161 recommendations ("Internet X. 509 Public Key Infrastructure, Time-Stamp Protocol (TSP)").

The SP is based on the following international standards implemented in it:
1) RFC3029 "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS)";
2) RFC3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)";
3) RFC6960 "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP".

The SP includes the following components:
1) Authentication Service (DVCS);
2) Time-Stamp Service (TSP);
3) SDK client for the DVCS service;
4) SDK client for the TSP service;
5) AWP (automated workplace) of the administrator.

The scheme of functioning of the SP TTPS Litoria DVCS is shown in the figure 1.

![Figure 1](image-url)  
**Figure 1.** Scheme of functioning of the SP TTPS Litoria DVCS.

4. Example of cross-border paperless e-document interchange
A large number of cross-border paperless e-document interchange projects have already been implemented in Russia. Some of them are published in [9, 10]. Let's take a closer look at one of these projects.
As an example of implementation of cross-border paperless legally significant e-document interchange (EDI), the experience of two trade business partners from Belarus and Russia in organizing cross-border legally significant exchange of electronic trade related documents (TRDs) should be presented. A pilot project for the exchange and mutual recognition of TRDs was implemented by two EDI operators: from Belarus - LLC "Modern Technologies of Trade" (LLC "CTT") and from Russia – KORUS Consulting CIS. A structural diagram of the composition and relationships of the pilot project components is shown in figure 2.

Two operators of the e-signature verification service were engaged to verify the e-signature in TRDs: on the part of Belarus - the National Center for Electronic Services (NCES), and on the part of Russia - LLC "Certifying Authority GAZINFORMSERVICE" (LLC "CA GIS").

Let's take a closer look at the implemented EDI TRDs process between a product supplier from Belarus and a product buyer from Russia. The supplier from Belarus, when delivering the product, passes the TRDs signed by the e-signature created using the cryptographic standard of the Republic of Belarus, to the EDI operator LLC "CTT", which in turn passes the TRDs to the EDI operator from Russia - CORUS Consulting CIS. The latter determines when processing TRDs that they are signed by a foreign cryptography and cannot guarantee their legal significance in accordance with the legislation of the country where the e-document was created and signed. Next, CORUS Consulting CIS forms a request for checking the TRDs e-signature, and sends it for verification to LLC "CA GIS".

In turn, LLC "CA GIS" determines that the TRDs are signed with a Belarusian signature and sends a request for verification of the e-signature to the Belarusian TTP operator - NCES. The NCES verifies the Belarusian signature, generates a receipt for the verification results, signs it with its own e-signature, and passes this receipt to the Russian partner – LLC "CA GIS" - the operator of the e-signature verification service. LLC "CA GIS" checks the e-signature under the receipt and, if it is correct, signs it with its own e-signature in Russian cryptography. Then the receipt is sent to the Russian operator EDI KORUS Consulting CIS, which passes it along with the TRDs to the buyer. The buyer, based on the results of the check reflected in the receipt, makes a decision on accepting or refusing to accept the TRDs. This concludes the EDI process.

![Figure 2. Structural diagram of the composition and relationships of the pilot project components.](image-url)
5. Conclusion
The article discusses the technological aspects of implementing e-signature validation services. TTP technology is used as the main form of implementation of the validation service. The historical aspect of the origin of the concept of TTP is considered. The list of services implemented in the TTP and the composition of conflict situations in which TTP services may be in demand is provided. The advantages and disadvantages of the three main validation protocols: DVCS, XKMS, and OASIS DSS are also briefly described and compared. Based on the results of the comparative assessment, the main attention is paid to the DVCS Protocol. The hardware and software aspects of implementing the TTP based on the DVCS Protocol in the form of a hardware and software package "Litoria DVCS TTP Service" are considered. Example of successful implementation of cross – border electronic legally significant document exchange between Russia – Belarus is also considered.

References
[1] Lyapidevsky N P 1875 History of the notary Moscow Univ Tip (Katkov and Co.) Vol.1 (Preprint copy) 321 (in Russian)
[2] Khrustalev V K 2013 Roman scribes during the late Republic Moscow Scientific journal Series "Historical Sciences. History / Studia classica et mediaevalia" Bulletin of RSUH 17 (118) 224-228 (in Russian)
[3] ITU-T 2002 recommendation X.842 information technology security techniques guidelines for the use and management of trusted third party services (Geneva): https://www.itu.int/rec/T-REC-X.842
[4] Network Working Group February 2001 Request for Comments 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols: https://tools.ietf.org/html/rfc3029
[5] Network Working Group August 2001 Request for Comments 3161 Internet X.509 Public Key Infrastructure Time–Stamp Protocol: https://www.ietf.org/rfc/rfc3161.txt
[6] Network Working Group June 2013 Request for Comments 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP: https://tools.ietf.org/html/rfc6960
[7] Swan M 2015 Blockchain Scheme of the new economy (Moscow: Olymp-Business) 208
[8] Software package "Trusted Third Party Services Litoria DVCS" 2018 Program Description 72410666.00044-01 13 01 (Spb) 36
[9] Kustov V N and Kiryushkin S A 2020 Russia – TTP – Belarus: here the third is not superfluous: https://habr.com/ru/company/gaz-is/blog/470816/ (in Russian)
[10] Kustov V N and Kiryushkin S A 2020 How to establish a legally significant electronic document flow for contractors in Russia and Kazakhstan?: https://habr.com/ru/company/gaz-is/blog/492514/ (in Russian)
[11] XML Key Management Specification (XKMS 2.0) Version 2.0 28 June 2005 W3C Recommendation: http://www.w3.org/TR/2005/REC-xkms2-20050628/
[12] OASIS Digital Signature Service Core Protocols Elements and Bindings Version 2.0 31 May 2019 Committee Specification 01: http://docs.oasis-open.org/dss-x/dss-core/v2.0/cs01/dss-core-v2.0-cs01.docx