Krajowa Izba Rozliczeniowa S.A.

KIR CERTIFICATION POLICY
FOR
QUALIFIED TRUST SERVICES

Version 1.6

Document history

Version number	Status	Date of issue
1.0	Document approved by the Management Board of KIR – version valid from the moment of entering KIR on the Trusted List, under the Act on Trust Services and Electronic Identification of 5 September 2016 valid to the 9th of October 2018.	28.04.2017
1.1	Document approved by the Management Board of KIR – version valid from the 10th of October 2018.	10.10.2018
1.2	Document approved by the Management Board of KIR – version valid from the moment of entering KIR on the Trusted List, under the Act on Trust Services and Electronic Identification of 5 September 2016 as a provider of management service of signature creation date on behalf of users.	28.02.2019
1.3.	Document approved by the Management Board of KIR – version valid from the moment of entering KIR on the Trusted List, under the Act on Trust Services and Electronic Identification of 5 September 2016 as a provider of management service of signature creation date on behalf of users to the 31th of May 2021.	31.05.2019
1.4.	Document approved by the Management Board of KIR version valid from the 1st of June 2021 till the 27th December 2022	28.05.2021
1.5	Document approved by the Management Board of KIR version valid from the 28th December 2022 till the 20th March 2024.	21.12.2022
1.6	Document approved by the Management Board of KIR version valid from the 21st March 2024.	09.02.2024

LIST OF CONTENTS

1. FOREWORD

The “KIR Certification Policy for Qualified Trusted Services” hereinafter referred to as the “Policy”, replacing the “KIR Certification Policy for Qualified Certificates” and the “KIR Certification Policy for the Time Stamping Service” shall define detailed solutions, including technical and organisational concerning provision of qualified trusted services by Krajowa Izba Rozliczeniowa S.A., hereinafter “KIR”, consisting in issuance of:

1) qualified certificates for electronic signature,
2) qualified certificates for electronic seal,
3) qualified certificates for website authentication, hereinafter referred to as “certificates”;
4) qualified electronic time stamps, hereinafter referred to as “time stamps”;
5) generating and managing signature creation data and seal creation data on behalf of the subscribes;
6) generating qualified electronic signatures based on signature creation data managing by KIR on behalf of subscribers,
7) generating qualified electronic seals based on seal creation data managing by KIR on behalf of subscribers.

The CP also defines parties that participate in the process of provision of qualified trust services, their rights and obligations.

The CP shall be used for issuing and managing certificates and time stamps issued by KKIR, hereinafter referred to as “KIR,” as part of the Szafir Electronic Signature Support Centre.

The CP has been prepared on the basis of recommendations included in RFC 3647 (Certificate Policy and Certification Practice Statement Framework), and is aimed at satisfying the information needs of all those participating in the PKI infrastructure described herein and supported by KIR.

1.1. Introduction

Certificates and time stamps are issued by the Szafir Electronic Signature Support Centre. The CP defines the rules of their issuance, actions that are performed by certification authorities, registration authorities and subscribers, and relying parties.

KIR provides qualified trust services with regard to issuance of certificates and time stamps in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, hereinafter referred to as the “eIDAS Regulation”, the Act on Trust Services and Electronic Identification of 5 September 2016 (Journal of Laws from 2021, item 1797), hereinafter referred to as the “Act on Trust Services”, and this Policy.

Krajowa Izba Rozliczeniowa S.A., NIP: 526-030-05-17, entered in the register of entrepreneurs maintained by the District Court for the Capital City of Warsaw, 13th Business Division of the National Court Register, under No. KRS 0000113064.

Whenever the agreement for the provision of trust services with KIR consisting in the issuance of certificates or the issuance of time stamps or other documents have referred to time stamping, it should be understood as a qualified electronic time stamp service.

1.2. Document name and its identification

The CP has the following registered object identifier (OID: 1.2.616.1.113571.1.1.1):

`iso(1) member-body(2) pl (616) organization(1) id-kir(113571 ) id-szafir(1) id-kw(1)id-certPolicy-doc(1).`

The current and previous versions of the CP are published at the website: www.elektronicznypodpis.pl.

1.3. Participants in the PKI infrastructure described in the CP

The CP describes the entire PKI infrastructure necessary for the provision of qualified trust services that is operated at KIR. Its major participants are:

1) certification authority –COPE Szafir Qualified;
2) time stamping authority – Szafir TSA
3) registration authorities;
4) principals;
5) subscribers;
6) relying parties.

1.3.1. Certification authority

The Qualified COPE SZAFIR certification authority issues certificates for subscribers and provides information necessary for verifying the validity of certificates issued by it. The tasks involving acceptance of requests for issuance, and issuance of certificates, as well as acceptance of requests for suspension/ revocation of certificates are carried out by the registration authorities.

1.3.2. Time stamping authority

The time stamping authority provides a service of time stamp issuance. Tasks related to reception of registration and management shall be carried out by registration desks.

1.3.3. Registration authorities

The registration authorities carry out tasks related to the support of principals and subscribers. Their tasks include e.g.:

1) execution of agreements with the principals;
2) verification of identity of subscribers and their entitlement to receive certificates;
3) registration of subscribers using a service of time stamp issuance,
4) provision of the certificates to the subscribers;
5) acceptance and implementation of requests for suspension, revocation or change in the certificate status following suspension;

6) generation one–off activation codes for a mobile application.

Tasks foreseen for registration authority are done by authorized person hereinafter referred to as a “Operator”.

Tasks from 1 to 5 for registration desks will be performed by KIR organisational units. Tasks 1, 2, and 4, with respect to issuance of qualified certificates for electronic signature and qualified certificates for electronic seal, may be carried out only by banks co-operating with KIR pursuant to separate agreements. Tasks 2 and 5 with respect to issuance of qualified certificates for electronic signatures for which the signature creation data are managed by KIR on behalf of the subscribers may be carried out by banks cooperating with KIR pursuant to separate agreements.

The list of units carrying out tasks of registration authorities, together with their office hours, is available at the website: www.elektronicznypodpis.pl.

1.3.4. Subscribers

Only a natural person may be a subscriber in case of qualified certificates of an electronic signature.

According to eIDAS Regulation in case of qualified certificate for electronic seal a legal person, an organisational unit without corporate existence or a public law body or other legal entity, including a natural person, as long as it acts as a public law body or carries out business activities may be in particularly subscriber in case of qualified certificates for electronic seal.

A natural person, a legal person, or an organisational unit without corporate existence whose data has been entered or is to be entered into a certificate may be a subscriber in case of qualified certificates of websites.

In case of qualified certificates for electronic seal and certificates for websites authentication issued to entities other than a natural person actions provided for in the Policy for a subscriber, including confirmation of certificate collection, confirmation of having a public key, acceptance of certificate content, determination of PIN and PUK codes, mobile application activation or passwords to demand cancellation or suspension of a certificate shall be carried out by a person authorised by an ordering party. This person has also been charge with responsibilities relating to the protection of a private key till the forwarding the private key to the subscriber and, in the case of access to keys using a mobile application, the control and supervision of persons or devices using the keys.

1.3.5. Principals

The notion of principal means a natural person, a legal person or an organizational unit without legal personality that has concluded an agreement for the provision of trust services with KIR consisting in the issuance of certificates or the issuance of time stamps, hereinafter referred to as the “Agreement.” Pursuant to the Agreement, the principal may order certificates or authorize to use time stamping service for individual subscribers.

1.3.6. Relying parties

A relying party is understood as a natural person, a legal person or an organizational unit without legal personality that undertakes actions or makes any decision relying on data which is electronically or digitally signed or electronically attested with the use of a public key contained in the certificate issued by KIR or the time stamp issued by KIR.

The relying party should pay attention to the type of certificate, time stamp and the policy pursuant to which they has been issued. In case of doubts whether a specific certificate or time stamp has been issued correctly and whether it is used by an entity that is authorised to do so, the relying party is obliged to report such doubts to KIR. It may be reported by telephone at the hotline number available during office hours or with the use of a contact form available 24h/day at: www.elektronicznypodpis.pl.

1.4. Applications of the certificates

Qualified certificates for electronic signature are used to verify qualified electronic signatures and to identify subscribers.

Qualified certificates for electronic seal are used to verify qualified electronic stamps and to identify subscribers.

Qualified certificates for websites authentication are used to certify websites and assign them to a natural person or a legal person to whom a certificate has been issued.

A qualified electronic time stamp relies on an alleged data integrity and authenticity of the origin of data with which a qualified time stamp is linked.

1.4.1. Types of certificates and areas of use

No.	Certificate type	Recommended application
1	Qualified certificates for electronic signature	To verify qualified electronic signatures
2	Qualified certificates for electronic seal	To verify qualified electronic seals
4	Qualified certificates for websites authentication	To confirm reliability of servers and to confirm their authenticity. They allow setting up a TSL encrypted connection among servers with such certificates, and also providing clients with safe logging in. Certificates of that type may be issued only for servers operating in public networks and that have a full, clear domain name defining location of a specific nod in DNS (FQDN - Fully Qualified Domain Name).

All certificates issued under the CP should be used in accordance with their intended purposes and by entities authorised to do so. The certificates should be used in properly adapted applications that satisfy at least the following requirements:

1) proper security of the source code and work performed in a safe operational environment;
2) proper support of cryptographic algorithms, the hash function;
3) proper management of certificates, public and private keys;
4) verification of statuses and validity of certificates;
5) proper manner of informing the user about the state of the application, status of certificates and verification of electronic signatures.

1.4.2. Prohibited areas of use

Certificates issued under the CP cannot be used outside the stated areas of use. The use of certificates by unauthorised persons is also prohibited.

1.5. Time stamps usage

A time stamp is used to certify the date and time and integrity of data with which the date and time are linked.

1.6. Management of the CP

The CP is subject to changes depending on the business and technological needs. The current version of the CP has the binding status. The previous version of the CP is effective until the next binding version is published. Working versions are not published.

Works on amendments and updates of the CP are performed by an organizational unit of KIR responsible for the provision of qualified trust services. Organization responsible for the management of the CP:

Krajowa Izba Rozliczeniowa S.A.
ul. rtm. W. Pileckiego 65
02-781 Warszawa
Poland

1.6.1. Contact details

All correspondence related to the provision of qualified trust services shall be directed to the address of the registered office of KIR:

Krajowa Izba Rozliczeniowa S.A.
Departament Kontaktów z Klientami i Operacji [Customer Service Point]
ul. rtm. W. Pileckiego 65
02-781 Warszawa
with the annotation reading "usługi zaufania" [trust services]
tel. 0-801 500 207
e-mail: kontakt@kir.pl

or to the addresses of field branches of KIR, if so agreed or if so provided in the customer service procedure established by KIR.

1.6.2. Entities determining the validity of rules provided for in the CP

The current validity of the rules set forth in this document and in other documents concerning the provision of qualified trust services is the duty of the organizational unit of KIR that is responsible for the provision of trust services.

1.6.3. CP approval procedures

The CP is approved by the Management Board of KIR. Following the approval it receives the effective status with the indication of its effective date. It is published on the KIR websites on that date at the latest.

2. RESPONSIBILITY FOR THE PUBLICATION AND GATHERING OF INFORMATION

2.1. Repository

The information concerning qualified trust services provided by KIR, including information about the manner of concluding Agreements, handling orders for new certificates, and renewing, suspending and revoking certificates, handling orders for time-stamping service is made available to all interested parties at the KIR website at the following address: www.elektronicznypodpis.pl.

All certificates and time stamps that have been issued by KIR are kept at KIR for a period of 20 years from the issuing date.

2.2. Publication of information in the repository

The information is published in the repository either automatically or following the approval by authorised persons. Basic information that is published in the repository includes:

1) certificate of the Qualified COPE SZAFIR certification authority;
2) certificate of the SZAFIR TSA time stamping authority;
3) certificates issued by the Qualified COPE SZAFIR certification authority;
4) lists of suspended and revoked certificates (CRLs) issued by the Qualified COPE SZAFIR;
5) templates of agreements and orders, if applicable for a given type of service;
6) descriptions of procedures for obtaining, renewing, suspending and revoking certificates;
7) description of procedures of obtaining a time stamp;
8) current and previous CPs;
9) reports on audits carried out by authorised institutions;
10) Regulation of online renewal of qualified and non-qualified certificates;
11) Regulation of the mSzafir services of the National Clearing House S.A.,
12) Regulations of the seal Service mSzafir of the National Clearing House S.A.;
13) Regulation of KIR's on-line store;
14) additional information.

2.3. Frequency of publication

The frequency of publication of individual documents and data is presented in the table below:

	Certificates of certification authorities and certificates of a time stamping authority	Each time and immediately after the new certificates have been generated.
	CRLs	For the Qualified COPE SZAFIR – not less frequently than every 24 hours or after the suspension or revocation of the certificate. The lists are updated within 1 hour from the suspension or revocation of the certificate.

		The permitted period of delay of certificate suspension or revocation may be 24 hours.
	Templates of agreements and orders	Each time when they are amended or updated.
	Descriptions of procedures for obtaining, renewing, suspending and revoking certificates	Each time after the amendment or update of procedures.
	Description of procedures of obtaining a time stamp	Each time after a procedure change or update.
	Current and previous CPs	Pursuant to Chapters 9.10 – 9.12
	Reports on audits carried out by authorised institutions	Each time after audit completion and reception of the report.
	Additional information	Each time when it is updated or changed.

2.4. Repository access control

All information published in the repository at the KIR websites are available to all interested parties.

Information published in the repository is protected against unauthorised changes, additions and removals, and is kept with the storage of backup copies.

In case of any actions undertaken by unauthorised entities or persons that could violate the integrity of published data KIR shall immediately take legal measures against such entities, and shall exercise its best efforts to have proper data published in the repository again.

3. IDENTIFICATION AND AUTHENTICATION

This chapter governs the procedures for identification of subscribers that apply to KIR for the issuance of a certificate, including certificates for electronic signature or electronic seal for which signature creation data are managed by KIR on behalf of a subscriber and the procedures for verification of requests for suspension or revocation and creation of another certificate.

3.1. Names used in certificates and identification of subscribers

Based on the data obtained in the course of registration, an identifier is created in accordance with the diagram below that allows for the identification of the subscriber linked to the public key included in the certificate.

The subscriber's identifier for qualified certificates for electronic signature may contain the following components:

Meaning (abbreviation in the certificate)	**Value**
Country name* **(C)**	Two-letter country abbreviation
Voivodeship (S)	Name of the voivodeship of the headquarters of the organization with which the subscriber is associated
Name of town/city (L)	Name of town/city of the headquarters of the organization with which the subscriber is associated
Postal code (PostalCode)	Postal code of the headquarters of the organization with which the subscriber is associated
Street (Street)	Street, house number and optional premises number) of the headquarters of the organization with which the subscriber is associated

Common name (CN)	Name identifying the subscriber
Surname* (SN)	Subscriber's surname plus, possibly, their family name
Given names* (G)	Subscriber's given names
Serial number* (serialNumber)	Subscriber identifier in accordance with ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures,
Organization (O)	Name of the principal with which the subscriber is associated
Organizational unit (OU)	Name of the organizational unit with which the subscriber is associated

An identifier of the subscriber for qualified certificates for electronic seal may contain the following elements:

Meaning	Value
Country name*	Two-letter country abbreviation
Voivodeship (S)	Name of the voivodeship of the organization
Name of town/city (L)	Name of town/city of the headquarters of the organization
Postal code (PostalCode)	Postal code of the headquarters of the organization
Street (Street)	Street, house number and optional premises number) of the headquarters of the organization
Common name (CN)	Name identifying the organization for which the certificate is intended in accordance with the registration name
Organisation identifier* (organizationIdentifier)	Organization identifier in accordance with ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures,
Organisation* (O)	Name identifying the organization for which the certificate is intended in accordance with the registration name
Organisational unit (OU)	Name of the organisational unit with which the subscriber is associated

An identifier of the subscriber for qualified certificates for websites authentication may contain the following elements:

Meaning	**Value**
Country name*	Country name abbreviation.
Voivodeship (S)	Name of the voivodeship of the organization
Name of town/city (L)	Name of town/city of the headquarters of the organization
Postal code (PostalCode)	Postal code of the headquarters of the organization
Street (Street)	Street, house number and optional premises number) of the headquarters of the organization
Common name (CN)	Domain name
Surname** (S)	Surname of the subscriber plus, possibly, the maiden name.
First names** (G)	Subscriber's first names.
Organization identifier (organizationIdentifier)	Organization identifier in accordance with ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures,
Organisation (O)	Name identifying the organization for which the certificate is intended in accordance with the registration name
Organisational unit (OU)	Name of the organisational unit with which the subscriber is associated

Domain name* (domeinName)	Name of the Internet domain registered in the DNS system for which a certificate is issued

*- mandatory fields

** - only in case of certificates for subscribers who are natural persons, mandatory fields

The Subscriber Identifier is created on the basis of a sub-set of attributes indicated for a given type of the certificate.

The subscriber's identifier is created on the basis of the subset of the attributes indicated for this type of certificate, where the identifier cannot be empty within a given technical infrastructure in KIR.

The common name field may contain sequence of letters, digits and spaces, with the maximum length of 64 characters, that unambiguously identifies the subscriber.

The subscriber can have any number of certificates with the same subscriber's identifier.

3.1.1. Need to use meaningful names

In the order for certificate the principal should indicate data for the subscriber's identifier that allow for unambiguous identification of the subscriber. In particular, the Subscriber Identifier for an SSL certificate shall contain a Fully Qualified Domain Name (FQDN).

In the process of generating certificates KIR examines whether for a Subscriber Identifier indicated in the order a certificate for another subscriber has not been previously issued. If the identifiers are repeated, with the exception of issuing another certificate for the same subscriber, KIR shall refuse issuance of a certificate and propose a change of the Subscriber Identifier.

3.1.2. Ensuring anonymity to subscribers

KIR does not issue certificates that ensure full anonymity to subscribers. Regardless of the contents of the certificate, KIR still keeps the data identifying the subscriber.

3.1.3. Uniqueness of names

The subscriber's identifier is indicated by the principal in the order. The identifier should comply with the requirements set forth above.

Each issued certificate has its serial number which is unique within a specific certification authority. Together with the subscriber's identifier, this guarantees unambiguous identification of the certificate.

3.1.4. Recognition, authentication and role of trade marks

The subscriber's identifier should contain only names to which the subscriber has rights. KIR has the right to call upon the principal or the subscriber to present documents confirming their right to use the names recorded in the certificate order. The right to use a trade mark may be particularly confirmed with:

1) document issued or provided by a state authority;

2) information obtained from a reliable source.

3.2. Identification and authentication at first certificate issuance when electronic signature data are carried out on a device or generated by a subscriber

Prior to the issuance of the first certificate, saved with key pair on a device managed by subscriber or generated on the basis of a certification request presented by the subscriber for key pair generated by himself, the principal concludes the Agreement and delivers the order to KIR with the data necessary to prepare the certificate. The order for certificate may also be submitted via the KIR website. The Agreement and the order should contain data about the principal.

KIR checks the data of the principal and the authorisation of persons who have signed the documents on its behalf on the basis of information obtained from lawful and reliable sources, including the generally accessible registers kept by public authorities.

If it is not possible to confirm the identification data of the principal or if the persons are not authorised to represent the principal, the order and the Agreement are not accepted by KIR, and the principal is informed about this fact.

If the certificate is to contain an additional identifier assigned by the state authority, e.g. tax identification number (Polish: NIP), number of right to practice the profession, then, before the certificate is provided to the subscriber, it is necessary to present a document confirming the assignation of such identifier, if provided it is not publicly online available in the register maintained by public authorities.

3.2.1. Method to proof possession of private key

The certificate may be issued with a pair of keys generated by KIR or to a public key from a pair generated by the subscriber.

If the subscriber generates a pair of keys on their own it should meet the requirements specified in section 6.1.7. Then it is required to present the file with request for certificate issuance in order to issue the certificate. Such file contains a public key for which the certificate is to be generated, the subscriber's data, and electronic signature or electronic seal generated with the use of a private key which constitute one pair with the public key. The file with the request shall be delivered personally to KIR by the subscriber or shall be send by email, whereby the file with the request signed with qualified electronic signature of the subscriber is then verified with qualified certificate of the subscriber by KIR's Operator.

Provision of a request containing a public key and signed with a private key is to establish whether a private key making a single pair with a public key is under control of the subscriber.

3.2.2. Identification of natural persons

The identification of a natural person is carried out when the data of such person are to be included in the certificate. The identification is to confirm that the indicated person actually exists and is the person whose data are stated in the order or in the Agreement. If the certificate is to include data about another entity, apart from the data of a natural person, then it is also verified whether this is consistent with the will of this entity. This involves the verification of the statement of the person authorised to represent this entity.

If a natural person applies for issuance of a qualified certificate for websites authentication, checking the right to have a domain is carried out in accordance with the description in section 3.2.3 and, additionally, requires presentation of a document confirming a purchase of the domain, e.g. an invoice issued by an entity registering the domain. Furthermore, verification comprises the steps described in section 3.2.

3.2.3. Identification of entities other than a natural person

In case of the qualified certificate for electronic seal and the qualified certificate for websites authentication that are to contain a name of the entity, before a certificate is issued, it will be checked, on the basis of information obtained from legitimate and reliable sources that are publicly available, including available registers maintained by public authorities, whether such entity exists, if the data indicated by an ordering party is compliant with the data presented in the register used and if the persons acting on behalf of the ordering party are authorised to so act. The address of the organisation may also be verified during a visit of the Operator at the registered office of the ordering party.

In case of the qualified certificate for websites authentication verification checks if the ordering party has the right to use the domain name and if the domain remains under its control. Verification carried out by KIR covers:

1) checking in the publicly available WHOIS services or directly with entities registering domains, if the ordering party is registered as a domain owner or has the right to use the domain name during a period of submission of an order for the certificate;

2) confirming control over the requested Domain Name by placing indicated by KIR random data in file kirdv.txt under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation. The file with random data has to be accessible by KIR via HTTP or HTTPS. Random data in file is unique for every certificate request, does not appear in the request HTTP nor HHTPS and data is not older than 30 days;

3) checking, if verification data indicated by KIR has been put on a server or a TXT type record in DNS for the domain;

4) the alternative way of checking the control over the requested Domain Name is placing the random data given by KIR in DNS record TXT, CAA or CNAME type. Random data sent by KIR is unique for each validation and is not older than 30 days;

5) in case of Wildcard Certificates checking if in the “public suffix list” (PSL) register http://publicsuffix.org/ (PSL), the sign “*” is not put in the first place on the left-hand side of the suffix of gTLD domains delegated by ICANN. KIR may issue a Wildcard Certificate for gTLD domains, if the subscriber properly proves its right to manage the entire space of names under the gTLD domain;

6) checking if the DNS of the domain does not contain restriction as a CAA (Certification Authority - Authorization) record describing which entities can issue certificates for a given domain. This check is performed by the dedicated tool by querying a CAA record.

To minimise the risk of using wrong data, KIR shall use data presented in the WHOIS service in combination with the IANA data and the WHOIS data provided by entities approved by ICANN that register domains.

If the Subscriber Identifier of the qualified certificate for websites authentication containing the domain name is also to contain a name of the country, then prior to issuance of the certificate KIR shall verify if the indicated name of the country is linked with the subscriber. Verification is carried out according to one of the methods described below and it consists in checking:

1) if an IP address of the domain indicated in DNS is within a range of IP addresses assigned for a country for entering of which into the Subscriber Identifier the applicant applies;
2) if the name of the country included in information provided by an authority registering the domain the name of which is to be placed in the certificate is compliant with the name of a country for entering of which into the Subscriber Identifier the applicant applies;
3) By verifying the name of the country KIR shall examine if the ordering party does not use a proxy server to substitute an IP address from another country than in which it is actually located.

3.2.4. Subscriber's data not subject to verification

The following data:

1) position;
2) organizational unit;
3) any other data that is marked as non-mandatory in the order form and that pertain to the contracting party

is verified only on the basis of a representation of the principal.

3.2.5. Checking rights to receive the certificate

Prior to the issuance of the certificate Operator checks:

1) the identity of subscriber on the basis of the identity document presented by him / her or in case qualified certificates for electronic seal and qualified certificates for websites based on the qualified certificates for electronic signature used for signing the request file if it was delivered electronically to KIR;
2) in case of qualified certificates for electronic seal and qualified certificates for websites authentication the right of a given person to receive a certificate on the basis of its indication in an order of the ordering party as an eligible person.

In case of qualified certificates for electronic seal and qualified certificates for websites, if the request file was delivered to KIR electronically in the form described in section 3.2.1, the certificate generated by KIR can be send back to the subscriber on the email address indicated in the order.

3.3. Identification and authentication at certificate renewal when electronic signature data are carried out on a device or generated by a subscriber

The certificate renewal requires having a valid agreement and submitting order for certificate renewal. The Agreement validity and data included in the order are verified as described in point 3.2.

3.3.1. Renewal during the period of validity of the current certificate

The data that is to be included in the certificate is verified as described in point 3.2.2 and 3.2.3.

Having a private key is proven as described in point 3.2.1.

The renewal can be done at registration authority after previous identification and authentication of the subscriber with the same methods that have been applied at the time of the first certificate issuance. A renewal may also happen without simultaneous presence of the parties, and the certificate is provided online. If the commercial offer provides so, the process of identification and authentication may also be carried out in a different place after the purchase of the relevant service of arrival of an authorised KIR representative.

If certificate is renewed online, prior to the transfer of the certificate to subscriber or eligible person, KIR checks right to collect the certificate on the basis of an electronic signature or an electronic seal signed under a request to renew the certificate verified with the use of a valid certificate issued by KIR.

3.3.2. Renewal after the expiry of the current certificate

If the validity period of the current certificate has expired, it is necessary to personally contact KIR and to buy a new certificate. If the commercial offer or the Agreement provides so, the process of identification and authentication may also be carried out in a different place after the purchase of the relevant service of arrival of an authorised KIR representative.

3.4. Identification and authentication upon the issuance or the renewal of certificate for electronic signature and seal with signature and seal creation data managed by KIR on behalf of a subscriber

3.4.1. Proving possession of signature and seal creation data

Signature and seal creation data are produced and managed by KIR. Therefore, the procedure of proving the possession of signature creation data by a subscriber does not apply.

3.4.2. Identification of natural persons applying for a qualified electronic signature certificate

Certificates for electronic signature contain as minimum the name and surname of the subscriber and:

1) PESEL or

2) the number and series of the document confirming the identity.

KIR does not generate qualified certificates containing a pseudonym.

The subscribers' identity and certificate data can be confirmed on the basis of:

1) electronic identification means accepted by KIR within the meaning of Art. 3 point 2 of eIDAS Regulation, meeting the requirements referred to in Art. 24 sec. 1 lit. b eIDAS Regulation;
2) a valid qualified certificate for electronic signature issued by KIR containing a personal identification number or ID number and the name and surname:
    a. for which the signature creation data are not managed by KIR or
    b. issued with the signature creation data managed by KIR;
3) verification of identity at registration authorities.

In the case of persons with full legal capacity who are under 18 years of age, the submission of data for the certificate requires only the use of the procedure referred to in point 3 above.

Data verification in the manner referred to in point 1 above consists in electronic identification and transfer of the subscribers data to KIR as part of the release of data from the electronic identification means (Article 24 (1) (b) of eIDAS Regulation). The issued qualified certificate will only contain data released from the electronic identification means.

Data verification in the manner referred to in point 2 above consists in signing the certification request with a qualified electronic signature. The qualified certificate will contain only the data derived from the qualified certificate used to verify the electronic signature submitted under the certification request.

Verification of data in the manner referred to in point 2 lit. b) above is possible only if the relevant process is made available by KIR at the subscriber's account at KIR service.

Verification of data in the manner referred to in point 3 above, consists in the personal verification of the subscriber's identity and personal data at a registration authority.

In the case of identity verification on the basis of an electronic identification means or a qualified certificate, KIR has the right to perform additional verification confirming the subscriber's data.

3.4.3. Identification of entities other than a natural person

Certificates with signature creation data managed by KIR are issued only to natural persons.

Certificates with electronic seal data managed by the NIR are issued to a person authorized to represent a particular organization whose data are included in the certificate. The data for an electronic seal certificate for which the electronic seal filing data is managed by KIR shall include only:

1) the name of the Organization in accordance with the registration name;
2) the organization's identifier;
3) the address of the Organization.

Data for the certificate shall be verified on the basis of information obtained from legal, reliable, publicly available sources, including available registers maintained by public authorities, whether such an entity exists, whether the data indicated by the ordering party is consistent with the data presented in the register used, and whether the persons acting on behalf of the ordering party are authorized to do so.

The address of the organization may also be verified during the Operator's visit to the contracting authority's premises.

The identity of the person authorized to represent the organization can be confirmed on the basis of:

1) a qualified electronic signature certificate containing the PESEL or identity document number and name;
2) identity verification at the point of registration.

3.4.4. Subscriber's data not subject to verification

The certificate does not contain any data other than those indicated in point 3.4.2 or 3.4.3. All data included in the certificate are subject to verification in accordance with point 3.4.2 or 3.4.3.

3.4.5. Transfer of the certificate

Certificates with signature and seal creation data managed by KIR are generated automatically, immediately after verification of the subscriber's identity. The certificate is handed over by making it available together with the signature and seal creation data in the system supporting the management of data for electronic signature and electronic seal by the KIR.

3.4.6. Renewing a certificate with signature creation data managed by KIR within the validity period of the current certificate

A certificate for which signature creation data are managed by KIR:

1) is not subject to renewal in the certification mode of the same signature creation data;
2) is subject to renewal only in the manner and on the terms of issuing a new certificate.

3.4.7. Renewing a certificate with signature creation data managed by KIR after the expiry of the validity of the current certificate

A certificate for which signature creation data are managed by KIR:

1) is not subject to renewal in the certification mode of the same pair of keys;
2) is subject to renewal only in the manner and on the terms of issuing a new certificate.

3.4.8. Renewing a certificate with seal creation data managed by KIR within the validity period of the current certificate

The certificate for which the electronic seal data is managed by KIR is subject to renewal only in accordance with the procedure and terms of issuance of a new certificate.

3.4.9. Renewing a certificate with seal creation data managed by KIR after the expiry of the validity of the current certificate

The certificate for which the electronic seal data is managed by KIR is subject to renewal only in accordance with the procedure and terms of issuance of a new certificate.

3.5. Identification and authentication upon the certificate suspension or revocation

The revocation or suspension of the certificate is applied for by the subscriber, the principal or a third party if its data has been included in the certificate, or another person if this arises from the Agreement or other obligations of KIR. Suspension and revocation can be done only by KIR.

The certificate that has been revoked cannot be then recognised as valid.

Certificates for which signature or seal creation data are managed by KIR on behalf of the subscriber cannot by suspended.

The request for certificate revocation or suspension may be submitted:

1) personally in the KIR offices, during the office hours of KIR;
2) by phone at the KIR hotline: 0 801 500 207 during the hotline operating hours;
3) 24/7 at the KIR website: www.elektronicznypodpis.pl.

The request for certificate revocation or suspension should contain at least:

1) full name of the notifying person;
2) PESEL number of the notifying person or another personal identifier assigned by a competent authority;
3) data concerning the certificate (e.g. serial number, subscriber's identifier, validity period);
4) reason for changing the certificate status.

Specimen request for certificate revocation/ suspension is published at the KIR website www.elektronicznypodpis.pl.

The request for certificate revocation/ suspension submitted personally is accepted on the basis of positive verification of:

1) identity of the person requesting the revocation/ suspension on the basis of identity document presented by them, and their right to request certificate revocation/ suspension;
2) data included in the request for certificate revocation/ suspension.

The request for certificate revocation/ suspension submitted by phone or via the Internet is accepted on the basis of positive verification of:

1) full name of the notifying person;
2) PESEL number of the notifying person or another personal identifier assigned by a competent authority;
3) data about the certificate;
4) password for revoking the certificate of the notifying person.

In the case of a request for a certificate for which signature or seal creation data are managed by KIR and the certificate’s validity period is shorter than 24 hours, no password is required.

If any of the information is incorrect, the request for certificate revocation/ suspension is rejected.

3.6. Identification and certification in a time stamping service

Commencement of provision of the service of issuance of a time stamp by KIR shall require conclusion of an agreement with KIR.

After conclusion of the agreement the ordering party shall provide KIR with:

1) a list of the subscribers authorised to obtain electronic time stamp;
2) a list of certificates or data allowing identification of certificates that the subscribers shall use who apply for time stamps.

Data received from the ordering party in the registration process is used to verify subscribers making requests for issuance of time stamps.

After receiving the request, the correctness of the request is verified in terms of its compliance with the format of the request for issuance of an electronic time stamp as defined in section 9.4.2. In the event of non-compliance, the request for issuance of an electronic time stamp shall be rejected.

After checking the correctness of the format of the request, KIR shall check if the subscriber applying for the issuance of a time stamp is authorised to use the services or if the electronic signature or the electronic stamp on the request for the issuance of the time stamp is valid. Certificates indicated to KIR by the ordering party in the registration process shall be used for verification of the electronic signature or the electronic stamp. Each of the certificates is additionally checked if it has not been placed on a CRL list relevant for a given certificate.

The request for the issuance of the time stamp is also rejected in the event whereby the time limit for time stamps agreed with the ordering party has been exceeded.

If the verification of the request for the time stamp has ended unsuccessfully, an error message shall be sent to the subscriber.

4. REQUIREMENTS FOR THE PARTICIPANTS OF THE PKI INFRASTRUCTURE IN THE CERTIFICATE LIFE CYCLE

The conclusion of the agreement for the provision of trust services is the basis for submitting orders for certificates and issuing them by KIR.

The Agreement may be concluded with a natural person, a legal person or an organizational unit without legal personality. Based on the Agreement, the principal indicates subscribers for whom it orders the certificates.

4.1. Request for certificate

The request for certificate issuance is submitted to KIR in the form of an order. The request may be submitted using both a dedicated order form available at the KIR website and at the KIR office. A request for certificate, for which signature and seal creation data are managed by KIR on behalf of subscriber can be submitted only by KIR’s dedicated website or KIR’s system.

4.1.1. Who may submit the request?

Requests, that is orders, may be submitted at KIR by persons authorised to represent the principal or attorneys indicated in the Agreement or separate powers of attorney.

4.1.2. Request registration process

Orders are registered by KIR Operators or automatically if they have been submitted via the Internet. The registration of orders submitted as hard copies consists in entering the data from the order to the system of the certification authority, following its prior verification. The KIR Operators are responsible for entering data correctly and in a way consistent with the order.

4.2. Verifying of the order for certificate

After receiving the order for certificate issuance, KIR starts the verification of data included in the order, as defined in section 3.2.2 and 3.2.3 or 3.4.and verification of a file with a request for certificate issuance, if keys were generated by a subscriber. Then if the data has been positively verified, KIR proceeds to register or approve the order in the system and to generate the certificate.

4.2.1. Performance of identification and authentication function

After receiving the order with full set of documents necessary to verification of the order, Operator verifies the data included in the order as defined in section 3.2.2, 3.2.3 and 3.4.

In the case of issuing certificates for which the signature creation data are managed by KIR on behalf of subscriber, only the data provided as part of the electronic identification means referred to in point 3.4 or a valid qualified certificate containing the data referred to in point 3.4 shall be used to prepare the certificate.

In the case of issuance of certificates for which the data for the electronic seal is managed by the NIR on behalf of the subscriber, only the data provided in the order and confirmed by the Operator pursuant to Section 3.4.3 shall be used to prepare the certificate.

If the subscriber generates pair of keys himself, Operator checks, as defined in section 3.2.1, certification request delivered by subscriber and if a public key included in a request for certificate issuance meets requirements specified in section 6.1.7.

In case of certificates renewed online, after the performance of actions related to order reception and acceptance, the Operator carries out the process of order and data acceptance in the KIR systems.

4.2.2. Acceptance or rejection of the order

Orders that are filled in correctly with data authenticated in the way described in Chapter 3 are accepted for execution. While verifying the order, Operator performs the following actions:

1) assigns the order to the right agreement for the provision of trust services;
2) checks the authorisation to place orders for the person who has signed the order for certificate;
3) verifies the data entered to the customer support system maintained by KIR during the registration of order against the data available in the KIR databases of other databases available to them;

4) compares the data entered to the order against the data derived from the submitted documents.

Some of the above-mentioned actions may be performed automatically.

If the result is positive and all data included in the request is correctly verified, Operator starts the execution of order and generation of the certificate, or forwards it to the relevant organizational unit of KIR for execution.

If any data in the order is incorrect, or not valid, the order is rejected and the principal or subscriber is informed about it. Order shall be rejected if:

1) The principal does not have valid agreement with KIR in the moment of checking the order, agreement was expired,
2) The person who signed the order is not authorised to represent the given company,
3) PESEL number is incorrect, the identity document is not valid (is registered in Restricted Document Database as restricted, in case of certificates for website validation the domain is not under control of the principal or subscriber),
4) organization identifier or the Principal name indicated in the order does not match with the information in the agreement or registers, which are used to check the identifier and name.
5) Qualified certificate used for identification of the subscriber does not contain data unambiguously identifying the subscriber;
6) A public key included in the request for certificate issuance does not meet requirements specified in section 6.1.7.
7) data released as part of the electronic identification means has not been confirmed by the subscriber or the order does not contain the required data.

4.2.3. Certificate generation

If the order together with the data contained therein was verified correctly then Operator proceeds to generate the certificate. In the case of certificates for which signature creation data are managed by KIR on behalf of subscriber, after verification of the subscriber's identity and obtaining data for the certificate, KIR automatically generates signature and verification creation data and a certificate.

KIR shall place, in a relevant certificate extension qcStatement – qcSSCD, information about storage of a key in the qualified device if the certificate is issued:

1. for a pair of keys generated by KIR on qualified electronic signature creation device or qualified electronic seal creation device, that is referred to in section 6.2 or
2. when a pair of keys, which meets the requirements specified in section 6.1.7, is generated in the presence of Operator in qualified electronic signature creation device or qualified electronic seal creation device that is under control of an ordering party or a subscriber and presented on list of certified qualified electronic signature creation devices or list of certified qualified electronic seal creation devices as referred to article 31 and article 30 eIDAS Regulation accordingly.

If a pair of keys is generated by KIR, the transfer of private key to the subscriber is confirmed with a document confirming the issuance of the certificate and signed by the subscriber.

If a pair of keys is generates by a subscriber, KIR does not check if the keys are stored in a qualified electronic creation device, and do not place qcStatement extension – qcSSCD in the certificate. In case the order concerns a certificate along with a pair of keys generated by KIR, then on the carrier selected in the order, dedicated to the subscriber, KIR generates a key pair and a certificate.

If the pair of keys is generated by KIR on the cryptographic card then Operator personalize the card by printing on the card the subscriber's name and securing the card by generating the PIN and PUK codes and print them in secure envelope.

If the subscriber generates a pair of keys himself, Operator after checking in accordance with paragraph. 3.2.1 certification request generates a certificate

KIR, generating certificate certifies subscriber's public key, along with subscriber data.

4.2.4. Waiting period for request processing

All requests are processed without undue delays in the order in which they have been submitted to KIR or according to certificate collection dates entered in the order.

All requests should not be processed longer than 5 business days, unless the Agreement provides for other waiting period for the processing of request or the subscriber had indicated the collection date in the order that falls after the 5-day processing period.

All requests regarding certificates for which signature creation data are managed by KIR are process online.

4.3. Issuance of the certificate

The issuance of the certificate follows the processing of the order and certificate generation.

If the verification of subscriber's identity was carried out by the Operator based on the identification document presented in the face to face registration process, then the certificate is only provided by the Operator. If the identity verification was carried out based on a qualified certificate used for signing the file with the request, then the certificate is sent by e-mail on the address indicated in the order.

The process of issuing another certificate after revocation of the previous one or issuing another certificate when the validity period of the certificate has elapsed is analogous to the process of issuing the first certificate.

Certificates for which signature and seal creation data are managed by KIR are made available to subscribers as soon as they are generated.

4.3.1. Actions performed during the certificate issuance

Certificates are issued directly to the subscriber or via the eligible person in case of the qualified certificates for electronic seal or the qualified certificates for certification of websites only by Operators. The provisions of point 1.3.3 apply accordingly. During the process of personal issuance of the certificate Operator performs the following actions:

1) checks the completeness of executed order against the request submitted by the principal;

2) compares the data included in the certificate confirmation against the data in the request;

3) verifies the identity and rights of the subscriber or entitled person based on the identity document shown by him;

4) if the data is found compliant and the identity is successfully verified, Operator issues certificate with the carrier depending of order. If pair of keys was generated by KIR on cryptographic card, Operator issues also secure envelop with PIN and PUK codes.

In case of certificates is renewed online, as define in section 3.3.1, KIR check also the subscriber’s or the eligible person right to collect the certificate. The check basis on an electronic signature or an electronic seal signed under a request to renew the certificate verified with the use of a valid certificate issued by KIR. After the performance of actions related to order reception and acceptance, Operator carries out the process of order and data acceptance in the KIR systems.

4.3.2. Informing the subscriber about the issuance of the certificate

The certificate collection date is indicated in the request. The certificate is ready for collection at the date indicated in the order. If the certificate is not collected at the date indicated in the order, the subscriber or the eligible person is informed, via telephone or electronic mail, about the necessity to collect the certificate.

The provision does not apply to the certificates for which the signature creation data are managed by KIR, which are made available to subscribers online immediately after generation.

4.4. Acceptance of the certificate

4.4.1. Confirmation of certificate acceptance

In case of certificates issuance by the Operators, the certificate is accepted by the subscriber by acknowledging the confirmation of certificate delivery which includes data from the collected certificate. The document confirming certificate delivery with the signature of the subscriber and the operator issuing the certificate is kept by KIR. The second counterpart is given to the subscriber.

In case of certificates renewed in the online mode, or certificates with signature or seal creation data managed by KIR on behalf of subscriber, the certificate is accepted by the subscriber by collecting it from the KIR system.

4.4.2. Publication of the certificate by the certification authority

Certificates are not published outside the internal network of KIR.

4.4.3. Notification of other entities about certificate issuance

KIR may inform other entities about the issuance of the certificate, provided that the certificate pertains to them or contains their data.

4.5. Time stamping service

A process of issuing electronic time stamps is carried out as follows:

1) the ordering party and Subscribers indicated by it are registered in KIR system;

2) a subscriber sends to KIR a request for issuance of an electronic time stamp;

3) the request is verified on the basis of the data provided in the registration process;

4) a time stamp is generated or error information in case of negative verification of the request by KIR;

5) the prepared electronic time stamp or the error message is sent back to the subscriber the same way in which the request for the issuance of the electronic time stamp was sent by the subscriber;

6) the subscriber or the ordering party shall check the correctness of the received electronic time stamp.

4.5.1. Request for issuance of an electronic time stamp

The time stamp is issued by KIR in response to a correct request for the issuance of an electronic time stamp. A description of the format of the request for the issuance of the electronic time stamp accepted by KIR is defined in section 7.4.1. The request for the issuance of the time stamp should contain an abbreviation of the document to which the time stamp is to be issued and should be signed with an electronic signature or with an electronic seal verified with the use of the certificate issued by KIR or the qualified electronic signature or the qualified electronic seal.

4.5.2. Issuance of the electronic time stamp

By issuing the electronic time stamp KIR shall attach the service execution time to the data included in the request for the issuance of the time stamp. Data so prepared shall be signed with the electronic seal and forward to the subscriber who has made the request.

4.6. Pair of keys and certificate application – obligations of the participants in the PKI infrastructure

4.6.1. Obligations of the subscriber

The subscriber undertakes to:

1) use the certificate in accordance with its intended purpose stated in a given certificate;

2) use the certificate only during its validity period stated therein;

3) protect its private key and in case of creation data for electronic signature and seal managed by KIR on behalf of subscriber to protect the data necessary to authorize access to them;

4) physical and IT protection of the device on which the mobile application is installed, in case the signature and seal creation data are managed by KIR on behalf of the subscribers, in particular by installing and updating software securing the device against the takeover of control over it by a third party

5) immediately notify KIR about the request for certificate revocation in cases provided for in the Agreement or the Policy in particular in the event of loss of the device or data securing access to the signature and seal creation data which are managed by KIR on behalf of the subscriber.

The Agreement may specify a more detailed scope of subscriber's responsibility. The subscriber may also be informed about its specific scope in the information sent in writing or by electronic means.

4.6.2. Obligations of the principal in the range of certificates

The principal undertakes to:

1) provide KIR with orders for the subscribers authorised to receive certificates in compliance with regulations governing personal data protection;
2) provide KIR with only true data, including personal data of the subscribers;
3) update data of persons authorised to receive and revoke the certificates;
4) acquaint the subscribers with the provisions of the CP;
5) comply with the rules set forth in the CP.

4.6.3. Obligations of the principal in the range of time stamps

The ordering party undertakes to indicate to KIR subscribers authorised to use the service of time stamp issuance in a manner that does not violate the interests of such persons.

Detailed obligations of the ordering party may be defined in an agreement.

After receiving the time stamp issued by KIR the ordering party or the subscriber shall be obliged to check, if:

1) the electronic seal generated by KIR is correct;
2) there are limitations in the use of the time stamps specified herein.

The ordering party and the subscriber shall be especially obliged:

- not to modify the time stamp;
- to use the time stamp in accordance with the provisions of the Policy and for purposes compliant with law and the intended purpose;

  to perform the obligations imposed on it under the Agreement, this Policy, or another document binding upon it.

4.6.4. Obligations of the relying party

A relying party is understood as a natural person, a legal person or an organizational unit without legal personality that undertakes actions or makes any decision relying on data which is signed electronically or sealed with electronic seal with the use of a public key contained in the certificate issued by KIR.

Relying parties are obliged to:

1) use the certificates in compliance with their intended purpose;
2) verify the electronic signature or electronic seal at the time of performing verification or at some other reliable time;
3) verify the electronic signature or electronic seal with the use of the list of suspended and revoked certificates and the right certification path;
4) inform KIR about any cases of a certificate being used by unauthorised persons or any suspicions of a certificate having been issued to the wrong entity.

4.7. Renewal of the certificate for an old pair of keys

4.7.1. Conditions for certificate renewal

A certificate may be renewed online with the use of the following website: elektronicznypodpis.pl by marking a relevant option in the renewal process.

The certificate for signature or seal creation data are managed by KIR, is subject to renewal only in the mode and on the terms of issuing a new certificate.

4.7.2. Who may request certificate renewal?

Certificate renewal may be requested by the principal or a person authorised by it.

4.7.3. Processing of the request for renewal

The request for renewal is processed in the same mode as the request for a new certificate.

4.7.4. Notification about the generation of renewed certificate

If the online mode for certificate renewal is selected, the information about certificate generation is provided to the subscriber by electronic means.

4.7.5. Issuance of renewed certificate

A certificate renewed in the online mode is made available to the subscriber via a dedicated website.

4.7.6. Publication of the certificate

Certificates are not published outside the internal network of KIR.

4.7.7. Notification of other entities about certificate issuance

A notification about certificate issuance to other entities shall be done pursuant to the terms applicable to new certificates. See: section 4.4.3.

4.8. Renewal of the certificate for a new pair of keys

4.8.1. Conditions for certificate renewal

A certificate may be renewed for a new pair of keys on a new card with the use of the following website: elektronicznypodpis.pl by marking relevant option in the renewal process. The renewal takes place at the KIR office, an office of the entity cooperating with KIR or at another agreed place.

The certificate for signature and seal creation data are managed by KIR, is subject to renewal only in the mode and on the terms of issuing a new certificate.

4.8.2. Who may request certificate renewal?

Certificate renewal for a new pair of keys may be requested by the principal or a person authorised by it.

4.8.3. Processing of the request for renewal

The request for renewal is processed in the same mode as the request for a new certificate.

4.8.4. Notification about the generation of renewed certificate

The notification about the generation of renewed certificate for a new pair of keys is the same as in the case of generation of the first certificate. See point 4.3.

4.8.5. Issuance of renewed certificate

The issuance of renewed certificate for a new pair of keys takes place in the same way as in the case of issuance of the first certificate. See point 4.3.

4.8.6. Publication of the certificate

Certificates are not published outside the internal network of KIR.

4.8.7. Notification of other entities about certificate issuance

Other entities are notified about certificate issuance in the same way as for the new certificates. See point 4.4.3.

4.9. Change of data included in the certificate

4.9.1. Conditions for introducing changes

The data included in the certificates that have been already issued by KIR cannot be changed. The principal may only request for the issuance of a new certificate for the new data. The certificate for the changed data is issued in the same way as the first certificate.

4.9.2. Who may request the change of data in the certificate?

No changes are allowed in the certificate that has already been issued. The necessity of changing data means the generation of a new certificate.

4.9.3. Processing of request for the change of data in the certificate

The request for the change of data in the certificate is processed in the same way as in case of the issuance of a new certificate. See point 4.2.

4.9.4. Notification about the generation of certificate with changed data

The notification about the generation of certificate with changed data may be done by electronic means, by phone or personally during the visit to the KIR office.

4.9.5. Issuance of the certificate

The certificate with changed data is issued in the same way as the first certificate. See point 4.3.

4.9.6. Publication of the certificate

Certificates are not published outside the internal network of KIR.

4.9.7. Notification about certificate issuance

Other entities are notified about certificate issuance in the same way as for the new certificates. See point 4.4.3.

4.10. Suspension and revocation of certificate

Every certificate whose validity has not expired may be revoked. Certificate suspension is a special case of revocation. A certificate that has been suspended may then be revoked or unsuspended. The suspension period should be used to clarify any doubts concerning the premises for revoking or unsuspending the certificate. The certificates for which signature and seal creation data are managed by KIR on behalf subscriber cannot be suspended.

If there occur circumstances indicative of the necessity to revoke or suspend the certificate, KIR revokes/ suspends it. The revocation/ suspension of the certificate takes place at the time of entering the certificate number to the list of revoked and suspended certificates. The information about the revocation/ suspension of the certificate is placed in the list of revoked and suspended certificates. KIR notifies the subscriber, a person whose data are included in the certificate and possibly another person about the revocation/ suspension of the certificate.

Following certificate suspension, the status of the certificate may be changed:

1) upon the request of the subscriber;
2) upon the request of the person authorised to request the revocation or suspension of the certificate who has submitted such request;
3) as a result of clarifying the suspicions referred to in point 4.10.11.

The certificate may be suspended till the end of its validity period.

The certificate may be unsuspended solely upon the subscriber's request submitted personally at KIR. The specimen of the request for status change is available at the KIR website. The status is changed into invalid in the manner set forth in point 4.10.2 and 4.10.3.

The certificate may be unsuspended only when the circumstances of mandatory certificate revocation are not confirmed.

If certificate revocation occurs after its prior suspension, then the date of certificate revocation is the same as the date of certificate suspension.

4.10.1. Conditions for certificate revocation

Certificate revocation may occur under the following circumstances:

1) it has been requested by the subscriber, principal or a third person indicated in the certificate or another person authorised to submit such request;
2) the certificate has been issued on the basis of untrue data;
3) private key of the subscriber linked with the public key in the certificate has been compromised;
4) the subscriber has lost control over the device or data used to authorize access to signature and seal creation data in particular in case the signature or seal creation data are managed by KIR on behalf of the subscriber;
5) KIR receives evidence that the certificate has been used contrary to its purpose;
6) the subscriber or the principal have not paid their liabilities arising from the issuance of the certificate;

7) data included in the certificate has ceased to be valid or is untrue;

8) KIR finds that the information included in the certificate has changed materially;

9) KIR finds that the information appearing in the certificate is imprecise or misleading;

10) KIR ceases to provide services concerning certificates, and no entity takes over the performance of services that involve the provision of information about the certificate status;

11) private key of the operational certification authority or the main certification authority has been compromised, or KIR obtains information that the said keys could have been compromised;

12) it is found that the obligations set forth in the CP or the Agreement have been violated, or there exist other circumstances that pose a threat to the security of electronic signature or electronic seal;

13) technical parameters of private key linked to the public key included in the certificate or the format of the certificate pose a threat to software or relying parties;

14) the subscriber has lost its full legal capacity.

15) KIR shall receive information that is evidence of the fact that the domain name entered in the certificate has ceased to be the property of the ordering party (e.g. an entity registering domains has been deprived of the rights to register domains or otherwise an agreement for domain registration executed between the domain owner and the registering entity has expired, or the entity registering domains has not extended registration of a given domain).

The authorisation to request certificate revocation may be derived from the Agreement.

The Agreement may provide for other instances of certificate revocation than those referred to above.

KIR may also revoke all certificates that have been issued by a given certification authority if it is necessary to end the certification activities or there occurs a threat to the security of the entire public key infrastructure supported by KIR.

The revocation of the certificate may arise from the following circumstances:

1) private key of the certification authority linked with the public key in the certificate has been compromised;

2) data included in the certificate has ceased to be valid or is misleading;

3) KIR ceases to provide services concerning certificates, and no entity takes over the performance of services that involve the provision of information about the certificate status;

4) it is found that the obligations set forth in the CP or the Agreement have been violated, or there exist other circumstances that pose a threat to the security of electronic signature;

5) technical parameters of private key linked to the public key included in the certificate or the format of the certificate pose a threat to software or relying parties.

4.10.2. Who may request for certificate revocation?

The revocation of the certificate may be requested by:

1) subscriber;

2) principal;

3) person authorised by the principal;

4) another person authorised to submit such request, including the person whose data is included in the certificate;

5) KIR;

6) supervision authority.

4.10.3. Processing of the request for certificate revocation

Upon receiving a request for certificate revocation, an authorised employee of KIR checks the data from the certificate and verifies it against the data in the request. They also check the authorisation of the person submitting the request.

If the verification is successful, the information about certificate revocation is put on the CRL, and the subscriber or another person receives confirmation of certificate revocation collecting it personally or by mail.

If the certificate contains data of another entity, such entity also receives confirmation of certificate revocation.

4.10.4. Permitted delays in certificate revocation

KIR exercises its best efforts for the certificate to be revoked without undue delay after the request for its revocation is submitted. The maximum permitted delay between the submission of the request and the publication of the information about certificate revocation status cannot exceed 24 hours.

4.10.5. Maximum permitted time for the processing of the request for revocation

The request for certificate revocation is processed without undue delay, and is a priority task for the operators. The maximum permitted time for the processing of the request is 24 hours as from the moment of submitting complete request.

4.10.6. Obligation to check for revocations by the relying party

A party relying on data included in the public key certificate issued by KIR is obliged to check, from time to time, whether the certificate has not been put on the list of suspended and revoked certificates before it is used for the verification of electronic signature.

4.10.7. Frequency of publishing CRLs

Current CRLs for certificates issued by the COPE SZAFIR Qualified certification authority are published always after the suspension or revocation of the certificate, but not less frequently than every 24 hours.

Current CRLs are available at the KIR website in the 24x7x365 mode.

KIR checks the availability of CRLs at least once a day.

4.10.8. Maximum delay in publishing CRLs

Current CRLs are published without undue delay, immediately after they have been created. KIR stipulates that any delay in publishing CRLs may not be longer than 60 minutes.

4.10.9. Availability of other methods of certificate status verification

KIR offers the possibility of verifying the status of the certificate issued by KIR in real time on the basis of the Online Certificate Status Protocol (OCSP). This service is available in the 24x7x365 mode and uses the CRLs issued by KIR. The OCSP service operates in compliance with RFC 2560 and RFC 5019 on the request – response basis. In order to obtain information on the status of the certificate issued by KIR, one should send a request containing data that allows for the identification of the certificate, that is certificate serial number and certificate issuer ID. The request should comply with the format set forth in RFC 2560. In response, the information about certificate status is provided:

1) good – means that the certificate has been issued by KIR and is not included in the CRL issued by KIR;
2) revoke – means that a given certificate has been issued by KIR and is included in the CRL, that is it has been revoked or is suspended;
3) unknown – means that the certificate has not been issued by KIR and the status of such certificate is not known.

4.10.10. Special obligations when the key has been compromised

In the event of the key of the COPE SZAFIR Qualified certification authority or Szafir TSA time stamping authority being compromised, KIR is obliged to inform the supervision authority, the subscribers, the contracting authorities and the relying parties about this fact as soon as possible by posting it on the KIR website.

4.10.11. Conditions for certificate suspension

The certificate may be suspended till the end of its validity period.

Following certificate suspension, the status of the certificate may be changed. A certificate that has been suspended may then be revoked or unsuspended.

If certificate revocation occurs after its prior suspension, then the date of certificate revocation is the same as the date of certificate suspension.

When certificate suspension is lifted, the information about such certificate is removed from the list of suspended and revoked certificates.

Information about revoked certificates whose validity period, as assigned by KIR, has passed is not removed from the list of suspended and revoked certificates.

KIR may suspend the certificate if it is suspected that the certificate contains incorrect data or the private key for this certificate has been compromised, and in other cases when it is reasonably suspected that there are premises for certificate revocation.

4.10.12. Who may request certificate suspension?

Certificate suspension may be requested by:

1) principal;

2) person authorised by the principal;

3) subscriber;

4) another person authorised to submit such request, including the person whose data is included in the certificate;

5) KIR;

6) supervision authority.

4.10.13. Processing of the request for certificate suspension

The request for certificate suspension is processed in the same way as the request for revocation. See point 4.9.3.

4.10.14. Permitted delays in certificate suspension

A permitted period between submission of the request and publication of the information on the status of certificate suspension may be 24 hours.

4.11. Verification of the certificate status

The status of certificates issued by KIR is verified on the basis of published CRLs.

The status of the certificate issued by KIR may also be verified with the use of the OCSP service if such information is included in the issued certificate. If the OCSP service address is included in the certificate, it means that the OCSP service is available for this certificate.

KIR shall store and make available data necessary for the verification of a certificate's status in the form of CRL lists for a period of 20 years starting from the beginning of the certificate's validity. During that period the archived CRL lists necessary for the verification of a certificate's status shall be made available free of charge to all those interested within 5 business days starting from the day of sending a notification to KIR. Such notification should include an indication of the date and time for which the verification of the certificate's validity should be performed.

4.12. Waiver of trust services

Trust services are provided under the Agreement. Termination of the agreement means that it is not possible to place further orders based on it. Termination of the agreement does not result in the revocation or suspension of certificates issued under the Agreement.

4.13. Recovery and storage of private keys

KIR does not provide the services of depositing and storing private keys of the subscribers.

4.14. Publication of information related to the service of an electronic time stamp

Information concerning the services of issuing a time stamp, time stamping by KIR, including this Policy, shall be made available to all those interested at www.elektronicznypodpis.pl or in the registered office of KIR.

Certificates issued for KIR necessary for the verification of time stamps shall be made available free of charge to all those interested at www.elektronicznypodpis.pl.

5. PROCEDURES CONCERNING PHYSICAL, OPERATIONAL AND ORGANIZATIONAL SECURITY

5.1. Physical security measures

The premises where the data related to issuing, suspending or revoking certificates and to issuing time stamps is processed, and where certificates are generated, suspended and revoked, and where signature and seal creation data are managed by KIR on behalf of subscriber are subject to physical protection in line with the requirements for the qualified trust service providers and the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 86/160;95/46/EC hereinafter referred to as “RODO”. The employed protection measures protect against:

1) access to premises by unauthorised persons;
2) consequences of natural disasters and fortuitous events;
3) fires;
4) infrastructure failure;
5) flooding, theft, burglary and assault.

The employed physical protection measures for the implemented on the basis of the Standard of security for persons and property in the premises of KIR, include:

1) access control system for the premises;
2) fire protection system;
3) burglary and robbery alarm system,
4) video monitoring system.

5.1.1. Location and buildings

The certification authorities are situated in two independent data centres for which security plans have been prepared describing:

5) general information on the location the premises;
6) general information on the physical security of the premises;
7) division of the premises into zones;
8) the measures taken to protect individual zones, including zones where ICT systems used to provide trust services are operated;

Generating, suspending, revoking and issuing certificates is also performed at local offices of KIR.

5.1.2. Physical access

The rules of access control are provided by the procedure for the management of access by persons and vehicles to KIR facilities.

Pursuant to an agreement, physical protection of KIR is entrusted to a licensed agency having HR and equipment resources that allow for full performance of tasks arising from the specific nature of the facility and its size (the agency has licensed physical protection guards). The superiors at all protection shifts at the facility have qualifications of physical protection.

The KIR facilities are logically divided into zones with diversified access levels and proper technical and organizational protection measures. The buildings have the following zones creating a security cascade:

1) public zone;

2) protected zone;

3) specially protected zone.

5.1.3. Power supply and air-conditioning

The KIR buildings are powered with two independent power supply lines. In the event of power outage in the two supply sources, power generating units are switched on. The ICT devices used for processing are powered from the so-called guaranteed power supply source which is provided with UPSs that ensure stable power supply parameters. In the buildings there are UPSs installed which operate in parallel circuit ensuring redundancy, which provides for the continuity of power supply even when one of the UPSs is down.

There are two types of air-conditioning systems installed in the buildings:

1) general system;

2) precise system which maintains constant temperature and humidity in the server rooms.

5.1.4. Flood hazard

Flood detectors are installed in the server room, and in the rooms housing the power supply node, boiler room, ventilation control rooms, heat exchangers and in lift shafts. The detectors constitute a part of signalling and alarm system. Security staff and the building manager are notified about flood alerts.

5.1.5. Fire protection

The building is fitted with fire protection systems that provide for early fire detection (SAP), limiting fire spreading (fire partitions), protection of the escape route against smoke, permanent fire-extinguishing system in the premises that are critical for the operation of KIR.

The building has the following security solutions in place:

1) passive protection, i.e. the building is fitted with structural fire protection barriers;

2) active protection, i.e.:

   a) signalling and alarm system fitted with detectors that allow for early detection of fire and buttons that enable transferring the alarm signal from every floor of the building to the fire signalling control room,

b) early smoke detection system,

c) permanent fire-extinguishing equipment (FM 200 gas) that is used for fighting fires in their first phase,

d) escape route lighting – in the building there are escape route lights installed, fitted with batteries that support the lights for at least two hours.

5.1.6. Information carriers

Information carriers which contain copies of current data are stored in strongboxes that are located in protected premises used for operations. Carriers with archive data are stored in fire-proof strongboxes in the premises with the highest degree of security in the primary and backup locations. Strongboxes can be accessed by employees who perform the function of security inspector.

5.1.7. Destruction of redundant carriers and information

Magnetic and optical carriers are destroyed by a commission. Data is deleted from magnetic carriers in a way that prevents its being read, and if it is impossible to delete the data, the carriers are physically destroyed in a way that makes access to data saved on them impossible.

Optical carriers are physically destroyed to a degree that makes accessing data saved on them impossible.

The carriers are destroyed in a way that ensures the minimum of 2nd security class in accordance with the DIN 32 757-1 standard.

The act of destroying the carriers is recorded with a relevant report. The destruction report contains:

1) destruction completion date;

2) description of the object of destruction;

3) description of the time span for destruction of the archive data;

4) signatures of persons performing and attending the destruction process.

The report is kept by the ICT security inspector for the SZAFIR system for a period not shorter than 3 years. A copy of the report is provided to the Information Security Administrator who keeps it for a period not shorter than 3 years.

5.1.8. Backup copies and backup location

In the event of failure of the primary location that makes the provision of trust services impossible, the system operations are taken over by the backup system in the backup location. In the event of failure, the backup system takes over the operations related to revocation and suspension of certificates and publication of lists of suspended and revoked certificates on an ongoing basis.

5.2. Organizational security measures

The system used for the provision of trust services is operated and managed by KIR employees performing the following rules:

1) security inspector who supervises the implementation and application of all procedures for safe use of IT systems used for the purposes of providing trust services;

2) inspector for registration (Operator) who receives orders, requests for suspension/ revocation/ unsuspension of certificates and starting time stamp service, and who issue certificates;

3) system administrators whose responsibilities include the installation, configuration and management of systems and ICT networks used for the purposes of provision of trust services, hereinafter referred to as “administrators”;

4) information security administrator whose responsibilities include supervision over the compliance with requirements set forth in the RODO;

5) audit inspector who analyses the records in the registers of events that happen in the IT systems used while providing trust services.

5.3. Staff supervision

The staff that are involved in the provision of trust services have the appropriate qualifications required of qualified trust service providers, in particular they have the knowledge in the field of public key infrastructure and personal data processing.

5.3.1. Qualifications, experience, authorisations

KIR employees who exercise supervision over the system used for the provision of trust services have multi-year experience and knowledge of:

1) cryptography, electronic signatures and public key infrastructure;

2) mechanisms of ICT network and system protection;

3) personal data protection;

4) automatic data processing in networks and ICT systems;

5) equipment and software used for electronic data processing;

6) forgeries of holograph signatures and documents establishing identity;

7) handling of applications and secured cryptographic devices used for the purposes of the provision of trust services.

5.3.2. Staff screening

Before assigning an employee with any of the roles described in point 5.2, KIR performs their screening. The screening is performed with regard to:

1) employment separation certificate from the previous workplace (this applies to new employees);

2) diplomas and certificates confirming the employee's educational background;

3) professional qualifications and experience;

4) clean criminal record certificate of the employee.

5.3.3. Training

Operators undergo training in PKI, operation of the certification authority system, identity verification on the basis of documents confirming identity, personal data protection and information protection. Training is conducted prior to granting authorisation to act as an operator and after introducing substantial changes in the system.

Technical staff are regularly trained in handling IT infrastructure by manufacturers or providers of technical solutions.

5.3.4. Training repetition

Training is repeated as needed and prior to the implementation of significant changes in the provision of services.

5.3.5. Frequency and sequence of rotation of the positions

The CP does not provide for the frequency and sequence of rotation of the positions.

5.3.6. Sanctions for unauthorised actions

If it is detected or suspected that an employee has performed unauthorised actions, the security inspector may decide to block such employee's access to the system. Further explanatory actions are carried out on the basis of internal regulations of KIR and provisions of the law.

5.3.7. Contracted employees

KIR does not envisage the performance of any actions related to the provision of trust services by persons not employed at KIR, unless they are provided as part of external registration points.

5.3.8. Documentation for the staff

The operators and administrators have access to operational procedures, user documentation of applications which are used at the certification authorities and which are necessary to perform the actions of an operator or an administrator.

5.4. Procedures for registering events and audit

KIR keeps a register of all events that are related to the provision of trust services. The events are registered to ensure security and exercise supervision over the correct operation of the system. This also allows for the accountability for actions of employees who perform actions related to the provision of trust services. The registers of events are kept in electronic form and as hard copies. All registers of events are properly secured and made available for the purposes of auditing. The person responsible for keeping the register of events is the security inspector.

5.4.1. Types of registered events

Registration is conducted for:

1) events directly related to the provision of trust services, and particularly: generation of CA keys, generation of TSA keys, acceptance of request for the issuance of certificate, generation of keys and certificates for subscribers, suspension and revocation of certificates, generation of CRLs, acceptance of request for the issuance of time stamp, electronic signature generation and authorization the access to signature and seal creation data when they are managed by KIR on behalf of subscriber;

2) actions related to customer and subscriber service: acceptance and execution of agreements, orders, issuance of certificates, delivery of certificates, invoicing, etc.;

3) system events (logs) from the servers and work stations that are part of the COPE Szafir Qualified and Szafir TSA;

4) events related to system technical support: errors and alarms, register of changes introduced in the system, user support.

The registers of events are kept in electronic form. The records contain even ID, date and time of occurrence, type of event and detailed description.

5.4.2. Frequency of inspection of events (logs)

System logs are subject to regular daily inspection. The key elements of the system are controlled automatically in real time. An inspection report is saved in the system log book. Logs are reviewed once a day. All detected irregularities must be clarified, and a relevant report is saved in the system log book.

Access to the registers of events is granted only to the security inspector, audit inspector and system administrator.

5.4.3. Period of storing records for registered events

The registers of events are kept on disks of servers and work stations as files, databases, records of system logs. The registers of events related directly to the provision of trust services are available throughout the entire period of operation of the CA.

5.4.4. Protection of records of registered events

The registers of events are kept on disk arrays. The arrays are configured in a way that prevents loss of data due to disk failure, and are monitored on an ongoing basis. Access to the registers is granted to security inspectors and administrators. Every record in the database of key certification system is an electronic signature, which ensures the integrity of the record.

5.4.5. Procedures for making backup copies of registered events

The registers of the certification authority system are copied in real time to the backup location with the use of the disk array mechanisms. Once a month, all registers are electronically signed by the security inspector, saved on optical carriers and put into strongboxes. Two copies of registers are created, one staying in the primary location and the other placed in the backup location. Access to strongboxes is granted to persons acting as security inspector.

5.4.6. System of collecting data for the audit (internal vs. external)

Programme modules of the key certification system and servers automatically create records in the registers of events. Other events are registered manually in relevant databases. For the purposes of internal audit data is made available online or from archive records kept in the strongboxes.

5.4.7. Notification of entities responsible for the occurring event

The elements of the certification system and supporting systems are subject to constant supervision by monitoring systems and technical staff. The information about detected threat or security violation is forwarded directly to the administrator and security inspector. Depending on the level and importance of threat, persons responsible for the operation of components to which such event relates are notified. Notification can take place electronically or by telephone.

In the event of security violation or loss of integrity that has a significant influence on the provided trust service or personal data processed during such service performance, KIR notifies the supervision authority and, if applicable, other competent entities about this fact not later than within 24 hours from the event occurrence.

5.4.8. Assessment of susceptibility to threats

KIR analyses susceptibility to threats in relation to procedures and systemic solutions on an ongoing basis. An internal system audit is performed periodically. To minimize susceptibility to threats, business continuity procedures are updated and tested. The person responsible for susceptibility analysis is the security inspector.

5.5. Data archiving

KIR keeps and archives documents and data in electronic form that are directly related to the provided trust services for a period of 20 years from the time of issuing the certificate. Storing and archiving take place in accordance with the requirements specified in the RODO. Documents and data in electronic form (with the exclusion of archive CRLs and certificates) are not made available outside. Signature creation data shall not be archived.

5.5.1. Types of archived data

Archiving covers:

1) orders;
2) agreements for the provision of trust services;
3) confirmations of certificate issuance, including confirmation of assignation of data used for the verification of electronic signature to the subscriber;
4) certificates;
5) CRLs;
6) requests for cancellation/suspension/resumption of the certificate;
7) requests of time stamp issuance;
8) time stamp issued by KIR;
9) certificates issued for KIR for the purpose of the provision of trust services;
10) Certification Policy.

5.5.2. Archiving period

Paper and electronic documents referred to in point 5.5.1 are kept for a period of 20 years.

5.5.3. Archives protection

Archive data stored electronically are kept in fireproof strongboxes. The strongboxes are put in the primary and backup locations in the top security zone. Access to strongboxes is granted to persons acting as security inspector.

5.5.4. Procedures for creating backup copies

Backup copies are created to protect data and to recover the system after failure. Copies of key certification system data are created in real time with the use of synchronous replication of disk resources that are stored in the disk arrays. Additionally, a full backup of databases is created once a day. In each location there are carriers with backup copies of system and application software.

Detailed procedures for creating backup copies are governed by the internal procedures of KIR.

5.5.5. Required time-stamping of archived data

Time-stamping of archived data is not in place.

5.5.6. (Internal vs. external) data archiving system

KIR outsources the archiving of data in paper form related to the provision of trust services. The archiving takes place in a company with considerable experience in this area that meets relevant criteria with regard to personal data. The company has the quality and information security management systems in place in accordance with the requirements of the PN-EN ISO 9001:2009 and PN ISO/IEC 27001:2014 standards in terms of customer service in the process of storing, scanning and destroying documentation.

5.5.7. Procedures for archived data verification and access

Access to the archives is granted only to authorised persons. Only authorised persons in KIR may request for access to data. Access to archived registers of events kept in the strongboxes is granted only to persons acting as the security inspector. The carriers in the archives are reviewed every 2 years. Data integrity is verified. Data from carriers that are older than 2 years are recorded on new carriers, while the older ones are destroyed in accordance with relevant procedures.

5.6. Replacement of the key

5.6.1. Replacement of COPE Szafir Qualified keys

The keys of certification authority are replaced in a way that ensures compliance with the established minimum validity period of the certificates. Well ahead of the expiry of the certificate of a given certification authority, a new independent public key infrastructure is created in which a new pair of keys and a certificate obtained from the supervisory authority of the new certification authority are generated. Two authorities operate until the expiry of the certificate of the old certification authority. The new certification authority assumes the role of the expiring one, and performs all actions related to the support of certificates: generation, suspension and revocation of certificates, and generation of CRLs. The expiring certification authority only handles revocations and suspensions of certificates issued within its infrastructure, and generates CRLs till it ceases to perform its operational activities (certificate expiry).

The frequency of replacement of certification authority keys depends on the validity periods of certificates issued to subscribers. The validity periods of certificates are described in point 6.3.2.

A new certificate of the certification authority is published at the website: www.elektronicznypodpis.pl and distributed in software made available by KIR.

5.6.2. Replacement of Szafir TSA keys

The replacement of the keys of Szafir TSA shall be done in a manner ensuring maintenance of the maximum validity period of issued time stamps. After a new pair of the keys for the authority has been generated and after obtaining a certificate from a supervision authority, time stamps shall be electronically sealed and verified with a new certificate. The authority's new certificate shall be published at www.elektronicznypodpis.pl and distributed in software made available by KIR.

5.7. Compromising of the key and launch after failures or natural disasters

KIR exercises its best efforts to ensure continued and failure-free operation of the COPE Szafir Qualified and Szafir TSA. The technical infrastructure of the certification authorities has, for example, a doubled hardware and software configuration outside the primary location, backup power supply (power generator) in both locations and other safety measures that enable continued operation in the event of any failure. In the event of failure of the primary location which prevents the provision of basic functionalities of the certification authority, it is launched in the backup location within 24 hours from the moment of detecting the failure.

5.7.1. Procedures for handling incidents and responding to threats

KIR has a set of procedures for handling incidents and unforeseen events. All incidents are analysed in detail by proper organizational units and corrective measures are implemented. Details are specified in the internal procedure of KIR.

If security is breached or integrity is lost which is of material impact on the provided trust service or personal data processed in it, KIR shall inform a supervision authority not later than within 24 hours from its occurrence.

5.7.2. Procedures for recovering computation resources, software and/or data

KIR has a set of operational procedures in the event of necessity to recover the resources. Each location has the resources that allow for the recovery of full functionality of the certification authority. These are, in particular:

1) data backup;
2) backup of keys of certification authorities;
3) copies of cryptographic cards with shared secrets and operators' cards;
4) carriers with software of the key certification system;
5) operational procedures of certification authorities.

The recovery procedures are included in the Business Continuity Plan, hereinafter referred to as “BCP,” and are regularly tested.

5.7.3. Actions in the situation when a private key of the certification authority ort time-stamping authority has been compromised

Compromising the key of the certification authority is a crisis situation and is subject to the BCP. If a private key of COPE Szafir Qualified or Szafir TSA has been compromised, KIR undertakes the following actions:

1) notifies the supervision authority;
2) applies to the supervision authority for the revocation of the certificate of the certification authority;
3) notifies about the revocation of the certificate of the certification authority using available communication channels.

Detailed actions in the event of compromising the key are described in the KIR internal procedures.

5.7.4. Ensuring business continuity after disasters

In the event of disasters and other unforeseen circumstances, KIR has the BCP. The BCP procedures strictly define the way of conducting actions necessary for restoring operations. The BCP procedures are periodically tested.

5.8. End of provision of qualified trust services

KIR has the right to discontinue the provision of qualified trust services. KIR has implemented and maintains the operations end plan which defines the actions of KIR in the event of decision about the end of provision of qualified trust services.

KIR shall have the right to discontinue provision of trust services. KIR has and maintains the Business End Plan defining how KIR will proceed if KIR takes a decision on ending provision of the qualified trust services.

Subscribers and ordering parties shall be informed about the end of business with a due notice. Subscribers, ordering parties, and trusted parties shall have no right to make any claims against KIR because of that.

KIR shall continue to perform its duties with regard to support of applications for suspension or cancellation of certificates and publication of a list of suspended and cancelled certificates. Otherwise, ordering parties shall have the right to reimbursement of remuneration proportionate to a period of use of the certificate due for its purchase.

All certificates, time stamps issued by KIR and related documents shall be provided to a minister competent for digitisation or an entity indicated by the minister.

6. TECHNICAL SECURITY PROCEDURES

Below are described the procedures for generation and management of cryptographic keys of the certification authority, time-stamping authority, operators and subscribers. This chapter also includes the description of technical solutions employed to secure keys and ensure high level of infrastructure security.

6.1. Generation and installation of a pair of keys

6.1.1. Generation of a pair of keys of the certification authority and subscribers

Keys are generated and installed on the basis of internal KIR procedure which governs the rules of generation and management of keys of the COPE SZAFIR Qualified certification authority.

The COPE SZAFIR Qualified authority acts as an operational authority. It has two pairs of RSA keys:

1) one pair of key, one of which public key is certified by NCCert National Certification Centre run by the National Bank of Poland is used to generate the certificates of subscribers and to publish the lists of revoked/ suspended certificates (CRLs).

2) the second pair of keys is used for securing communication within the COPE SZAFIR Qualified infrastructure.

The COPE SZAFIR Qualified keys are generated within a separate environment, this is the CA server is dedicated only to supporting the processes related to COPE SZAFIR Qualified, and is equipped with the cryptographic module with the Common Criteria EAL4+ certificate. The generation of keys and operations related to the use of private key are performed only in the cryptographic module and they are registered.

In order to generate the keys a committee comprised of KIR employees is established. All actions and their completion times are registered in the action registration document. After the generation procedure is completed, the document, together with relevant reports, is signed by the committee and filed in the archives.

The operators' keys are used for signing the subscribers' requests for the certification of keys. They are also used for the authorisation of operators in the system and securing communication between the client application and the Registration Authority programme module. The operators' keys are recorded on cryptographic cards and issued to authorised employees under the supervision of the security inspector.

A separate pair of keys with the certificate issued by COPE Qualified Szafir shall be used for signing OCSP responses.

A subscriber themselves may generate a pair of keys and present a public key for certification in the form of the PKCS#10 request. The keys for subscribers may also be generated by COPE SZAFIR Qualified on cryptographic cards.

Signature and seal creation data managed by KIR on behalf of subscriber are generated in a qualified electronic signature creation device which meets the requirements specified in Annex II of eIDAS Regulation and published on the list referred to in art 31 par 2 eIDAS Regulation (Qualified Signature and Seal Creation Device (QSCD) Cryptomathic Signer, version 4.8, Cryptomathic Signer SAM v5.1 for Utimaco Cryptoserver CP5). All cryptographic operations are performed by the SCE Secure Code Execution module, which is an integral part of the cryptographic module. During the signature operation to the SCE module, encrypted signature creation data are sent. Signature creation data are decrypted in a cryptographic module and used for signing. The cryptographic module returns the signature.

6.1.2. Time-stamping authority pair of key generation

Qualified electronic seal creation devices are used to generate electronic stamps. Such devices are used solely for the provision of a time stamping service. As used in KIR they have a Common Criterial EAL 4+ certificate and are protected against unauthorised access. Only authorised persons shall have access to the devices. Each attempted access to a given device, irrespective of the undertaken action and its outcome, including, but not limited to, actions related to generation of data used to seals on time stamps or their use is monitored and registered in an information and communication technology system.

6.1.3. Authorities' infrastructure keys

Each of the authorities has its own infrastructure keys used to:

1) ensure integrity of transmission of data related the provision of services (request for the issuance of time stamps, information on errors resulting in the process of issuance of time stamps)) and storing data (data in rest) such as signature creation data;

2) ensure integrity of the registers of events stored at KIR;

3) ensure integrity of data relating to archiving of data related to the provision of time stamping services;

4) secure access to the software and devices used for the provision of a service of time stamp issuance.

5) signing the code placed in the cryptographic module.

6.1.4. Delivery of the private key to the subscriber or entitled person

If keys are generated in COPE Qualified SZAFIR, the private key and the public key is provided to the subscriber (an electronic signature in case of qualified certificates) or to the eligible person (in case of other certificates) together with the public key certificate. During the first registration in COPE SZAFIR Qualified, the subscriber/entitled person must personally appear in the registration authority in order to verify their identity and collect the carrier with private key, or, if the Agreement provides so, the process of identity verification and delivery of private key may also take place in the offices of the principal or another place when a relevant on-site service of the operator has been purchased. If the keys are issued on a cryptographic card, access to the private key is secured with the PIN/PUK codes which are individually assigned by the subscriber after receiving the card.

When KIR generates signature and seal creation data on behalf of subscriber and manages these data on behalf of subscriber they are not deliver to the subscriber. The subscriber has access to these data based on:

1) identification with electronic identification means that is referred to in section 3.4,

2) mobile application which generates access codes to authorization to signature creation data.

In the case of authorization of access to signature creation data based on the mobile application, the link of a given subscriber with the mobile application used by him is based on:

1) authorization with the use of electronic identification means that is referred to in section 3.4;

2) qualified certificate used by the subscriber containing the name and surname and PESEL or number and series of document confirming the identity

3) identity verification at the registration authority.

Linking a mobile application with a given subscriber requires:

1) installation of a mobile application on a mobile device which is under the control of the subscriber;

2) entering by the subscriber a PIN code prepared by him that protects access to the application;

3) obtaining a one-off activation code by log on to the dedicated website using an electronic identification means that is referred to in section 3.4 or a qualified certificate held by the subscriber or an identity verification at the registration authority;

4) entering the activation code referred to section 3), in the mobile application together with the subscriber's PESEL number or number and series of the ID document, depending on which data was used to identify the subscriber before generating signature creation data and certificate.

Where KIR generates electronic seal data for the subscriber, which is managed by KIR on behalf of the subscriber, it is not transferred to the subscriber. Authorization of access to the seal data is carried out based on an active mobile application that generates access codes for authorization of access to the signature data.

After the generation of a seal certificate, for which data is managed by the NIR, the mobile application used by the subscriber is activated. Activation takes place on the basis of:

1) qualified certificate of electronic signature held by the subscriber, including name and PESEL or number and series of identity document;

2) verification of identity at the point of registration.

A subscriber who has an active mobile application may activate the mobile application for another user associated with the organization whose data is indicated in the electronic seal certificate. In such a case, the subscriber is responsible for verifying the person to whom he allows access.

Associating the mobile application with a particular subscriber or user authorized by the subscriber requires:

1) installation of the mobile application on a mobile device under the control of the subscriber or user;

2) entry by the subscriber or user of a self-prepared PIN code protecting access to the application;

3) entering the authorization code in the mobile application along with the organization's identifier.

Providing access to data for electronic signatures based on a mobile application is a 2FA (two facto authorization) two-component process, which is an example of strong authentication.

1. Type1 factor - something you know - a multi-valued component that appears as:

   a) PIN for a mobile application installed on a mobile device that is under the user's control;

b) one-off authorization code generated in the mobile application;

2. Type2 factor - something you have. The second component is the type-two component that is inseparably connected with the subscriber - that is, a mobile device with a mobile application profiled for a given user.

6.1.5. Delivery of public key to the certification authority

If a pair of keys is generated by the certification authority, it is not necessary for the subscriber to deliver the public key. If the keys are generated by the subscriber, they deliver their public key to the registration authority in the form of electronic request signed with the private key which complies with the PKCS#10 standard.

6.1.6. Delivery of public key of certification authorities to relying parties

The public key of the certification authority and the public key of the time-stamping authority are made available to relying parties in the form of certificates. The certificates of authorities are certificates signed by the NCCert National Certification Centre run by the National Bank of Poland. Certificates of certification authorities are published on the KIR website: www.elektronicznypodpis.pl.

Certificates of certification authorities are also distributed in the proprietary software of KIR that is used to support electronic signature.

6.1.7. Length of keys

The keys of the certification authority have the length of 2048 or 4096 RSA bits. The keys of time-stamping authority have length of 4096 bits. The keys of subscribers shall have the length at least of 2048 RSA bits and ECC 256 bits. The infrastructure keys used for managing signature and seal creation data on behalf of users have the length of 3072 bits DSA and 256 bits of symmetric AES Parameters of public key generation and quality check.

The process of generating keys in the certification and time-stamping authorities is conducted using pseudo-random number generator with the application of strong cryptographic algorithms. KIR checks if the key presented for certification satisfies the requirements set forth in point 6.1.5.

6.1.8. Application of keys (by key usage field for X.509 v.3 certificates)

Key usage is defined in the KeyUsage field (OID: 2.5.29.15) with extensions of standard certificates.

Key	Application
CA keys used for the certification of subscribers' keys	Certificate Signing CRL Signing
CA keys used for communication within the infrastructure	Digital Signature Non-Repudiation Key Encipherment Data Encipherment Key Agreement
Keys of the time stamping authority for generation of time stamps	TimeStamp
Keys of the registration operators	Digital Signature Non-Repudiation

Keys of the subscribers	Non-Repudiation and Digital Signature for certificates for electronic signature and electronic seal Digital Signature for certificates for electronic signature and electronic seal Digital Signature and Key Agreement for the certificates for certification of websites

6.2. Protection of private key and technical control of the cryptographic module

Private keys of the certification authority and time-stamping authority are protected in a way that prevents their unauthorised usage, loss or disclosure. The keys are generated and stored in secure environment that is protected by cryptographic hardware modules. The keys are divided into secrets, and access to secrets is granted only to the appointed and trusted employees of KIR.

Keys of the subscribers for certificates of electronic signature and for electronic seal, if they are generated by KIR, shall be generated on cryptographic cards that meet the requirements of the eIDAS Regulation for qualified electronic signature creation device or qualified electronic seal creation device.

Pair of keys generated by KIR on cryptographic card is secured by KIR with PIN and PUK codes generated by KIR and printed in the secure envelope. Before the first usage of card subscriber shall change PIN code on his own code.

Keys of the subscribers for the certificates for websites authentication may be generated by a certification authority in the form of PKCS#12 password-protected.

Signature and seal creation data which are managed by KIR on behalf of subscriber, are generated and used for creating signature or seal in hardware cryptographic modules dedicated to this purpose, meeting the requirements for a qualified signature and seal creation device within the meaning of the eIDAS Regulation. Access to these data is organize according to section 6.1.4.

6.2.1. Standards for the cryptographic module

Hardware modules used in the certification authority for the trusted services meet the following standards:

- the module for the protection of the COPE SZAFIR Qualified key – Common Criteria EAL4+;
- the module for the protection of the Szafir TSA key – Common Criteria EAL4+.
- Cryptographic modules secured infrastructure keys for signature and seal creation data managed by KIR on behalf of the subscriber - Common Criteria EAL4+ with the function SCE (Secure Code Execution) and firmware complied with eIDAS Regulation requirements.

6.2.2. Private key division

The private key of the certification authorities is divided into secrets that are co-shared according to the *m* z *n* model.

Chart of the private key division:

Certification authority	Total number of secrets [n]	Number of secrets necessary to use the key [m]
COPE SZAFIR Qualified	5	2
Szafir TSA	5	2

Each of the secrets is stored on a cryptographic card protected with a PIN code. Secrets are distributed among trusted persons during the key generation ceremony. Persons having access to secrets must be present during the key generation ceremony and supervise the correctness of its completion. The fact of key generation, the correctness of the ceremony and the delivery of the card are confirmed by the secret holders in a report. The secret holders are responsible for duly securing the cards with a PIN code known only to them. A secret holder is obliged to ensure a secure place for keeping the secret, its protection against disclosing, copying and making it available to unauthorised persons, and to prevent the unauthorised use of the secret. A secret holder must, at the same time, ensure the possibility of recovering the secret if the holder is not available.

A secret holder is responsible for due protection of the secret. In the event of loss, theft, damage to the card or any other situation that violates the security of the secret, one should immediately inform the security inspector about this fact.

6.2.3. Depositing of the private key

KIR does not provide the services of depositing and storing private keys of the subscribers with the exception of signature and seal creation data managed by KIR on behalf of subscribers The keys of the certification authority and time-stamping authority are not deposited outside KIR.

Signature and seal creation data managed by KIR on behalf of subscribers are stored in the encrypted form and are used only inside the cryptographic module.

6.2.4. Backup copies of the private key for certification and time-stamping authority

For the certification authority and time-stamping authority there are createed backup copies of keys and stored in the backup location. Copies of the cards with shared secrets are deposited in the strongboxes of the authority, and access to the strongboxes is granted only to security inspectors. PINs to the cards are kept in sealed envelopes deposited in strongboxes in other rooms. Disk files of the closed security environment of cryptographic modules are kept on backup servers in the form encrypted with the 3DES algorithm. A full set of materials used for recovering a private key of the authority is not to be kept in a single place. Should the need arise to recover the key from backup copies, the procedure for entering the key into the module is performed, as described in point 6.2.6.

6.2.5. Archiving of the private key

KIR does not archive private keys of the certification authority and time-stamping authority. After the expiry of the certificate of public key of the certification authority and time-stamping authority and the discontinuance of operations, the private keys of the authorities are destroyed.

KIR does not archive private keys of the subscribers including signature and seal creation data managed by KIR on behalf of users.

6.2.6. Uploading private key to the cryptographic module or its downloading

Private key is uploaded to the cryptographic modules in the following situations:

1) launch of the certification authority or time-stamping authority, during the system start-up;
2) recovery of the key of the certification authority or time-stamping authority in the backup location;
3) recovery of infrastructure for signature and seal creation data managed by KIR In backup location or exchanging SCE code stored inside the cryptographic module;
4) replacement of the cryptographic module.

The key is uploaded to the module in the presence of holders of co-shared secrets. To upload the key it is necessary to have present the number of secrets described in point 6.2.2. Uploading is carried out in a closed security environment. A private key is made up of elements. Fragments of the secret key are provided in sequence from the cards, enciphered files are uploaded to the module memory, and then deciphered. The private key is ready to use. Uploading the key to the module is recorded in the register of events.

6.2.7. Storing the private key in the cryptographic module

After deciphering and uploading the private key to the memory of the cryptographic module, it is hardware protected. It is not possible to read the value of the private key from the module, as this key never leaves the module. Operations that require the use of a private key are performed in the cryptographic module.

The keys of the registration authorities and of the operators are stored in the cryptographic cards protected with PIN and PUK codes.

6.2.8. Activation of the private key

Once uploaded into the module, the key is active. Signature/ seal operations are performed in separate sessions. The programme module of the certification authority that uses a private key must be authenticated to perform the signature/ seal operation. Only a programme module that uses the infrastructure keys may perform such operations. After the authentication, an active session is opened, and data for signature/ seal are sent to the module.

6.2.9. Deactivation of the private key

When the operation of signing/ sealing the data in the module has been completed, the session between the module and the software is closed. The execution of another signature/ seal requires the opening of a new session. The key may be deactivated in the module by system administrator upon the request of the security inspector or if it is necessary to perform deactivation (in the event of threat to the key, system shut-down). Deactivation is performed by clearing the memory of the cryptographic module. Deactivation of the key is recorded in the register of events.

6.2.10. Destruction of the private key

After the end of operations of the certification authority or time-stamping authority, all elements used for the recovery of the private key for this authority are destroyed.

The cards that contain co-shared secrets are cleared with the use of utility software and then physically destroyed by cutting.

Carriers and cards are destroyed by a specially formed committee. The fact of destroying the carriers and cards is confirmed with a report signed by the committee members.

6.2.11. Possibilities of the cryptographic module

The parameters of cryptographic modules are described in point 6.2.1.

6.3. Other aspects of key management

The following points describe aspects related to the certificate validity period and archiving of keys.

6.3.1. Archiving of public keys

KIR archives the public keys of certification authority and time-stamping authority. Archiving is to create the possibility of verifying electronic signatures after the lapse of the validity period of the certificate of the authority and the closure of its operations.

Archiving pertains to the keys of the certification authority and the time-stamping authority. Public keys are archived in the form of certificates. The archiving is conducted by the security inspector. The archiving is performed by recording files with certificates on optical carriers. Archive files are electronically signed by the security inspector. Details of creating electronic archives are described in point 5.5.

The archiving period for public keys of the certification authority and the time-stamping authority is 20 years.

6.3.2. Validity period of certificates

Validity period of certificates:

Certificate of an entity	Maximum validity period
COPE SZAFIR Qualified	11 years
Subscriber	3 years
Szafir TSA	11 years

6.3.3. Validity period of time stamps

The maximum period of validity of a certificate used for verification of electronic stamps for electronic time stamps shall be 11 years starting from the certificate issuance date.

A time stamp issued by KIR shall be valid through the end of a validity period of the certificate issued for KIR. If the period of validity or storage of a document for which an electronic time stamp has been issued is longer, the subscriber should apply for issuance of another electronic time stamp prior to the end of the validity period of the certificate that is referred to above.

6.4. Activation data

If the certificate and the pair of keys have been generated on a cryptographic card, the subscriber receives PIN and PUK codes securing access to the card in a safe envelope.

The subscriber or another person authorised to submit a request for revocation/ suspension of the certificate is obliged to provide KIR with passwords for certificate suspension and revocation. The password, written down on a piece of paper, should be put in a non-transparent envelope.

The following data should be additionally placed on the internal envelope:

1) full name of the authorised person;
2) PESEL number of the authorised person or another personal identifier assigned by a competent authority.

If the password is submitted by a person other than the subscriber, they are obliged to present legal grounds authorising them to request the revocation or suspension of the certificate.

The envelopes with passwords are stored at KIR or in the archives, and access to them is granted only to persons authorised at KIR to suspend and revoke the certificates.

The person authorised to submit request for revocation or suspension of the certificate has the right to change the previously given password.

Failure to provide the password shall prevent submission of a request for cancellation or suspension of a certificate over the Internet.

Failure to provide a password makes it impossible to submit a request for revocation or suspension of the certificate by phone, unless it concerns a certificate for which signature creation data are managed by KIR and whose validity period is shorter than 24 hours.

6.4.1. Generation and installation of activation data

The subscriber should assign the codes to secure the card with a pair of keys and the certificate with the use of the application for card management that has been provided by KIR together with the card.

6.4.2. Protection of activation data

The PIN code assigned by the subscriber and the PUK code received by the subscriber with the cryptographic card should be known only to the subscriber.

It is the subscriber's responsibility to protect the PIN and PUK codes for the card.

Any disclosure of the PIN and PUK codes should be a premise for the request for suspension or revocation of the certificate.

Disclosure of data used for authorization of access to signature and seal creation data managed by KIR on behalf of subscribers constitutes a prerequisite to request suspension or revocation of the certificate.

6.4.3. Other aspects related to activation data

Copies of passwords to protect access to files with pairs of keys are not stored at KIR. KIR does not have any codes or data that enable recovering the PIN and PUK codes securing access to the card that have been assigned by the subscriber.

6.5. Time source

The public ntp servers of the Central Office of Measurements (GUM) executing UTC time (PL) are used for the provision of a service of the time stamp as a reference source of time. Time from the time source and reference servers is constantly audited and compared with relevant accuracy.

KIR shall also use its own NTS-3000 clocks by Elproma. KIR has two NTS-3000 clocks, with one in each certification authority. The clocks used for the issuance of electronic time stamps are synchronised with Universal Coordinated Time on the basis of a GPS signal reaching the device from the satellites circling the globe. The accuracy of GPS synchronisation is +/-500 nanoseconds. Each of the clocks provides time with the use of the three independent network interfaces using protocols for sending a NTP and SNTP time format. Time accuracy at the level of an NTP protocol is +/- 10 milliseconds.

6.6. Supervision over computer system security

For the provision of trust services there are used hardware and specialist software that make up a closed computer system.

6.6.1. Technical requirements concerning specific security measures for computer systems

Servers and work stations of the system are specially prepared to work in the certification system (hardening of operating systems) and protected with anti-virus software. The management of accounts in the system is multi-level, and takes place at the level of domain/ operating system, application of the certificate management system, time-stamping system and databases. User accounts are assigned in accordance with the rules described in internal documents of KIR.

6.6.2. Assessment of computer system security

Computer system security is assessed on the basis of the requirements of the eIDAS Regulation.

6.7. Life cycle of technical security measures

6.7.1. System development supervision

System development is supervised by the security inspector. They approve the system configuration, and the planned changes in software and hardware. All changes in the system are recorded in the system documentation and entered to the register of events.

Computer hardware and cryptographic modules are selected in such a way as to meet the specified functionality and security standards.

6.7.2. Supervision over security management

KIR has extended internal procedures for security management. System security is constantly monitored at many levels. The examinations cover software integrity, network traffic, configuration of the system and security devices. A system inspection report is drawn up regularly. System security is supervised by professionals from KIR.

6.7.3. Supervision over the life cycle of security measures

The CP does not impose any life cycle for the applied security measures. Security measures are replaced in the event of necessity to apply other measures than those that are currently used, amendments in legal regulations or if they are technologically outdated and do not comply with the current standards and norms.

6.8. Supervision over computer network security

The KIR computer network security is supervised by qualified staff members.

7. CERTIFICATE, CRLs and TIME STAMP PROFILE,

7.1. Certificate profile

Certificates issued by KIR consist of three parts:

- contents of the certificate (*tbsCertificate*);
- identifier of the electronic seal algorithm (*signatureAlgorithm*);
- electronic seal (*signature*).

The first part of the certificate (*tbsCertificate)* consists of the following basic fields:

Field name	Field meaning	Content
version	marking of the certificate version	3
serialNumber	certificate serial number	unique certificate number assigned in the system for the issuance of certificates
signature	identifier and parameters of electronic seal used by KIR	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identifier specifying KIR as the issuer of the certificate	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN=COPE SZAFIR Qualified
validity	marking of the beginning and end of validity of the certificate issued by KIR	time of certificate generation and end of the certificate validity period with the accuracy of up to a second
subject	identifier of the subscriber linked to the public key placed in the certificate	value referred to in point 4
subjectPublicKeyInfo	value of the public key with the algorithm identifier with which the key is associated	public key
extensions	standard and special extensions	according to the table below

Permitted extensions of the certificate are presented in the table below:

Extension name	Critical/ non-critical	Extension meaning	Content
Standard extensions			
authorityKeyIdentifier	non-critical	identifier of the public key used to verify the issued certificate	160 bit SHA-1 hash function of the key
subjectKeyIdentifier	non-critical	identifier of the certificate containing the hash of the public key included in the certificate	160 bit SHA-1 hash function of the key
keyUsage	critical	determines the scope of use of the public key included in the certificate	Pursuant to 6.1.9
extendedKeyUsage	non-critical	defines the permitted scope of application of the public key included in the certificate – this applies to certificates for certification of websites only	clientAuthentication – verification of the client's certificate, serverAuthentication – verification of the server's certificate,

certificatePolicies	non-critical	determines the certification policy according to which a given certificate has been issued	- identifier compliant with point 7.1.4
subjectAltName	critical/ non-critical	complementary name of the subscriber	In case of the qualified certificates for electronic signature and the qualified certificates for electronic seal the field contains an electronic mail address. In case of the qualified certificates for websites authentication the field is mandatory and contains the domain name (FQDN - Fully- Qualified Domain Name).
basicConstraints	critical	allows for checking if the certificate owner is an end user or an entity issuing certificates	empty sequence
cRLDistributionPoints	non-critical	defines URL at which the current CRL is published	
authorityInfromation Access	non-critical	indication of OCSP URL at which the certificate validity status may be checked	
Special extensions – qcStatement			
qcCompliance	non-critical	statement of the issuer of qualified certificate	statement that the certificate is a qualified certificate for electronic signature
qcSSCD	non-critical	indication that the private key is stored on qualified electronic signature creation device or on qualified electronic seal creation	indication that the private key is stored on qualified electronic signature creation device or on qualified electronic seal creation device
qcType	non-critical	indication of a type of the qualified certificate	Indication of one of the three types of the certificate: - certificate for electronic signature, - certificate for electronic seal, - certificate for authenticating websites.
qcLimitValue	non-critical	amount limit	limit of transaction that may be confirmed with the certificate at one time;
qcPDS	non-critical	Information about KIR services	link to the document describing the basic terms and conditions of the provision of trust services involving the issuance of certificates

subjectSignatureType	non-critical	indication on whose behalf the certificate owner acts	permitted values: a. on their own behalf; b. as a representative of another natural person, legal person or organizational unit without legal personality; c. as a member of authorities or authorities of legal person or organizational unit without legal personality; d. as a body of public authorities.
*qcPSD2**	non-critical	Roles regarding to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2)	a. roles according PDS2; b. name and identifier of the competent authority.

*- only in the certificates for electronic seals or for website authentication

7.1.1. Algorithm identifiers

The certification authority seals the certificates with the RSA algorithm having 2048 or 4096 bit keys and the SHA-256 hash function.

Subscribers' certificates are issued for the RSA keys with a minimum length of 2048 bits or ECC 256 bits and the SHA-256 hash function.

Till 1 July 2018 subscribers’ certificates were issued with RSA 2048 algorithm and SHA-1 has function.

7.1.2. Name forms

The certificates contain indication of the subject of the certificate issuer (KIR) and the subject of the certificate (subscriber) drawn up in accordance with point 3.1.1.

7.1.3. Restrictions imposed on names

The qualified certificates may not contain IP addresses in the subject and subjectAltName fields.

Domain names may be included only in the qualified certificates for certification of websites. In the subject and subjectAltName fields those certificates may not contain domain names that are not registered in the online DNS system.

7.1.4. Identifiers of certification policy

The identifier of policy for the qualified certificates for electronic signature is as follows:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-kw szafir-osoba fizyczna(1).
```

The policy identifier for the qualified certificates for electronic seal looks as follows:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-kw szafir-osoba prawna(3).
```

The policy identifier for the qualified certificates for websites authentication looks as follows:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-kw szafir-witryna(4).
```

The policy identifier for the qualified certificates for electronic signature where the signature data are managed by KIR looks as follows:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-kw mszafir-podpis(5).
```

The policy identifier for the qualified certificates for electronic seal where the seal data are managed by KIR looks as follows:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-kw mszafir-pieczec(6).
```

7.1.5. Applications of extensions not allowed in the certification policy

KIR does not envisage placing other extensions than those indicated in point 7.1 in the certificates.

7.1.6. Processing of semantics for critical extensions of the certification policy

KIR does not define any requirements in this respect.

7.2. CRL profile

The list of suspended and revoked certificates consists of three parts:

- content of the certificate (*tbsCertList*);
- identifier of the electronic seal algorithm (*signatureAlgorithm*);
- electronic seal (*signature*).

The first part of CRL (*tbsCertList)* consists of the following basic fields:

Field name	Field meaning	Content
version	marking of the version of the list of suspended and revoked certificates	2
signature	identifier and parameters of electronic seal used by KIR	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identifier distinguishing a qualified trust service provider that has issued the certificate	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN=COPE SZAFIR Qualified
thisUpdate	date of issuing the list of suspended and revoked certificates	time of CRL generation with the accuracy of up to a second
nextUpdate	planned time of issuing the next list	planned time of generation of the next CRL with the accuracy of up to a second
revokedCertificates	list of suspended and revoked certificates	– certificate serial number – date and time of certificate revocation/ suspension – code of certificate revocation/ suspension

crlExtension	extensions for the list of suspended and revoked certificates:	– identifier of the key of entity for verifying the signature under the list of suspended and revoked certificates – monotonically increasing number of the list of suspended and revoked certificates – point in which CRLs are placed (IssuingDistributionPoint)

Permitted codes of certificate revocation/ suspension are:

- *unspecified* – cause for certificate revocation is not known;
- *keyCompromise* – certificate has been revoked due to compromise or suspected compromise of the private key;
- *cACompromise* – certificate has been revoked due to compromise or suspected compromise of the CA key;
- *affiliationChanged* – certificate has been revoked due to the change of data included in the certificate;
- *susperseded* – certificate has been revoked because the private key has been superseded;
- *cessationOfOpertion* – certificate has been revoked due to the discontinuation of its use for the purposes for which it has been issued;
- *privilegeWithdrawn* – certificate has been revoked due to the change of data included in the certificate defining the role of the certificate owner;
- *certificateHold* – certificate has been suspended.

In the event of the *certificateHold* code occurrence, the list of suspended and revoked certificates may contain additional non-critical extensions defining possible procedures for handling the suspended certificate:

- indication of the need to contact the certificate issuer to clarify the cause for certificate suspension;
- indication of obligatory rejection of the reviewed certificate.

The *signatureAlgorithm* field contains the identifier of the algorithm used by the certification authority to generate electronic seal under CRL. In case of certification authorities, it is the RSA algorithm having 2048 or 4096 bit keys and the SHA-256 hash function.

The *signature* field contains an electronic seal generated by the issuer of CRL, the certification authority. For data included in the tbsCertificate field there is generated the value of the hash function which is enciphered with the private key of the certification authority.

CRLs are published at the following website: www.elektronicznypodpis.pl. Access to lists is unlimited and free of charge.

7.3. OCSP profile

KIR provides an on-line certificate status verification service on the basis of OCSP (Online Certificate Status Protocol) in accordance with RFC 6960. The OCSP service is provided for all certificates described in the CP. The service is provided in the authorized responder mode (Authorized Responder). Responses of the responder are authenticated with a special certificate issued for that purpose by the authority the status of whose certificates is authenticated by the responder. Responders' certificates include the extendedKeyUsage extension that corresponds to the value of id-kp-ocspSigning (OID 1.3.6.1.5.5.7.3.9).

The certification authority that makes the OCSP service available includes information about the way of accessing the service in the issued certificates. Such information is included in the AuthotityInformationAccess extension and has the following form:

```
id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }

   AuthorityInfoAccessSyntax  ::=
           SEQUENCE SIZE (1..MAX) OF AccessDescription

   AccessDescription  ::=  SEQUENCE {
           accessMethod          OBJECT IDENTIFIER,
           accessLocation        GeneralName  }
```

In the accessMethod field there is the access method for OCSP (OID id-ad-ocsp), while the accessLocation field contains a URL to the OCSP service.

7.3.1. Certificate status query

The OCSP server accepts queries about the certificate status with the syntax compliant with RFC 2560:

```
OCSPRequest     ::=     SEQUENCE {
       tbsRequest                  TBSRequest,
       optionalSignature   [0]     EXPLICIT Signature OPTIONAL }

   TBSRequest      ::=     SEQUENCE {
       version             [0]     EXPLICIT Version DEFAULT v1,
       requestorName       [1]     EXPLICIT GeneralName OPTIONAL,
       requestList                 SEQUENCE OF Request,
       requestExtensions   [2]     EXPLICIT Extensions OPTIONAL }

   Signature       ::=     SEQUENCE {
       signatureAlgorithm      AlgorithmIdentifier,
       signature               BIT STRING,
       certs               [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL}

   Version         ::=             INTEGER  {  v1(0) }

   Request         ::=     SEQUENCE {
       reqCert                     CertID,
       singleRequestExtensions     [0] EXPLICIT Extensions OPTIONAL }

   CertID          ::=     SEQUENCE {
       hashAlgorithm       AlgorithmIdentifier,
       issuerNameHash      OCTET STRING, -- Hash of Issuer's DN
       issuerKeyHash       OCTET STRING, -- Hash of Issuers public key
 serialNumber        CertificateSerialNum }
```

7.3.2. OCSP server response

The OCSP server returns responses about the certificate status with the syntax compliant with RFC 6960:

```
OCSPResponse ::= SEQUENCE {
      responseStatus         OCSPResponseStatus,
      responseBytes          [0] EXPLICIT ResponseBytes OPTIONAL }

   OCSPResponseStatus ::= ENUMERATED {
       successful            (0),  --Response has valid confirmations
       malformedRequest      (1),  --Illegal confirmation request
       internalError         (2),  --Internal error in issuer
       tryLater              (3),  --Try again later
                                   --(4) is not used
       sigRequired           (5),  --Must sign the request
       unauthorized          (6)   --Request unauthorized }

   ResponseBytes ::=       SEQUENCE {
       responseType   OBJECT IDENTIFIER,
       response       OCTET STRING }

   BasicOCSPResponse       ::= SEQUENCE {
      tbsResponseData      ResponseData,
      signatureAlgorithm   AlgorithmIdentifier,
      signature            BIT STRING,
      certs                [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL }

   ResponseData ::= SEQUENCE {
      version              [0] EXPLICIT Version DEFAULT v1,
      responderID              ResponderID,
      producedAt               GeneralizedTime,
      responses                SEQUENCE OF SingleResponse,
      responseExtensions   [1] EXPLICIT Extensions OPTIONAL }

   ResponderID ::= CHOICE {
      byName               [1] Name,
      byKey                [2] KeyHash }

   SingleResponse ::= SEQUENCE {
      certID                       CertID,
      certStatus                   CertStatus,
      thisUpdate                   GeneralizedTime,
      nextUpdate         [0]       EXPLICIT GeneralizedTime OPTIONAL,
      singleExtensions   [1]       EXPLICIT Extensions OPTIONAL }

   CertStatus ::= CHOICE {
       good        [0]     IMPLICIT NULL,
       revoked     [1]     IMPLICIT RevokedInfo,
       unknown     [2]     IMPLICIT UnknownInfo }

   RevokedInfo ::= SEQUENCE {
       revocationTime              GeneralizedTime,
 revocationReason    [0]     EXPLICIT CRLReason OPTIONAL }
```

Information about the certificate status is included in the CertStatus field of the SingleResponse structure. Three values are possible:

0 – good – certificate has been issued by KIR and is not included in CRL,

1 – revoked – certificate has been issued by KIR and has been revoked or suspended, and is included in CRL,

2 – unknown – certificate status is not known.

In case of status 1 (revoked), the information about time and cause of revocation is put in the revocationTime and revocationReason fields of the RevokedInfo structure. The revocationReason field may assume the CRLReason values according to RFC 2459 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”:

```
CRLReason ::= ENUMERATED {
        unspecified(0),
        keyCompromise(1),
        cACompromise(2),
        affiliationChanged(3),
        superseded(4),
        cessationOfOperation(5),
        certificateHold(6),
        privilegeWithdrawn(9)
}
```

7.3.3. Version number

Responses of the OCSP services generated by the OCSP server are compliant with RFC 6960. The version number is marked with 0, which corresponds to version v1.

7.3.4. OCSP extensions

The OCSP server response contains the OCSP Nonce Extension (OID 1.3.6.1.5.5.7.48.1.2) that contains a phrase linking the query with the response. The value in the OCSP response is the same as the phrase in the query. The purpose of using the phrase is to prevent replay attacks on the OCSP server.

Responses of the OCSP server do not contain private extensions.

7.4. Time stamp profile

In response to a correct request for the issuance of a time stamp, KIR shall issue a time stamp on the basis of the time source and information included in the request. The time stamp contains an abbreviation of the document included in the request and the time current at the moment when such electronic time stamp is generated.

In the event of an incorrect request or other obstacles preventing submission or issuance of a correct time stamp, the subscriber shall receive information about an error.

7.4.1. Format of the request for the issuance of an time stamp

The subscriber making a request for the issuance of a time stamp shall prepare the request electronically signed or sealed in accordance with a syntax of the TSP protocol according to RFC 3161 and ETSI EN 319 422.

To identify the user applying for a time stamp, besides the format of the request for the issuance of a time stamp defined in RFC 3161, a mechanism of signing requests in accordance with CMS (PKCS#7) TimeStampReq will be applied. Only requests that have been electronically signed or sealed (CMS SignedData) shall be accepted. The request must contain a single electronic signature or electronic seal. The request must contain a certificate of the subscriber making a request for generation of a time stamp. The request may not contain other certificates. The request may not contain CRL list. The request's size may not exceed the maximum set to be 32000B.

```
TimeStampReqToken ::= ContentInfo
   -- contentType is id-signedData ([CMS])
   -- content is SignedData ([CMS])
```

SignedData will contain an electronic signature in accordance with CMS (PKCS#7) TimeStampReq.

```
SignedData ::= SEQUENCE {
   version CMSVersion,
   digestAlgorithms DigestAlgorithmIdentifiers,
   encapContentInfo EncapsulatedContentInfo,
   certificates [0] IMPLICIT CertificateSet OPTIONAL,
   crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
   signerInfos SignerInfos }
```

```
TimeStampReq ::= SEQUENCE  {
  version                INTEGER  { v1(1) },
  messageImprint          MessageImprint,
    --a hash algorithm OID = SHA-1 hash

  reqPolicy              TSAPolicyId              OPTIONAL,
  nonce                  INTEGER                  REQUIRED,
  certReq                BOOLEAN                  DEFAULT FALSE,
  extensions              [0] IMPLICIT Extensions    OPTIONAL  }

MessageImprint ::= SEQUENCE  {
  hashAlgorithm              AlgorithmIdentifier,
  hashedMessage               OCTET STRING  }
```

-- file hash must be done with the use of the SHA-256, SHA-384 or SHA- 512 algorithm (hashAlgorithm)

```
TSAPolicyId ::= OBJECT IDENTIFIER
```

The request may not contain the Policy identifier, however, if it does, it must be the KIR Policy identifier. Requests containing other identifier of the policy shall be rejected.

7.4.2. Time stamp format

The syntax of a time stamp response shall be compliant with the TSP protocol defined in [RFC 3161] and [ETSI EN 319 422 101 861] and shall have the following profile:

```
TimeStampResp ::= SEQUENCE  {
status                  PKIStatusInfo,
timeStampToken          TimeStampToken     OPTIONAL  }
```

If the status field shows an error preventing generation of an electronic time stamp, the timeStampToken is not present.

```
PKIStatusInfo ::= SEQUENCE {
   status        PKIStatus,
   statusString  PKIFreeText     OPTIONAL,
   failInfo      PKIFailureInfo  OPTIONAL  }

PKIStatus ::= INTEGER {
   granted              (0),
   -- when the PKIStatus contains the value zero a TimeStampToken, as
     requested, is present.
   grantedWithMods       (1),
    -- when the PKIStatus contains the value one a TimeStampToken, with modifications, is present.
   rejection             (2),
   waiting               (3),
   revocationWarning     (4),
    -- this message contains a warning that a revocation is
    -- imminent
   revocationNotification (5)
    -- notification that a revocation has occurred   }

   -- When the TimeStampToken is not present
   -- failInfo indicates the reason why the
   -- time-stamp request was rejected and
   -- may be one of the following values.

PKIFailureInfo ::= BIT STRING {
   badAlg             (0),
     -- unrecognized or unsupported Algorithm Identifier
   badRequest          (2),
     -- transaction not permitted or supported
   badDataFormat       (5),
     -- the data submitted has the wrong format
   timeNotAvailable    (14),
     -- the TSA's time source is not available
   unacceptedPolicy    (15),
     -- the requested TSA policy is not supported by the TSA.
   unacceptedExtension (16),
     -- the requested extension is not supported by the TSA.
   addInfoNotAvailable (17)
     -- the additional information requested could not be understood
     -- or is not available
   systemFailure       (25)
     -- the request cannot be handled due to system failure  }

TimeStampToken ::= ContentInfo
    -- contentType is id-signedData ([CMS])
    -- content is SignedData ([CMS])

SignedData ::= SEQUENCE {
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos SignerInfos }
```

If the certReq field in the request has had the TRUE value, the ‘certificates’ field shall contain a certificate of an entity providing the service and the ‘Time Attribute Certificate’.

```
id-ct-TSTInfo  OBJECT IDENTIFIER ::= { iso(1) member-body(2)
  us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}

TSTInfo ::= SEQUENCE  {
  version                INTEGER  { v1(1) },
  policy                 TSAPolicyId,
  messageImprint         MessageImprint,
    -- MUST have the same value as the similar field in
    -- TimeStampReq
  serialNumber           INTEGER,
   -- Time-Stamping users MUST be ready to accommodate integers
   -- up to 160 bits.
  genTime                GeneralizedTime,
  accuracy               Accuracy              OPTIONAL,
  ordering               BOOLEAN           DEFAULT FALSE,
  nonce                  INTEGER               OPTIONAL,
    -- MUST be present if the similar field was present
    -- in TimeStampReq.  In that case it MUST have the same value.
  tsa                    [0] GeneralName       OPTIONAL,
  extensions             [1] IMPLICIT Extensions   OPTIONAL  }
```

The only extension in TSTInfo object is qcStatements.

```
id-etsi-tsts OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0)
id-tst-profile(19422) 1 }
id-etsi-tsts-EuQCompliance OBJECT IDENTIFIER ::= { id-etsi-tsts 1 }
-- statements
esi4-qtstStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-tsts-EuQCompliance }
-- By inclusion of this statement the issuer claims that this
-- time-stamp token is issued as a qualified electronic time-stamp according to
-- the REGULATION (EU) No 910/2014.
```

When issuing an time stamp KIR shall append the data included in the electronic time stamp issuance request, the service execution time. Data prepared in such way shall be sealed with advanced electronic seal. The advanced electronic seal attached by KIR below the electronic time stamp shall be generated with the use of an RSA algorithm and SHA-512 hash function.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

KIR is subject to the supervision of the minister responsible for digitalization acting as supervisory body. KIR is subject to audit by a conformity assessment body with the frequency given in eIDAS Regulation. The purpose of the audit shall be to confirm that services provided by KIR fulfils the requirements laid down in eIDAS Regulation. As the result of audit is conformity assessment report which KIR submits to the supervisory body.

Supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment.

In case on non-compliance, supervisory body requires to remedy any failure within a given time limit.

Internal audit is performed to check the compliance of actual actions and activities undertaken by KIR with the procedures and processes described in the documentation of the certification authority.

8.1. Issues covered by the audit

Issues covered by the audit include:

1) control mechanisms concerning the management of the key life cycle;
2) control mechanisms concerning the certificate life cycle;
3) information security management;
4) management of resources and their classification;
5) staff security;
6) physical and environmental security;
7) management of operational tasks and system access;
8) system development and maintenance;
9) business continuity management;
10) monitoring and ensuring compliance with the procedures;
11) logging/ registration of events.

8.2. Frequency and circumstances of the assessment

External audits are carried out in the periods required by the eIDAS Regulation.

Internal audits are carried out according to the plan adopted at KIR for audits covering the trust services.

8.3. Identity/ qualifications of the auditor

External audits are carried out by a company licensed to carry out such compliance audits.

Internal audits are carried out by persons with appropriate experience in carrying out audits.

8.4. Relation between the auditor and the audited unit

The company that performs external compliance audits must be independent from KIR.

Persons conducting internal audits are not directly involved in the provision of trust services.

8.5. Actions undertaken to remove defects detected during the audit

Any information about defects detected during the audit is forwarded to persons managing the certification authority of KIR or the security inspector. Such persons immediately undertake actions aimed at removing defects.

8.6. Information about audit results

Information about audit results in the form of audit report or summary of such report is made available only internally.

9. OTHER BUSINESS AND LEGAL ISSUES

9.1. Fees

Fees for the provision of trust services are set in the price list of trust services published at the KIR website: www.elektronicznypodpis.pl, in the Agreement, the offer or another document containing price proposals.

9.1.1. Fees for certificate issuance and renewal

KIR charges fees for certificate issuance and renewal. Depending on the certificate type, the amount of such fees is set forth in the price list of trust services, the Agreement, the offer or another document containing price proposals.

9.1.2. Fees for access to certificates

KIR does not charge fees for access to certificates. KIR shall not charge fees for access to certificates. KIR shall not make certificates available to third parties.

9.1.3. Fees for revocation or information about certificate status

KIR does not charge fees for revoking a certificate, downloading CRLs and using the OCSP service.

9.1.4. 9.1.4 Fees of issuance of a time stamp

KIR shall collect fees for the issuance of a time stamp. Depending on the type of the settlement model selected by the ordering party the amount of such fees shall be defined in the price list of trust services, the agreement, the offer, or another document containing price proposals.

9.1.5. Fees for other services

As regards the provision of trust services, KIR may also charge other fees, provided they are entered to the price list of trust services. These may, for example, be fees for:

1) training and consultations;

2) cards;

3) readers;

4) software licenses;

5) usage of signature or seal creation data managed by KIR on behalf of subscriber.

9.1.6. Reimbursement of fees

The reimbursement of fees is permitted under regulations of the Polish law in the event of non-performance or improper performance of the Agreement by KIR.

9.2. Financial liability

KIR is liable for the damage related to services that are governed by the CP.

The principles of liability are determined by the eIDAS Regulation and the Act on Trust Services.

The injured party should file a claim for damage within 30 days from its occurrence. In the event of filing a claim for damage at a later date, KIR may refuse to review such claim.

KIR undertakes to pay compensation if it confirms that the damage has been caused by the operations of KIR and is included in the scope of liability of KIR. The amount of paid compensation shall not be higher than the amount of damage that has been demonstrated and recognized, and cannot exceed the amounts specified in point 9.8.

9.2.1. Financial liability

Damage is paid for in cash or satisfied otherwise, particularly by means of restitution, e.g. issuance of a new certificate, time-stamp, card or reader.

9.2.2. Other assets

KIR has sufficient financial resources necessary to conduct its operations and meet its obligations.

9.2.3. Extended scope of warranty

The CP does not provide for any requirements in this respect.

9.3. Business information confidentiality

Agreements, personal data, any information related to the provision of trust services and obtained in the course of their provision are confidential. They are respectively protected under the provisions of:

1) Act of 16 April 1993 on Combating Unfair Competition (Dz. U. [Journal of Laws] of 2018, No. item 419) to the extent applicable to company secrets, and

2) the RODO.

9.3.1. Scope of confidential information

The following information held by KIR is subject to protection:

1) internal procedures concerning the provision of trust services;

2) private keys of KIR infrastructure used to provide trust services;

3) passwords for suspending and revoking certificates;

4) archives, logs of operations of the ICT system used for the provision of trust services;

5) data of subscribers or other entities related to issuing, revoking and suspending certificates,

6) signature creation data managed by KIR on behalf of subscriber;

7) seal creation data managed by KIR on behalf of subscriber.

9.3.2. Information that is not confidential information

Non-confidential information is all information that has not been marked as confidential by the subscribers, relying parties or KIR.

Data entered in the certificate is deemed as not subject to confidentiality.

9.3.3. Responsibility for the protection of confidential information

KIR is responsible for the protection of entrusted confidential information.

9.4. Personal data protection

Personal data of subscribers and persons authorised by the principals that has been provided to KIR are subject to protection in line with the RODO.

Personal data is processed at KIR pursuant to the principles set forth in the RODO.

9.4.1. Privacy rules

Protection of privacy of the subscribers and persons authorised by the principals is of special importance to KIR.

Personal data of the subscribers are processed at KIR upon their consent and only for the purposes and to the extent necessary for the provision of trust services.

Personal data of persons authorised by the principals are processed only for the purposes and to the extent necessary for the performance of the agreement for the provision of trust services.

Personal data of the subscribers are processed for the purposes of promoting KIR services on the basis of a separate consent granted by the subscribers. The subscribers are informed about the voluntary nature of such consent and the possibility of withdrawing it.

Every person has the right to access the contents of their personal data processed by KIR.

9.4.2. Information considered as private

KIR treats personal data as private information.

9.4.3. Information not considered as private

Information other than information indicated in point 9.4.2 is not considered as private.

9.4.4. Responsibility for the protection of private information

Krajowa Izba Rozliczeniowa S.A. 02-781 Warszawa, ul. rtm. W. Pileckiego 65, is the controller of the subscriber's personal data within the meaning of the RODO and is responsible for the protection of personal data.

9.4.5. Reservations and permit to use private information

Pursuant to the requirements of the RODO, KIR may entrust personal data processing to a third party.

9.4.6. Disclosure of information in compliance with court or administrative order

Pursuant to the requirements of the RODO, KIR is obliged to provide access to personal data to entities that may submit such requests on the basis of mandatory provisions of the law.

9.4.7. Other circumstances of information disclosure

This CP does not provide for other circumstances of information disclosure.

9.5. Protection of intellectual property

Copyrights to this document belong to Krajowa Izba Rozliczeniowa S.A. It may be used solely for the purposes of using certificates. Any other uses, including the use of the entire document or its part, require written consent of KIR, where KIR expresses its consent to copying and publishing this document in its entirety.

The principal is fully responsible for the data provided by it and included in the certificate. KIR does not verify data provided by the subscribers in terms of its subject-matter, also in the aspect of the use of registered trademarks.

9.6. Representations and warranties

9.6.1. Obligations and warranties of KIR with respect to issuing certificates

KIR undertakes to:

1) issue certificates in response to certificate orders correctly submitted to KIR;
2) reliably verify the identity of subscribers, at the time of delivery of the carrier with a private key or certificate at the latest;
3) reliably generate pairs of keys for the subscribers;
4) reliably verify the requests for the issuance of certificates, if they are not generated by KIR;
5) reliably verify the identity of persons requesting the revocation or suspension of a certificate and their rights to request the suspension or revocation of the certificate;
6) revoke and suspend certificates in response to the properly submitted requests;
7) make information about suspended and revoked certificates available at the website;
8) protect processed data about the subscribers;
9) protect its private keys used for the generation of certificates and lists of suspended and revoked certificates in accordance with the CP;
10) comply with the rules settled down in section 2.4. Annex II eIDAS Regulation;
11) perform other obligations provided for under the law;
12) register and verify reports concerning the reliability of certificates issued by it and submitted by the subscribers, the principals or the relying parties.

Additional obligations of KIR may be provided for in the Agreement.

KIR is responsible for storing and archiving of data related to the issuance, suspension and revocation of a given certificate.

KIR is responsible for the security of private keys used in the process of issuing, suspending and revoking certificates.

The Agreement may specify a more detailed scope of KIR's responsibility.

9.6.2. Obligations and warranties of the registration point

Since all registration points are organizational units of KIR, they do not provide any additional warranties and are not burdened with any additional obligations.

9.6.3. Obligations and warranties of the subscriber

With regard to the electronic seal data managed by KIR on behalf of subscribers, the person authorized to use the electronic seal data is only the subscriber acting through users designated by him/her. The granting and revoking of authorizations to users is carried out by the subscriber or another user only using the mechanism provided in the mobile application provided by KIR.

Other obligations and guarantees of the subscriber have already been described above.

If the subscriber individually generates keys, it shall be held liable for the quality of keys and for providing them with proper protection at the stage of their generation and use.

9.6.4. Obligations and warranties of the relying party

All obligations and warranties of the relying parties have already been described hereinabove.

9.6.5. Obligations and warranties of other entities

All obligations and warranties of other entities have already been described hereinabove.

9.6.6. Liabilities and guarantees of KIR with respect to the services of issuing time stamps

KIR undertakes to:

1) provide a service of issuance of time stamps in compliance with the requirements of the eIDAS Regulation and the Act on Trust Services;
2) apply organisational and operating procedures preventing tampering with time used for the provision of a service of issuance of a qualified electronic time stamp;
3) use for the time stamp service the electronic seal creation data generated for this service only;
4) protect its private keys used for the issuance of time stamps in compliance with this Policy;
5) protect, in compliance with the RODO, personal data of the subscribers provided by the ordering party under an agreement;
6) verify the correctness of requests for the issuance of time stamps delivered to KIR,
7) issue time stamps in response to correct verification of the request of issuance of time stamps delivered to KIR.

The subscriber and other third party entities shall bear the risk related to damage resulting from undertaking actions, despite a negative or not completely verified or invalid time stamp, and also in the event whereby they neglect verification of the status or completeness of the time stamp.

Detailed obligations of KIR may be defined in an agreement.

9.6.7. Liabilities and guarantees of KIR with respect to the services of creation of electronic signatures

In scope of signature creation data managed by KIR on behalf of subscribers, KIR undertakes to:

1) provide a service of creating electronic signatures in compliance with the requirements of the eIDAS Regulation and the Act on Trust Services;
2) apply organizational and operational procedures preventing access to signature creation data managed by KIR on behalf of subscriber exclusively to subscriber;
3) protect signature creation data managed by KIR on behalf of subscriber in compliance with this Policy;
4) protect personal data of subscribers transferred by the principal under the Agreement;
5) access for the subscriber to signature creation only after positive verification of the identity of the subscriber.

KIR shall be responsible for the signature process from the moment when the hash function value for the signed document along with the data confirming the subscriber's right to access to signature creation data are delivered to KIR.

Detailed obligations of KIR may be defined in the agreement.

9.6.8. KIR's obligations and guarantees with respect to the management of electronic seal data

With respect to the electronic seal creation data managed by KIR on behalf of subscribers, KIR undertakes to:

1) provide the service of creating electronic seals in accordance with the requirements of the eIDAS Regulation and the Law on Trust Services;
2) apply organizational and operational procedures that ensure access to electronic seal creation data managed by KIR on behalf of the subscriber only to subscribers or designated users;
3) protection of the data for electronic seal submission, managed on behalf of subscribers, in accordance with this Policy;
4) protect personal data of subscribers provided by the ordering party under the Agreement;
5) provide electronic seal submission data to the subscriber only after positive verification of the identity of the subscriber or designated user.

KIR shall be responsible for the process of electronic seal submission from the moment the value of the hash function for document sealing is provided to KIR along with data confirming the subscriber's or designated user's authorization to access electronic seal submission data managed by KIR on behalf of subscribers.

KIR's detailed obligations may be specified in the Agreement.

9.7. Exclusions from liability under the warranty

KIR is not liable for damage resultant from the use of certificates outside the scope defined in the CP that has been indicated in the certificate, including particularly damage resulting from exceeding the maximum limit value of transaction, if such value has been disclosed in the certificate.

KIR is not liable for damage resultant from untrue data included in the certificate, whose verification has been based on their statements, or entered in accordance with the submitted documents that have been forged or presented untrue or non-valid data.

KIR is not liable for damage resultant from non-validity of data entered to the certificate if, at the time of certificate issuance, it has been true.

KIR shall not be liable for damage arising from the use of the certificate if the keys relating to the public key included in the certificate have not been generated by KIR.

KIR grants no warranties to the users of software or hardware in which certificates of the KIR certification authorities have been placed on the basis of license referred to in point 9.5, and is not liable for damage resultant from the use of such software.

9.8. Limitations of liability

KIR shall be liable for the request of issuance of time stamps, containing document’s hash function, since the moment of delivery to KIR’s systems.

KIR shall be responsible for signature and seal generation from the moment of delivery to KIR a hash value with the data enabling the authorisation to signature and seal creation data if KIR manages signature or seal creation data on behalf of subscriber.

KIR shall be responsible for the signature generation from the moment when the hash function value for the signed document along with the data confirming the subscriber's right to access to signature creation data are delivered to KIR.

KIR shall be subject to mandatory third party liability insurance for damage caused to recipients of trust services arising during the period of provision of trust services.

The sum guaranteed of third party liability insurance (OC) with respect to a single event the consequences of which are covered by the third party insurance agreement (OC) shall be a PLN equivalent of EUR 250,000, however, not more than EUR 1,000,000 with respect to all events. The KIR's liability for damages does not cover lost benefits and is limited to the actual damage.

KIR may limit liability in relation to a given certificate by specifying in the certificate a maximum transaction limit that can be confirmed using a given certificate. In the agreement with the principal, KIR may set a maximum liability limit.

The principles of KIR's liability are determined by the eIDAS Regulation and the Act on Trust Services.

9.9. Compensation

Compensation is payable on the basis of a recognized complaint, settlement, including court settlement, or judgement of a common court.

9.10. Term of the document and its expiry

9.10.1. Term

This document shall be effective from the moment it has been assigned the status of effective and published at the KIR websites to the moment of publication of the next effective version.

9.10.2. Expiry

Another published version of the CP includes its effective date which, at the same time, is the expiry date for the present CP. Thus, the previous CP loses its status of being effective.

9.10.3. Effects of document expiry

After the expiry of this CP, the users of certificates issued by KIR during its term should follow its provisions until the expiry of validity of the certificate.

9.11. Individual notices and communication with users

For the purposes of communication between KIR and the users, means of communication are used that are commonly available and generally accepted at a given moment. The parties may define special additional methods of communication in the agreement.

Some types of messages exchanged between KIR and the users necessitate the use of strictly defined methods of communication, e.g. specific network protocols.

Information such as CRLs and current certificates of the authorities is made available for all interested parties in a continuous manner. Any information about violations of the private key of any of the authorities covered by this document is immediately made available to all interested parties.

9.12. Introduction of amendments to the document

A review of the applicable Policy shall be performed once a year. The review shall be carried out by a team appointed for that purpose. Compliance of the Policy with the procedures implemented at KIR and the applicable law shall be analysed during the review.

9.12.1. Procedure for amendment introduction

Amendments to the CP may be introduced as needed, particularly as a result of detecting errors or need to introduce updates. Amendments may also result from suggestions submitted by interested persons.

Proposals of amendments may be submitted via internal mail of KIR by authorised KIR employees, as well as by other interested persons via electronic mail to the contact addresses of KIR or via regular mail.

Interested persons who may submit proposals of amendments to be introduced to the CP are:

1) auditors;
2) principals;

3) subscribers;

4) KIR employees, particularly the security inspector;

5) other entities, especially in the event of detecting conflicts between the provisions of the CP and the provisions of the applicable law.

After the introduction of amendments, the document is updated, and its publication date and version number are changed. Each time, the amendments must be approved by the Management Board of KIR.

9.12.2. Mechanisms and dates of notifying about amendments and waiting for comments

Prior to the introduction of material amendments, all interested parties are informed about them by being sent information about planned amendments or placing such information at the KIR website.

The interested parties may send comments to the amendments within 10 business days from their sending or publication. Amendments arising from comments, if relevant, must be published again and subjected to the above procedure for notifying interested parties.

In other cases, a new version of the CP, with amendments, is subject to the procedure of approval at KIR until it receives the “effective” status.

Amendments submitted by interested parties may be accepted in their entirety, accepted with adjustments or rejected after the lapse of deadline for submitting responses to the next version of the document.

Amendments that do not require the notification of interested parties and may be introduced without notification are:

1) editorial changes;

2) changes that do not materially affect a large group of users.

Such amendments are not subject to the procedure for amendment introduction.

9.12.3. Circumstances that require a change of identifier

A change of identifier (OID) indicated in 1.2 may take place in the event of change of entity managing the certification authority or time-stampin authority.

9.13. Procedures for dispute resolution

If a dispute is not settled under the procedure for complaint review, it shall be subjected to resolution by a common court of competent and subject-matter jurisdiction in Poland.

9.14. Governing law and jurisdiction

Polish law is the governing law, and disputes are resolved by a common court of competent and subject-matter jurisdiction in Poland.

9.15. Compliance with applicable law

KIR runs all of its operations in compliance with and pursuant to the law applicable in Poland.

9.16. Miscellaneous provisions

The CP does not provide for any requirements in this respect.

9.16.1. Completeness of the provisions of the agreement

The parties are bound by the provisions of the Agreement and the CP.

9.16.2. Assignment of rights

No third party may assume the rights and obligations of a party to the Agreement without the other party's consent.

If the operations consisting in the provision of services covered by this CP have been discontinued, KIR may transfer the rights to use the private key, and issue and publish the CRL to another entity without the consent of the principal, the subscriber or the relying party, however, after informing the supervisory authority of the change.

9.16.3. Severability of provisions

In case of doubts or discrepancies between the provisions of the agreement and the CP that cannot be removed, the agreement prevails over the CP.

If the provisions of any of the above-mentioned documents do not comply with the law resulting in their invalidity, the non-defective provisions included in other documents remain in force.

9.16.4. Enforceability clause

Temporary non-execution of the rights of KIR, as well as failure to use them against one or more of the principals or subscribers, may not be construed as a waiver or permanent withdrawal from their use, and does not affect the contents and interpretation of the CP.

9.16.5. Force Majeure

The circumstances of force majeure are understood as any extraordinary events that are external and impossible to predict, such as disasters, fires, floods, explosions, social unrest, military operations, acts of state authorities, power supply failure or ICT connection failure, which, in part or in whole, prevent the satisfaction of obligations included in the Agreement or the CP, or hinder the performance of such obligations in accordance with the terms and conditions specified therein.

KIR shall not be liable for any violation of its obligations if this is caused by a force majeure event.

9.17. Other provisions

The CP does not specify any other provisions.