Krajowa Izba Rozliczeniowa S.A.

CERTIFICATION PRACTICE STATEMENT OF KIR for TRUSTED NON-QUALIFIED CERTIFICATES

Version 1.18

Document history

Version number	Status	Date of issue
1.0	Document approved by the Management Board of KIR – version effective until 22 March 2012	19 December 2011
1.1	Document approved by the Management Board of KIR – version effective until 30 September 2012	22 March 2012
1.2	Document approved by the Management Board of KIR – version effective until 9 October 2013	1 October 2012
1.3	Document approved by the Management Board of KIR – version effective until 24 April 2014	10 October 2013
1.4	Document approved by the Management Board of KIR – version effective as from 25 April 2014 until 19 November 2014	18 April 2014
1.5	Document approved by the Management Board of KIR – version effective as from 20 November 2014 until 1 March 2015	13 November 2014
1.6	Document approved by the Management Board of KIR – version effective as from 2 March 2015 until 10 July 2016	26 February 2015
1.7	Document approved by the Management Board of KIR – version effective as from 11 July 2016 unlit 13 July 2017	30 June 2016
1.8	Document approved by the Management Board of KIR – version effective as from 14 July 2017 until 6 May 2018	10 July 2017
1.9	Document approved by the Management Board of KIR – version effective as from 7 May 2018 until 24 January 2019	12 April 2018
1.10	Document approved by the Management Board of KIR – version effective as from 24 January 2019 until 30 March 2020	22 January 2019

1.11	Document approved by the Management Board of KIR – version effective as from 30 March 2020 until 31 August 2020	30 March 2020
1.12	Document approved by the Management Board of KIR – version effective as from 1 September 2020 until 17 September 2020	26 August 2020
1.13	Document approved by the Management Board of KIR – version effective as from 18 September 2020 until 30 April 2021	17 September 2020
1.14	Document approved by the Management Board of KIR – version effective as from 1 May 2021 until 30 June 2021	30 April 2021
1.15	Document approved by the Management Board of KIR – version effective as from 1 July 2021 until 20 January 2022	23 June 2021
1.16	Document approved by the Management Board of KIR – version effective as from 21 January 2022 until 6 April 2023	13 January 2022
1.17	Document approved by the Management Board of KIR – version effective as from 6 April 2023 until 19 October 2023	5 April 2023
1.18	Document approved by the Management Board of KIR – version effective as from 20 October 2023	20 October 2023

LIST OF CONTENTS

1. FOREWORD

The “Certification Practice Statement of KIR for Trusted Non-Qualified Certificates”, hereinafter referred to as the “CPS” sets forth detailed solutions, including technical and organisational, that indicate the manner, the scope, and the terms and conditions for creating and applying certificates. The CPS also defines parties that participate in the process of provision of trust services, recipients of services, and entities that use certificates, their rights and obligations.

The CPS shall be used for issuing and managing trusted non-qualified certificates issued by Krajowa Izba Rozliczeniowa, hereinafter referred to as “KIR”, under the Szafir Electronic Signature Support Centre.

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

The general rules of procedure applied by KIR for provisions of trust services have been described in the “Policy of KIR for Trusted Non-Qualified Certificates” hereinafter referred to as the “Policy”. Details concerning implementation of the rules described in the Policy have been presented in this CPS.

1.1. Introduction

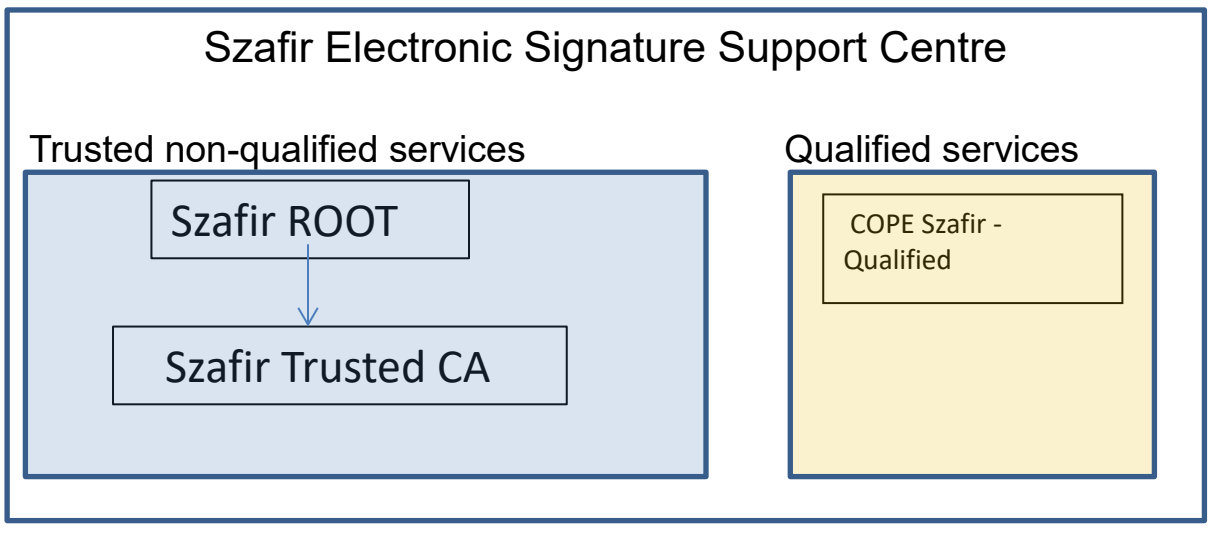
Trusted non-qualified certificates are issued by the Szafir Electronic Signature Support Centre. Provision of such services is performed in compliance with WebTrust requirements (www.webtrust.org). The CPS defines the rules of their provisions, actions that are performed by certification authorities, registration authorities, and subscribers and trusted parties. Issuance of trusted non-qualified certificates, hereinafter referred to as the "certificates" shall be done irrespective of provision of qualified trust services.

Certificates issued by KIR are compliant with the X.509 v3 standard and the following documents:

- the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at www.cabforum.org reffered to as “Baseline Requirements”.
- Network and Certificate System Security Requirements published at www.cabforum.org.

In the event of any discrepancies between the CPS and the Baseline Requirements, said document shall prevail over the CPS.

Diagram



…to be supplemented

1.2. Document Name and Its Identification

The CPS has the following distinguished identifier (OID: 1.2.616.1.113571.1.2.1.1):

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

The current and the previous versions of the CPS are available at the web site www.elektronicznypodpis.pl.

1.3. Participants of the PKI Infrastructure Described in the CPS

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

1) the root certification authority – Szafir Root and Szafir Root CA2;
2) the operational certification authority – Szafir Trusted CA a sub CA under Szafir Root oraz Szafir Trusted CA 2 and Szafir Trusted CA3 a sub CA under Szafir Root CA2 ;
3) registration authorities;
4) contracting authorities;
5) subscribers;
6) trusted parties.

1.3.1. Certification Authorities

Root Certification Authority

The root certification authority – Szafir Root and Szafir Root CA2 – are the certification authorities that issues certificates for itself (the so-called self-signed certificate) and certifies the sub CAs..

Operational Certification Authority

The Szafir Trusted CA issues certificates for subscribers and provides information necessary for verifying certificates issued by it. CA does not generate certificates as of 2019.

Trusted CA2 and Sapphire Trusted CA3 certification authority issue certificates for subscribers and provide the information necessary to verify the validity of the certificates they issue. Tasks related to accepting requests for issuing/suspending or revoking certificates, and issuing certificates are carried out by registration points.

1.3.2. Registration authorities

Registration authorities shall carry out tasks relating to support of contracting authorities and subscribers. Their tasks, among others, include:

1) execution of agreements with contracting authorities;
2) verification of identity of subscribers and their rights to receive certificates;

3) provision of certificates to subscribers;

4) acceptance and implementation of requests for suspension, revocation, or change in the certificate status following suspension.

Only registration authority of KIR shall perform tasks of registration points. No other entities are authorised to validate domains on behalf of KIR.

A list of units carrying out tasks of registration authorities together with their office hours is available at the web site of www.elektronicznypodpis.pl.

1.3.3. Subscribers

A subscriber can be a natural person, a legal person, or an organisational unit without corporate existence whose data has been or is to be entered into the certificate.

In case of certificates issued to entities other than a natural person actions provided in the CPS for a subscriber, including confirmation of certificate reception, confirmation of having a private key, acceptance of the certificate contents, determining the PIN and PUK codes, or passwords for requesting revocation and suspension of the certificate shall be performed by a person authorised by the contracting authority . This person is also charged with obligations relating to protection of the private key.

1.3.4. Trusted Parties

A trusted person shall be understood to mean a natural person, a legal person, or an organisational unit without corporate existence that shall undertake actions or any decision trusting electronically signed or sealed data or the signature data with the use of a public key contained in the certificate issued by KIR or the issuer certificate of KIR.

A trusted party should pay attention to the type of a certificate and the policy pursuant to which it has been issued. In case of doubts whether a specific certificate has been issued correctly and whether it is used by an entity that is authorised to that, a trusted party shall be obliged to report doubts to KIR. Reporting may be done by telephone at the hotline number during its office hours or on a 24h basis by using a contact form available at www.elektronicznypodpis.pl .

1.3.5. Other Participants

The term of a contracting authority shall mean a natural person, a legal person, or an organisational unit without corporate existence that has concluded an agreement with KIR for provision of trust services consisting in issuance of certificates. Pursuant to an agreement the contracting authority may order certificates for individual subscribers.

1.4. Appropriate Uses of the Certificate

Certificates issued in accordance with the CPS shall be used to provide integrity, identity, confidentiality, and non-repudiation of sent data.

Certificates that have been issued in accordance with the CPS are not qualified certificates. A digital signature verified with the use of such certificates does not have legal consequences equalling those of a hand-affixed signature.

Certificates may contain data and be used to identify entities other than natural persons.

1.4.1. Types of Certificates and Recommended Areas of Use

No.	Certificate Type	Recommended Uses
1.	Standard Certificates	For protection of information sent electronically, using mainly e-mail, for authorising access to systems, customer authentication in TLS connections. It allows signing and encrypting data in an electronic form and authenticating subscribers.
2.	TLS Certificates	For confirming reliability of servers and confirming their authenticity. It allows setting up an TLS encrypted connection between servers that have such certificates, and also providing secured logging to customers. Certificates of that type may be issued only for servers that operate in public networks and have a non-ambiguous domain name defining location of a specific node in the DNS system (FQDN - Fully Qualified Domain Name). TLS certificates are issued in two variants: - DV (domain validated) – containing only a domain name, - OV (organization validated) – containing a domain name and additional data allowing the identification of the entity managing the domain.
3.	Test Certificates	For testing co-operation of the certificate with solutions used or developed by a contracting authority or a subscriber.
4.	Elixir Certificates	For protecting information sending within Elixir and EuroElixir systems. This kind of certificates are issued only for Participants of Elixir and EuroElixir systems.
5.	Server Certificates	For confirming identity of servers and network devices.

Test certificates may be issued for each type of certificates referred to in items 1 and 4 and 5 in the above table. Such certificates do not provide any guarantee about identification of the subscriber that uses such certificate.

TLS certificates are issued only by Szafir Trusted CA2. Other types of certificates are issued by Szafir Trusted CA2 and Szafir Trusted CA3.

All certificates issued under the CPS shall be used in compliance with their intended purposes and by entities that have been so authorised. Certificates should be used in applications that have been prepared for that and that satisfy at least the requirements specified below:

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 certificate validity periods;
5) proper manner of informing the user about the condition of the application, status of certificates, verification of electronic signatures or electronic seals.

1.4.2. Prohibited Areas of Use

Certificates issued pursuant to the CPS are not allowed to be used outside the stated areas of use. It is also prohibited to use certificates by unauthorised persons.

1.5. CPS Administration

The CPS shall be subject to changes relative to business and technological needs. The current version of the CPS shall be binding. The previous version of the CPS is effective until the next binding version has been published. Working versions shall not be published.

Work on amendments and updates of the CPS have been performed by an organisational unit of KIR S.A. that is responsible for the provision of trust services. An organisation that is responsible for managing the CPS:

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

1.5.1. Organization Administering the Document

Work on amendments and updates of the CPS have been performed by an organisational unit of KIR S.A. that is responsible for the provision of trust services. An organisation that is responsible for managing the CPS:

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

1.5.2. Contact Particulars

Any correspondence related to the provision of trust services shall be directed to the address of the registered seat of KIR:

Krajowa Izba Rozliczeniowa S.A.
Departament Kontaktu z Klientami [Customer Service Point]
ul. rtm. W. Pileckiego 65
02-781 Warszawa
with an annotation reading “certyfikaty” [certificates]
tel. 0-801 500 207
e-mail: kontakt@kir.pl

or to addresses of branches of KIR, if so agreed or the customer service procedure set forth by KIR so provides.

For each entity listed in section 4.9.2 KIR makes available the following website with instructions on how to report a suspected compromise of the private key, misuse of the certificate, other types of possible fraud, violations, and any issues related to certificates:

https://www.elektronicznypodpis.pl/informacje/jak-zawiesic-lub-uniewaznic-certyfikat/

1.5.3. Entities Defining Validity of the Rules Provided in the CPS

The update of the principles set forth herein and other documents concerning provision of trust services is the responsibility of an organisational unit of KIR that is responsible for the provision of trust services.

1.5.4. CPS Approval Procedures

The CPS shall be approved by the Management Board of KIR After approval it shall receive a status as effective with indication of its effective date. It is published on the websites of KIR on that date at the latest.

2. RESPONSIBILITY FOR PUBLICATION AND COLLECTING INFORMATION

2.1. Repository

Information concerning trust services provided by KIR, including information about the manner in which Agreements are concluded, orders for and renewals, suspension, and revocation of certificates are processed shall be made available to all interested parties at the website of KIR or in the branches of KIR at www.elektronicznypodpis.pl.

All certificates that have been issued by KIR shall be kept at KIR for the period of 20 years as from the beginning of the validity period of certificates. The TLS certificates are published also by https://www.certificate-transparency.org according to section 4.4.2.

2.2. Publication of Information in the Repository

Publication of information in the repository shall be made either automatically or following approval by authorised persons. Basic information that is published in the repository shall include:

1) certificate of the Szafir Root CA and Szafir Root CA2 certification authority;
2) certificates for sub CA by issued the Szafir Root CA and Szafir Root CA2 certification authority;

3) lists of suspended and revoked certificates (CRLs) issued by Szafir Root cA, Szafir Root CA2, Szafir Trusted CA, Szafir Trusted CA2 and Szafir Trusted CA3;

4) templates of agreements and orders if applicable for the given type of contract;

5) descriptions of procedures of obtaining, renewing, suspending and revoking certificates;

6) current and previous Polices and CPSs;

7) reports on audits carried out by authorised institutions;

8) additional information.

2.3. Frequency of Publication

The frequency of publishing individual documents and data has been presented in the table below:

1.	Certificates of certification centres	Each time and immediately after new certificates have been generated.
2.	CRLs	For Szafir Root and Szafir Root CA2 – not less seldom than once a year or after certificate suspension or revocation. For Szafir Trusted CA and Szafir Trusted CA2 – not less seldom than every 24 hours or after certificate suspension or revocation. Updates of lists shall be done within 1 hour from certificate suspension or revocation. The permitted period of delay in suspending or revoking a certificate may be 24 hours.
3.	Templates of agreements and orders	Each time when they are amended or updated.
4.	Descriptions of procedures of obtaining, renewing, suspending and revoking certificates	Each time after procedures have been amended or updated.
5.	Current and previous Polices and CPSs	At least once a year, pursuant to Chapters 9.10 to 9.12.
6.	Reports on audits carried out by authorised institutions	Each time after audit completion and reception of the report.
7.	Additional information	Each time it has been updated or changed.

2.4. Repository Access Control

All information published in the repository at the websites of KIR shall be available for all interested parties.

Information published in the repository is protected against unauthorised changing, adding, and removing and is stored with back-up copies.

In case of any actions undertaken by unauthorised entities or persons that could violate 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 procedures of identifying subscribers that request KIR to issue a certificate and 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, there is a distinguished name created in accordance with the scheme below that will allow identification of the subscriber linked to a public key included in the certificate.

Distinguished Names (DN) placed on certificates are consistent with X.500 and X.520 Recommendations. The distinguished name may contain the following components:

Meaning	Value
country name	Abbreviated country name
common name	Name identifying the subscriber, common name of the subscriber or network or mobile device. In case of TLS certificates it is an optional componentincluding domain name being one of the FQDN SANs
surname*	Subscriber's surname plus, possibly, their family name
first names*	Subscriber's first name
Organisation**	Name of the contracting authority on behalf of whom the subscriber acts, and in the case of Elixir certificate abbreviation running clearing system (KIR). With the exclusion of Elixir certificates, placing that element means a necessity of placing the “state” or “locality” element in the certificate, too. This field is required in case of TLS OV certificates.
organisational unit	Name of the organisational unit, and in the case of Elixir certificate clearing number
State**	Name of the state in the territory of which the subscriber lives or has its registered office
Locality**	Locality in which the subscriber lives or has its registered office
electronic mail address***	Subscriber's e-mail address
postal address**	Postal address

domain name	Name of the internet domain interested in the internet DNS system for which the certificate has been issued - only in the case of TLS certificates and test certificates for testing TLS connections

* - only in case of certificates for subscribers who are natural persons
**- excluding TLS certificates containing only a domain name (DV)
***-excluding TLS certificates

The subscriber's distinguished name is created on the basis of a subset of the above attributes, provided that the distinguished name must be not empty within specific technical infrastructure at KIR.

The common name field may contain any string of letters, figures, and spaces, having the maximum length of 64 characters, that unambiguously identifies the subscriber. It is allowed to include in the common name field names of Internet domains in case of certificates issued for the subscriber who is not a natural person.

The subscriber may have any number of certificates that contain the same distinguished name of the subscriber.

3.1.1. Necessity to Use Meaningful Names

The subscriber or contracting authority should indicate in the certificate order data for the subscriber's distinguished name allowing unambiguous identification of the certificate user. In particular, the subscriber's distinguished name for an TLS certificate should contain a Fully Qualified Domain Name (FQDN).

In the process of generating certificates, KIR shall examine whether for the subscriber's distinguished name indicated in the order a certificate has not been generated for another subscriber. In case distinguished names have been repeated, with the exception of issuing another certificate for the same subscriber, KIR may refuse issuance of a certificate and propose a change in the subscriber's distinguished name.

3.1.2. Ensuring Anonymity to Subscribers

KIR shall not issue certificates that ensure anonymity to subscribers. Irrespective of the contents of the certificate KIR shall continue to keep data identifying the subscriber and contracting authority.

3.1.3. Uniqueness of Names

The subscriber's distinguished name is indicated by the subscriber or contracting authority in the order. The distinguished name should comply with the requirements set forth above.

Each issued certificate has a unique serial number within a specific certification authority. Together with the subscriber's distinguished name this guarantees unambiguous identification of the certificate.

3.1.4. Recognition, Authentication, and the Role of Trade Marks

The subscriber's distinguished name defined by the contracting authority or the subscriber shall contain only names to which it is entitled. KIR has the right to notify the contracting authority or the subscriber to present documents confirming the right to use names recorded in the certificate order. Confirmation of the right to use a trade mark may particularly include:

- a document issued or provided by a state authority;
- information obtained from a reliable source;
- information obtained from a state authority responsible for registration of trade marks.

3.2. Initial Identity Validation

Prior to the issuance of the first certificate for a specific subscriber, the contracting authority shall execute an Agreement or submit to KIR an order containing data necessary for certificate preparation. An order for the certificate may also be submitted via a form available at the website of KIR.

KIR shall check data of the contracting authority and appointment of persons that have signed documents on its behalf on the basis of information obtained from lawful, reliable sources, including generally accessible registers maintained by public authorities.

For issuing TLS/SSL certificates KIR may use the ACME (Automatic Certificate Management Environment) protocol for validating, issuing, and managing certificates.

In the event it is not possible to confirm identification data of the contracting authority or if persons who have executed documents are not authorised to represent the contracting authority, the order and the agreement shall not be accepted by KIR and the order shall not be executed about which the contracting authority shall be informed.

If a certificate applies to a natural person and is to contain an additional identifier assigned by a state authority, e.g. tax identification number (NIP), then before a certificate is provided to a subscriber, it shall be necessary to present a document confirming assignment of such identifier.

Subscriber's identity can be confirmed:

1) based on the measure, electronic identification within the meaning of art. 3 point 2 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services in relation to electronic transactions in the internal market and repealing Directive 1999/93 / EC (OJ. UE. No. 257, p. 73) (eIDAS), which meets the requirements referred to in Art. 24 paragraph 1 lit. b eIDAS, for which compliance with the requirements set out in Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on establishing minimum technical specifications and procedures regarding levels of confidence in electronic identification means pursuant to art. 8 clause 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services in relation to electronic transactions in the internal market (Journal of Laws EU L of 2015 No. 235 p. 7, as amended) has been confirmed by the conformity assessment body referred to in Art. 21 paragraph 1 eIDAS;
2) a qualified certificate of an electronic signature containing the name and surname and PESEL number or the number and series of the document confirming identity;
3) verification of identity at the registration point;

4) on the basis of authentication data defined in 7.3.4. External Account Binding in RFC 8555 and communicated by KIR at the stage of placing an order for a certificate - in case of TLS/ SSL certificates issued on the basis of ACME protocol.

3.2.1. Method To Prove Possession of Private Key

A 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 a pair of keys is generated by KIR, a document confirming issuance of the certificate signed by the subscriber or a person authorised to collect the certificate shall be confirmation of provision of private key to the subscriber.

If the subscriber individually generates a pair of keys presentation of a file with a request to issue a certificate shall be required for certificate issuance. Such file shall contain a public key for which a certificate is to be generated, data of the subscriber and an electronic or digital signature generated with the use of a private key that makes up one pair with a public key. Proving possession of a public key is to establish that a public key that is to be placed in the certificate makes one pair with a private key possessed by the subscriber.

For TLS/SSL certificates issued using the ACME protocol, subscribers shall provide CSRs in the Finalize method in accordance with RFC 8555, Section 7.4.

KIR may request another proof of having the private key pursuant to the descriptions included in the specification RFC 4211.

3.2.2. Identification and Authentication of Entities Other Than Natural Person

If a certificate is to contain data on a contracting authority other than a natural person, such as a name of the organisation and its address, KIR prior to issuance of a certificate, on the basis of information obtained from legal and reliable, publicly available sources, including available registers maintained by public authorities, shall check if such entity exists if data indicated by a contracting authority is compliant with that presented in the register used and if persons acting on behalf of the contracting authority are authorised to that. Such sources are defined by KIR as trusted An address of the organisation may also be verified during a visit authorized by KIR natural person, who registers subscribers and/ or applications for the issuance, suspension and revocation of certificates, hereinafter referred to as the Operator of KIR at the registered seat of a contracting authority.

A list of trusted sources used by KIR to verify data is available at https://www.elektronicznypodpis.pl/informacje/zaufane_zrodla_informacji/. KIR shall verify the list of trusted sources at least once a year.

If a certificate is to provide for security of electronic mail, verification of the electronic mail address shall be done. Verification shall consist in checking if an electronic mail address indicated in the and to be included in the certificate belongs to the subscriber. Checking shall be done by confirming that the subscriber has collected unique, secret authentication data sent to an electronic mail address given in the order. Checking is to determine that the e-mail address is legally used by the subscriber.

The subscriber has 3 hours to confirm receipt of the credentials.

Domain names can be included only in TLS certificates and test certificates to test TLS connections. Checking the domain name shall include the verification if a contracting authority has the right to use the domain name and if the domain remains under its control. Verification is preceded by checking in publicly available WHOIS services or directly with entities registering domains, if such information is available, if a contracting authority is registered as a domain owner or has the right to use the domain name during the period of ordering the certificate. Verification of domain control performed by KIR shall comprise:

- 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. The file with random data has to be accessible by KIR via HTTP or HTTPS over an Authorized Port. The HTTP response code indicates that the request was successfully processed (class 2xx response code received).Random data in file is unique for every certificate request, does not appear in the request and data is not older than 30 days. Verification shall be conducted in accordance with requirements described in Section 3.2.2.4.18 of the Baseline Requirements;
- 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 are unique for each validation and they are not older than 30 days, and CAA record checked not earlier than 8 hours before certificate generation. Verification shall be conducted in accordance with requirements described in Section 3.2.2.4.7 of the Baseline Requirements;
- the second alternative way of checking control of over the requested Domain Name is validation using the ACME HTTP Challenge method. The data contained in the Authorization Token (as defined in RFC 8555) are not older than 30 days from its creation. Verification shall be conducted in accordance with requirements described in Section 3.2.2.4.19 of the Baseline Requirements;
- 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. Verification shall be conducted in accordance with the Baseline Requirements described in Section 3.2.2.4.6 and 3.2.2.4.7;
- 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. Verification shall be conducted in accordance with RFC 8659 and requirements mentioned in Baseline Requirements described in Section 3.2.2.8. This check is performed by the dedicated tool by querying a CAA record.

To minimise the risk of using inappropriate data KIR shall use data presented in the WHOIS service in combination with IANA data and the WHOIS data supplied by ICCAN approved entities that register domains.

If the identifier of the subscriber's certificate containing the domain name is to include a name of the country, too, then prior to issuing the certificate KIR shall verify if the indicated name of the country is connected to the subscriber. Verification shall be performed in accordance with one of the methods described below and consists in checking:

- if a domain IP address indicated in DNS is within the range of IP addresses assigned for a country for entering of which into the subscriber's identifier the contracting authority has applied
- f the name of the country included in the information provided by an authority registering the domain whose name is to be placed in the certificate is compliant with the name of the country for entering of which into the subscriber's identifier the contracting authority has applied.

While verifying the name of the country KIR S.A shall check, if the contracting authority does not use a proxy server to substitute an IP address from another country in which it is actually located.

A positive result of domain validation process can be used for certificate issuance within 12 months since the end of validation process.

3.2.3. Identification and Authentication of Natural Persons

Identification and authentication of a natural person is performed when data of such person – upon request of the subscriber or contracting authority contracting authority – is to be included in the certificate. Additionally, identification and authentication of a natural person is done when a specific natural person is indicated a subscriber by the contracting authority contracting authority . Identification is to confirm that an indicated person actually exists and that it is a person whose data has been indicated in an order or an agreement. If data concerning the organisation is to be placed in the certificate together with data of a natural person, then checking shall also comprise verification if an indicated person is unauthorised to act on behalf of such organisation. Checking shall consist in verifying a statement executed by persons authorised to represent a specific organisation.

If an electronic mail address is to be put into a certificate for a natural person, then checking the address given in the order shall be done in a manner similar to that in Clause 3.2.2.

If a natural person applies for issuance of an TLS certificate, including a test certificate containing the domain name, checking the right to own the domain is done as described in Clause 3.2.2. In addition, verification comprises the steps described in Clause 3.2.

3.2.4. Subscriber's Data Not Subject to Verification

KIR shall verify all information included in the distinguished name of the issued certificate.

3.2.5. Checking Rights to Receive Certificate

Before issuing a certificate to the subscriber or a person authorised to receive the certificate, KIR shall check:

- identify of such person on the basis of an identification document presented by it, and in case of a test certificate on the basis of supplied data, such as the first name, the surname, and the number and series of the identification document and in the case of TLS/SSL certificates issued on the basis of the ACME protocol - on the basis of authorization data used under this protocol,
- right of such person to receive the certificate on the basis of its indication in the order by the contracting authority as a subscriber or a person authorised to collect the certificate, except that in the case of TLS/SSL certificates issued based on the ACME protocol on the basis of authorization data used within this protocol, the certificate is transferred in accordance with this protocol without additional verification of the recipient's authorization.

Issuance of the first certificate may be performed at a branch of KIR after prior identification and authentication. Provided that the commercial offer provides for it, the process of identification and authentication may also be performed in the registered office of the ordering party, after it has purchased an appropriate travel service of an authorised representative of KIR.

3.3. Identification and Authentication During Renewal of the Certificate

Renewal of the certificate shall require having a valid agreement for the provision of trust services and submission of an order for certificate renewal. Verification of the agreement validity and data included in the agreement and in the order shall be done in accordance with Clause 3.2.

3.3.1. Renewal During Validity Period of the Current Certificate

Verification of data that is to be put in the certificate shall be done as described in Clause 3.2.2 and 3.2.3, for persons who are not natural persons and for natural persons, accordingly.

Proving the ownership of a private key shall be done as described in Clause 3.2.1.

Before issuing a certificate to the subscriber or a person authorised to collect the certificate, KIR shall check:

- the right of such person to receive a certificate on the basis of its indication on the order by the ordering party as a subscriber or a person authorised to receive the certificate, provided that in case of TLS/SSL certificates issued pursuant to the ACME protocol on the basis of authorisation data used under this protocol the certificate is transferred pursuant to this protocol without additional verification of the recipient's authorisation;
- identity of such person on the basis of the identification document presented by it or on the basis of an electronic signature/ electronic seal affixed in the request for certificate renewal verified with the use of a valid certificate issued by KIR, and for TLS/SSL certificates issued under the ACME protocol additionally on the basis of the correctness of the authentication data used under this protocol, the possibility to carry out renewal operations in relation to the available number within a given package and the current validation of the data contained in the certificate.

Renewal may be done at a branch of KIR after prior identification and authentication of the subscriber using the same methods that were applied at the time of the issuance of the first certificate. If the

commercial offer so provides, the process of identification and authentication may also be performed in the offices of the contracting authority, after an on-site service for an authorised representative of KIR has been purchased.

Test certificates are not subject to renewal.

3.3.2. Renewal After Expiry of the Current Certificate's Validity Period

If the validity period of the current certificate has expired, a personal contact with KIR S.A. shall be required. If the commercial offer or the Agreement so provides, the process of identification and authentication may also be performed in the offices of the contracting authority, after an on-site service for an authorised representative of KIR S.A. has been purchased.

In both instances, identification and authentication of the subscriber shall be performed just like in case of the issuance of the first certificate.

3.4. Identification and Authentication During Certificate Suspension or Revocation

Certificate revocation or suspension shall be requested by a subscriber, contracting authority or a third person, provided its data was included in the certificate or by another person, provided it is so established in the Agreement, or other obligations of KIR . Test certificates are not subject to suspension and revocation.

TLS certificates shall not be suspended.

A certificate that has been revoked may not be then recognised as operational.

A request for certificate revocation or suspension may be submitted:

1) personally at the branches of KIR, during office hours of KIR;
2) by phone calling a helpline at 801 500 207, during the help line's office hours;
3) 24hr at the website of KIR at www.elektronicznypodpis.pl;
4) according to mechanisms made available by ACME protocol - for TLS/ SSL certificates generated with the use of ACME protocol.

A request for certificate revocation or suspension shall at minimum include:

1) the given name and surname of the notifying person;
2) PESEL of the notifying person or another personal identifier assigned by an authority to do so;
3) data concerning the certificate (e.g. serial number, the subscriber's distinguished name, validity period);
4) reason for changing the certificate status.

For TLS/ SSL certificates generated using the ACME protocol, it is sufficient to transmit the authorization data provided by this protocol.

A specimen of the request for revocation/ suspension of the certificate is available at the website of KIR and www.elektronicznypodpis.pl.

The request for revocation/ suspension of the certificate submitted personally shall be based on positive verification of:

1) the identity of a person requesting revocation / suspension established on the basis of a presented identification document and its right to request certificate revocation / suspension;
2) data included in the request for certificate revocation / suspension.

The basis for acceptance of the request for certificate revocation/ suspension made by telephone or via the Internet shall be positive verification of:

1) the given name and the surname of the notifying person;
2) PESEL of the notifying person or another personal identifier assigned by an authority to do so;
3) data concerning the certificate;
4) passwords for revoking the certificate of the notifying person.

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

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

Conclusion of an Agreement for the provision of trust services shall be the basis for submission of orders for certificates and their issuance by KIR.

The Agreement may be concluded with a natural person, a legal entity or an organisational unit without corporate existence. Based on the Agreement the contracting authority shall indicate subscribers for whom it orders certificates or who shall be responsible for collecting certificates.

Conclusion of the Agreement is not required in case of test certificates.

4.1. Certificate Request

A request for certificate issuance shall be submitted to KIR in the form of an order. The request may be submitted using both a dedicated order form available at the website of KIR and also in a hard copy at a branch of KIR.

A certificate request can also be submitted via the ACME protocol. The prerequisite is to have the authorization data defined in 7.3.4 External Account Binding in RFC 8555.

4.1.1. Who may submit the request?

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

4.1.2. Request registration process

Requests shall be registered by Operators or they shall be registered automatically if they have been submitted via the Internet. Registration of requests delivered in a hard copy consists in entering data from the request into the system of the certification authority, following its prior checking. Operators shall be responsible for entering data in the correct way and in compliance with the order.

4.2. Processing of the Certificate Request

After receiving the order for a certificate KIR shall start verification of data included in the request, and then – if data has been positively verified – proceeds to register or approve the request in the system and to generate a certificate.

4.2.1. Performance of Identification and Authentication Function

After receiving the request with a full set of documents necessary to identify the customer, the Operator shall authenticate the data included in the request. Depending on the certificate type the authentication process may be different and based on actions described in Chapter 3 of this CPS.

With the exception of TLS certificates, an application for a certificate with an electronic signature can be processed automatically based on the data it contains.

The Operator that has confirmed – on behalf of KIR – the subscriber's identity or the person authorised to collect the carrier with the private key, shall certify performance of such confirmation with its own hand and give its PESEL number on the confirmation of certificate issuance. Confirmation of certificate issuance contains data concerning the certificate, data concerning the person to whom the certificate is given, and authentication of the Operator.

For TLS certificates KIR may reuse the previous domain validations provided if they were successfully performed not later than 12 months before issuance of a new certificate.

4.2.2. Acceptance or Rejection of the Request

Requests (orders) that are correctly filled in with authenticated data in the manner described in Chapter 3 are accepted for execution. The Operator who verifies the request must perform the following actions:

1) assign the request to a relevant agreement for the provision of trust services;
2) check authority to place orders vested upon a person who has signed the request for the certificate;
3) verify the data entered into the customer support system maintained by KIR during registration of the request against the data available in databases of KIR or other bases accessible to it;
4) make comparison of the data entered into the request against the data that is derived from the supplied documents.

Part of the above actions may be performed automatically.

If checking has been positive and all data included in the request is correctly verified, the Operator shall commence implementation of the request and generation of the certificate or forwards it to a relevant organisational unit of KIR for implementation.

If any data in the request is incorrect, the Operator shall reject the request about which it shall inform the contracting authority or the subscriber.

4.2.3. Request Processing Waiting Period

All requests are processed without undue delays in the order in which they have been filed with KIR or in accordance with the certificate collection dates that are entered in the order.

All requests should not be processed longer than 7 business days, unless the Agreement provides for other waiting period for processing of the request or the subscriber has indicated a collection date in the order that falls after a 7-day processing period.

4.2.4. Certificate Authority Authorization Records Processing

Before generating the certificate, KIR checks Certification Authorities Authorization (CAA) records, authorizing certificate authorities to issue certificates for given domains. If the CAA record is present, then KIR generates the certificate only if the CAA records include the following name: elektronicznypodpis.pl.

The CAA record indicating KIR as the certification authority authorized to issue the certificate takes the form:

1) for standard TLS certificates: domain name IN CAA 0 issue "elektronicznypodpis.pl";
2) for wildcard certificates: domain name IN CAA 0 issuewild "elektronicznypodpis.pl".

4.3. Issuance of the Certificate

Certificate issuance shall follow processing of the request and is performed by the Operator. Depending on its type the certificate shall be issued either on the basis of the request containing the public key that has been delivered by the subscriber, or for a pair of keys generated by KIR.

In case whereby the order concerns a certificate together with a pair of keys then KIR will generate a pair of keys on the carrier selected in the order dedicated to the subscriber notified in the order and shall record the generated certificate. TLS certificates are generated only on the basis of the request containing the public key generated by the subscriber.

By issuing the certificate KIR shall create the electronic seal linked with the subscriber's public key and the subscriber’s data.

The process of issuing another certificate after revocation of the previous or issuance of another certificate in case when the validity period of the certificate held by the subscriber has expired shall be similar to the process of issuance of the first certificate. If the certificate has been revoked not due to a necessity of changing the subscriber's distinguished name, then the new certificate may contain the distinguished name that was previously assigned.

The process of issuing an TLS certificate, in accordance with the requirements set out at http://certificate-transparency.org, is preceded by the issuance of a precertificate, which is published to at least 3 Certificate Transparency logs, with at least 1 of the logs being managed by Google and at least 1 not being managed by Google. The Signed Certificate Timestamp (SCT) obtained from the logs

is placed in the TLS certificate as the x509v3 extension. It should be emphasized that pre-certifications, as defined in RFC 6962 (Certficate Transparency), are not the certificates specified in RFC 5280 and are not subject to these requirements.

In case of TLS certificates KIR verifies compliance of pre-certificates with the Baseline Requirement using pre-issuance linters (zlint, crt.sh). An issued certificate shall be subject to the post-linting procedure.

For TLS/ SSL certificates generated using the ACME protocol, the subscriber's certificate is also made available through ACME mechanisms.

4.3.1. Actions by the Certification Authority During Certificate Issuance

Certificates shall be issued by KIR personally to the subscriber. An exception are test certificates that may be remotely delivered to the subscriber, e.g. via electronic mail to an address given in the order and verified in accordance with Clause 3.2.2. During the process of personal issuance of the certificate the Operator shall perform the following actions:

1) checks completeness of the executed order against the request submitted by the contracting authority;
2) compares the data included in the certificate confirmation against the data in the request;
3) verified the identity and rights of the subscriber;
4) if the compliance of data has been established and the identity has been successfully verified – it shall issue the certificate.

Issuance of a certificate by the root certification authority to subordinate operational certification authorities requires a person authorized by the KIR (i.e., a security inspector and a system administrator) to intentionally issue a direct order to the root certification authority to perform certificate signing operations.

4.3.2. Informing the Subscriber of the Certificate Issuance

The certificate collection date is indicated in the order. 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 shall be informed by telephone or electronic mail about the necessity to collect the certificate.

4.4. Certificate Acceptance

4.4.1. Confirmation of the Certificate Acceptance

The certificate shall be accepted by the subscriber by signing confirmation of certificate issuance on which data from the collected certificate is printed. A document confirming certificate issuance with the signature of the subscriber and the Operator issuing the certificate shall be kept by KIR. The second counterpart shall be given to the subscriber.

For TLS/ SSL certificates generated using the ACME protocol, certificate acceptance is confirmed by downloading the certificate within the ACME protocol.

4.4.2. Publication of the Certificate by the Certification Authority

In order to ensure compliance with Certificate Transparency (http://certificate-transparency.org), TLS certificates are placed in selected public registers https://www.certificate-transparency.org/known-logs. The rest of the 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 issuance of the certificate, provided that the certificate related to them or contained their data.

4.5. Pair of Key and Certificate Application – Obligations of the PKI Infrastructure Participants

4.5.1. Obligations of the Subscriber

The subscriber undertakes to:

1) use the certificate in accordance with its intended purpose indicated in a given certificate;
2) use the certificate only during the validity period of the certificate indicated therein;
3) protect its private key;
4) immediately notify KIR about the request to revoke the certificate in cases provided for in the Agreement, and information for the subscriber, the Policy, or this document.

The Agreement may provide for a more detailed scope of the subscriber's responsibilities. The subscriber may be also informed about its specific scope in information delivered in writing or electronically.

4.5.2. Obligations of the Contracting authority

The contracting authority undertakes to:

1) provide KIR with orders for subscribers authorised to receive certificates in compliance with regulations governing personal data protection;
2) provide KIR with lists of persons authorised to revoke certificates in compliance with regulations governing personal data protection;
3) provide KIR only with true data, including personal data of subscribers;
4) update personal data of persons authorised to receive and revoke certificates;
5) make subscribers acquainted with the provisions of the Policy and the CPS;
6) comply with the rules specified in the Policy and the CPS.

Additionally, if a certificate has been issued for a subscriber who is not a natural person, the contracting authority undertakes to:

1) use certificates with their intended purpose;
2) use certificates only during the validity period indicated in the certificate;

3) protect private keys;

4) notify KIR about the request to revoke the certificate.

4.5.3. Obligations of the Trusted Party

A trusted person shall be understood to mean a natural person, a legal person, or an organisational unit without corporate existence that shall undertake actions or any decision trusting electronically signed or sealed data with the use of a public key contained in the certificate issued by KIR.

Trusted parties are obliged to:

1) use certificates with their intended purpose;

2) verify the electronic signature or electronic seal at the moment of performing verification or at some other reliable time;

3) verify the electronic signature or electronic seal using the list of suspended and revoked certificates and the relevant certification path;

4) inform KIR S.A. about any cases of certificate use by unauthorised persons or suspicions that a certificate has been issued to a wrong entity.

4.6. Renewal of the Certificate for an Old Pair of Keys

4.6.1. Terms and Conditions of Certificate Renewal

The certificate for an old pair of keys may be renewed remotely by using a relevant form available at the website of KIR S.A. by marking an appropriate option during the renewal process or using the ACME protocol. Renewal may also be performed at a branch of KIR S.A.

Test certificates are not subject to renewal.

4.6.2. Who May Request Certificate Renewal?

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

4.6.3. Processing of the Renewal Request

A renewal request shall be processed in the same manner as requests for a new certificate.

4.6.4. Informing About Renewed Certificate Generation

If the subscriber or the contracting authority has selected on-line certificate renewal, information about renewed certificate generation shall be most often delivered to the subscriber by e-mail or telephone. For TLS/ SSL certificates generated using the ACME protocol, the certificate generation information is transmitted within the ACME protocol.

In case of renewal performed at a branch of KIR informing about renewed certificate generation shall be done during the subscriber's visit. In special cases, this may be done by telephone or e-mail.

4.6.5. Issuance of the Renewed Certificate

Issuance of a renewed certificate may be performed in the manner similar to issuance of a new

certificate. If the certificate is renewed on-line, the issued certificate shall be provided to the subscriber through a website dedicated to it.

4.6.6. Publication of the Certificate

Certificates are not published outside the internal network of KIR.

4.6.7. Notification of Other Entities About Certificate Issuance

In the same way as for new certificates. See Clause 4.4.3.

4.7. Renewal of the Certificate for a New Pair of Keys

4.7.1. Terms and Conditions of Certificate Renewal

The certificate for a new pair of keys may be renewed remotely by using a relevant form available at the website of KIR by marking an appropriate option during the renewal process. Renewal may also be performed at a branch of KIR or in the offices of the contracting authority , provided it has purchased a relevant service.

4.7.2. Who May Request Certificate Renewal?

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

4.7.3. Processing of the Renewal Request

A renewal request shall be processed in the same manner as a request for a new certificate. A request for renewal of the certificate for a new pair of keys submitted on-line must contain a request with the public key that is subject to certification.

4.7.4. Informing About Renewed Certificate Generation

Informing about generation of a renewed certificate for a new pair of keys shall be done in the same way as in case of generating renewal for the old pair of keys. See Clause 4.6.4.

4.7.5. Issuance of the Renewed Certificate

Issuance of the renewed certificate for a new pair of keys shall be done in the same way as in case of issuing of a renewed certificate for an old pair of keys. See Clause 4.6.5.

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

Notification of other entities about certificate issuance shall be done in the same way as in case of new certificates and certificates renewed for the old pair of keys. See Clause 4.4.3.

4.8. Change of Data Included in the Certificate

4.8.1. Terms of Making Changes

Data in certificates that have already been issued by KIR cannot be changed. The contracting authority

may only request certificate renewal with new data prior to the end of its validity period. Renewal with changed data may not be performed remotely. The only way of certificate renewal with the changed data is personal collection of the certificate and completion of the full certification path for the changed data.

4.8.2. Who May Request Changing Data in the Certificate?

There are not changed allowed in a certificate that has already been issued. The necessity of changing data means generating a new certificate, provided that the contracting authority or a person authorised by it shall decide whether the certificate with the data that requires changing shall be revoked or suspended.

4.8.3. Processing of the Request for Changing the Certificate Data

Processing of the request for changing data in the certificate shall be done in the same way as in case of issuing of a new certificate. See Clause 4.2.

However, confirmation of authorisation to collect the certificate, and also check the data, may be performed remotely with the use of the electronic signature or electronic seal, unless the CPS or the Policy requires personal appearance.

4.8.4. Informing About Generation of the Certificate with Changed Data

Informing about generation of a certificate with changed data may be performed electronically, by telephone, or personally during a visit at a branch of KIR.

4.8.5. Certificate Issuance

Issuance of a certificate with changed data shall be performed in the same way as in case of issuing of a new certificate. See Clause 4.3. In the event of applying Clause 4.8.3 second sentence, the certificate may be issued electronically.

4.8.6. Publication of the Certificate

Certificates are not published outside the internal network of KIR.

4.8.7. Notification of Certificate Issuance

Notification of other entities about certificate issuance shall be done in the same way as in case of new certificates, certificates renewed for the old and new pair of keys. See Clause 4.4.3.

4.9. Certificate Suspension and Revocation

Each certificate may be revoked before expiry of its validity period. Certificate suspension is a special case of revocation however, it is not possible to suspend all types of certificates. TLS certificates and test certificates shall not be suspended. A certificate that has been suspended may then be revoked or unsuspended. A suspension period shall be used to clarify doubts concerning conditions for having certificate revoked or unsuspended.

If there occur circumstances indicative of a necessity to revoke or suspend the certificate, KIR shall revoke/ suspend it.

Certificate revocation / suspension shall be done at the moment when the certificate number is entered in the list of revoked and suspended certificates. Information on certificate revocation / suspension shall be put in the list of revoked and suspended certificates. KIR shall notify the subscriber, a person whose data is included in the certificate, and, possibly, another person about certificate revocation/ suspension.

Following certificate suspension the certificate status may be changed:

1) upon the subscriber's request;
2) upon a person authorised to request certificate revocation or suspension that has submitted such request;
3) as a result of clarifying suspicions referred to in Clause 4.9.11.

Certificate suspension may continue until the end of the certificate's validity period.

A certificate may be unsuspended solely upon the subscriber's request personally submitted at KIR. A specimen of the request to change the status is available at the website of KIR.

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

If certificate revocation occurs after its previous suspension, then the certificate revocation date shall be the same as the certificate suspension date.

4.9.1. Terms and Conditions of Certificate Revocation

Certificate revocation may occur under the following circumstances:

1) It has been requested by the subscriber or a third person indicated in the certificate or another person authorised to submit such request;
2) Certificate has been issued on the basis of untrue data or has been issued without due verification of the application for certificate issuance and without consent of the contracting authority for its issuance;
3) Private key of the subscriber related to the public key in the certificate has been compromised or does not satisfy the requirements set forth in the Baseline Requirements;
4) KIR has received evidence that the certificate has been used contrary to its purpose;
5) Subscriber or the contracting authority have not paid their liabilities relating to certificate issuance;
6) KIR has received information confirming that the domain name entered in the certificate has ceased to be owned by the contracting authority (e.g. a domain registering entity has been revoked rights to register domains or an agreement for domain registration concluded between the domain owner and the domain registering entity has expired or the domain registering entity has not extended registration of a specific domain);
7) KIR has received information that a wildcard certificate for the domain has been used for authorisation of an inappropriate sub-domain;

8) Data included in the certificate has ceased to be valid or is untrue;

9) KIR has established that the data included in the certificate has materially changed;

10) KIR has established that information appearing in the certificate is imprecise or misleading;

11) Certificate has been issued contrary to the CPS or Policy;

12) KIR shall cease provision of services concerning certificates and no entity shall take over performance of information provision services having a certificate status;

13) Private key of the operational certification authority or the main certification authority has been compromised or KIR has obtained information that the said keys could have been compromised;

14) Violation on the obligations specified in law, the CPS or there exists another circumstance that poses a threat to the security of the electronic signature or electronic seal;

15) Technical parameters of the private key related to the public key contained in the certificate or the certificate format pose a threat for the software or trusting parties;

16) Content or certificate format does not satisfy the requirements concerning parameters of cryptographic algorithms specified in the document of the Baseline Requirements

17) Subscriber has lost its full legal capacity;

18) KIR has acquired information clearly evident that the certificate for signing a code issued by KIR has been used for signing malicious or damaging software.

19) KIR is made aware of a demonstrated or proven method that can easily compute the Subscriber's private key based on the public key in the certificate;

20) KIR has acquired information that that verification of control over the requested domain has been performed on the basis of incorrect information.

21) KIR is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed;

22) KIR has acquired information indicating that use of the email address in the certificate is no longer legally permitted.

KIR shall revoke a certificate within 24 hours if one of the following circumstances occurs:

1) It has been requested by the subscriber or a third person indicated in the certificate or another person authorised to submit such request;

2) Certificate has been issued on the basis of untrue data or has been issued without due verification of the application for certificate issuance and without consent of the contracting authority for its issuance;

3) Private key of the subscriber related to the public key in the certificate has been compromised;

4) KIR is made aware of a demonstrated or proven method that can easily compute the Subscriber's private key based on the public key in the certificate;

23) KIR has acquired information that that verification of control over the requested domain has been performed on the basis of incorrect information.

5) Private key of the operational certification authority or the main certification authority has been compromised or KIR has obtained information that the said keys could have been compromised;

6) KIR has acquired information clearly evident that the certificate for signing a code issued by KIR has been used for signing malicious or damaging software.

7) Subscriber has lost its full legal capacity;

8) KIR has acquired information indicating that use of the email address in the certificate is no longer legally permitted.

KIR shall revoke a certificate within 5 days if one of the following circumstances occurs:

1) Private key of the subscriber related to the public key in the certificate does not satisfy the requirements set forth in the Baseline Requirements;

2) KIR has received evidence that the certificate has been used contrary to its purpose;

3) Violation on the obligations specified in law, the CPS or there exists another circumstance that poses a threat to the security of the electronic signature or electronic seal;

4) Subscriber or the contracting authority have not paid their liabilities relating to certificate issuance;

5) KIR has received information confirming that the domain name entered in the certificate has ceased to be owned by the contracting authority (e.g. a domain registering entity has been revoked rights to register domains or an agreement for domain registration concluded between the domain owner and the domain registering entity has expired or the domain registering entity has not extended registration of a specific domain);

6) KIR has received information that a wildcard certificate for the domain has been used for authorisation of an inappropriate sub-domain;

7) Technical parameters of the private key related to the public key contained in the certificate or the certificate format pose a threat for the software or trusting parties;

8) KIR has established that the data included in the certificate has materially changed;

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

10) Certificate has been issued contrary to the CPS or Policy;

11) Data included in the certificate has ceased to be valid or is untrue;

12) KIR shall cease provision of services concerning certificates and no entity shall take over performance of information provision services having a certificate status;

13) Content or certificate format does not satisfy the requirements concerning parameters of cryptographic algorithms specified in the document of the Baseline Requirements;

14) KIR is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed;

Authorisation to request certificate revocation may be derived from the Agreement.

A request to revoke/suspend a TLS/ SSL certificate generated using the ACME protocol can be made using this protocol. Authentication and verification of such a request is done automatically using this ACME protocol.

Anyone can revoke any certificate through the ACME protocol if they can sign the revocation request with the private key associated with the certificate. No other information is required in such cases.

Subscribers can revoke certificates belonging to their accounts through the ACME API if they can sign the revocation request with the private key of the associated account. In such cases, no other information is required. 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 there is a necessity to end activities or there occurs a threat to the entire infrastructure of the public key supported by KIR.

Revocation of the certificate of the operational certification authority and the main certification authority may be caused by the following circumstances:

1) Certificate has been issued on the basis of untrue data or has been issued without due verification of the application for certificate issuance;

2) Private key of the operation certification authority related to the public key in the certificate has been compromised or does not satisfy the requirements set forth in the Baseline Requirements;

3) KIR has received evidence that the certificate has been used contrary to its purpose;

4) The certificate has been issued in violation of the CPS or Practice or is contrary to the requirements of the Baseline Requirements;

5) Data included in the certificate has ceased to be valid or is imprecise or misleading;

6) KIR shall cease provision of services concerning certificates and no entity shall take over performance of information provision services having a certificate status;

7) Private key of the main certification authority has been compromised or could have been compromised;

8) Violation on the obligations specified in the Policy, the CPS or the Agreement has been established or there exists another circumstance that poses a threat to the security of the electronic or digital signature;

9) Technical parameters of the private key related to the public key contained in the certificate or the certificate format pose a threat for the software or trusting parties.

10) Content or TLS certificate format does not satisfy the requirements concerning parameters of cryptographic algorithms specified in the document of the Baseline Requirements.

4.9.2. Whom May Request Certificate Revocation?

Certificate revocation may be requested by:

1) the contracting authority ;

2) a person authorised by the contracting authority ;

3) the subscriber;

4) relying parties, application software suppliers, and other third parties informing of reasonable cause to suspend or revoke the certificate;

5) another person authorised to submit such request.

4.9.3. Processing of the Certificate Revocation Request

After receiving a request for certificate revocation, the Operator shall check data from the certificate and verifies it against the data in the request. Operator shall also check authorisation of the person submitting the request.

If verification has been correct, information about certificate revocation shall be put on the CRL, and the subscriber or the contracting authority shall receive, confirmation of certificate revocation collecting it personally or by mail.

If a certificate revocation request is received under the ACME protocol, certificate revocation proceeds automatically in accordance with paragraph 7.6 of Certificate Revocation RFC 8555.

Information about certificate revocation/ suspension is present on CRL and in OCSP response at least until the end of the certificate's validity period.

If the certificate has data of another entity, it shall also receive confirmation.

4.9.4. Permitted Delays in Certificate Revocation

KIR shall exercise best efforts that following a request for its revocation a certificate is revoked without undue delays. The maximum permitted period of delay in certificate revocation may not exceed 24 hours.

4.9.5. Maximum Permitted Time for Revocation Request Processing

The certificate revocation request shall be processed without undue delays and shall be a priority task for the Operators. A maximum permitted time for request processing shall be 24 hours as from the moment of submitting a complete request.

4.9.6. Obligation to Check Revocations by a Trusted Party

A party trusting the data put in the public key certificate issued by KIR shall be obliged to check from

time to time if the certificate has not be put on a list of suspended and revoked certificate before it is used for verification of an electronic signature or electronic seal.

4.9.7. Publication Frequency of CRLs

CRLs for certificates issued by the root certification authority Szafir Root shall be published always after certificate suspension or revocation, however, not less frequently than every 12 months.

CRLs for certificates issued by the operational certification authority Szafir Trusted CA shall be published always after certificate suspension or revocation, however, not less frequently than every 24 hours.

CRLs are available at the website of KIR on a 24x7x365 basis.

KIR shall check availability of CRLs at least once a day.

4.9.8. Maximum Delay in Publication of CRLs

CRL lists are published without undue delays, immediately after they have been created. KIR stipulates that a delay in publication of CRLs may be not longer than 60 minutes.

4.9.9. Availability of Other Methods to Verify the Certificate Status

KIR shall provide a possibility of verifying the status of a certificate issued by KIR in real time by means of Online Certificate Status Protocol (OCSP). The service is available on a 24x7x365 basis and operates on a certificate database issued by KIR. The OCSP service operates in compliance with RFC 9690 on a request – response basis and handles POST and GET methods of HTTP protocol requests. To obtain information on the status of a certificate issued by KIR please send a request containing data that allows certificate identification, i.e. its serial number and an identifier of the certificate issuer. The request should comply with a format defined in RFC 2560. In response, information on the certificate status is provided:

1) Good – means that the certificate has been issued by KIR and is not in CRL issued by KIR
2) Revoke – means that a specific certificate has been issued by KIR and is in CRL, i.e. it has been revoked
3) Unknown – means that a certificate has not been issued by KIR and the status of such certificate is not known.

4.9.10. On-line revocation checking requirements

In case of subscribers' certificates KIR shall update information provided via the OCSP protocol every few minutes. The maximum validity period of the OCSP response is greater than 8 hours and less than 9 hours.

In case of certificates of intermediate authorities KIR shall update information provided via the OCSP protocol at least once a year and maximum up to 24 hours after revocation of the intermediate certificate.

4.9.11. Special Responsibilities When a Key Has Been Compromised

In the event of a key of the Szafir Root, Szafir Root CA2, Szafir Trusted CA or Szafir Trusted CA2 certification authority has been compromised, KIR shall be obliged to inform the subscribers, contracting

authority, and trusted parties about such fact as soon as possible by disclosure put up at the website of KIR S.A.

Entities that are not subscribers may report compromise of the subscriber's key by presenting the following evidence of the private key associated with the TLS certificate issued by KIR:

1) a file with a request for certificate issuance where the following entry has been placed in the Own Name field "Proof of Private Key Compromise for KIR" or
2) a signed text file with the contents agreed upon with KIR with the use of a compromised key
3) a respective private key.

For this type of notification the notifying entity shall be obliged to provide a valid e-mail address to which a confirmation of acceptance of the notification shall be sent and which shall be used for further explanatory correspondence.

KIR may allow other alternative methods of proving possession of the private key that have not been mentioned in the above section at its own discretion.

In case of certificates that have been issued on cryptographic cards, a sufficient reason for changing the certificate status to revoked shall be submitting to KIR evidence of holding the card by providing the card's serial number or a photograph showing the card's serial number.

4.9.12. Terms and Conditions of Certificate Suspension

TLS certificates and test certificates shall not be suspended. A certificate that has been suspended may then be revoked or unsuspended.

If certificate revocation occurs after its previous suspension, then the certificate revocation date shall be the same as the certificate suspension date.

Following certificate suspension the certificate status may be changed. Certificate suspension may continue until the end of the certificate's validity period.

Following removal of the previous certificate suspension, information about such certificate shall be removed from the list of suspended and revoked certificates.

Information on revoked certificates the validity period of which assigned by KIR has expired may not be removed from the list of suspended and revoked certificates.

With the exception of TLS and test certificates, KIR may suspend a certificate if there is a suspicion that the certificate has untrue data or the private key for such certificate has been compromised and in other cases of becoming reasonably aware that there are conditions for certificate revocation.

4.9.13. Who May Request Certificate Suspension?

Certificate suspension may be requested by:

1) the contracting authority ;
2) a person authorised by the contracting authority ;

3) the subscriber;

4) another person authorised to submit such request.

4.9.14. Processing of the Certificate Suspension Request

A request for certificate suspension shall be processed in the same way as in case of a revocation request. See Clause 4.9.3.

4.9.15. Permitted Delays in Certificate Suspension

The permitted period of delay in suspending a certificate may be 24 hours.

4.10. Verification of the Certificate Status

Verification of the status of certificates issued by KIR shall be done on the basis of published CRLs.

4.11. Waiver of Trust Services

Trust services are provided under an agreement. Termination of the agreement means discontinuance in the provision of services for the contracting authority . Termination of the agreement shall not result in revocation or suspension of certificates that have been issued under the agreement.

4.12. Recovery and Storage of Private Keys

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

5. PROCEDURES OF PHYSICAL, OPERATIONAL AND ORGANISATIONAL SECURITY

5.1. Physical Security Measures

Premises in which processing of data relating to issuance, suspension, or revocation of certificates takes place and where certificates are generated, suspended, and revoked 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”. Applied measures of protection shall protect against:

1) unauthorised access to the premises;

2) natural disasters and fortuitous events;

3) fire;

4) infrastructure failure;

5) flooding, theft, burglary, and robbery.

Applied measures of physical protection of the premises implemented on the basis of the Standard of security for persons and property in the premises of KIR

shall include, but are not limited to:

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

5.1.1. Location and Premises

The certification centres are located in two independent processing centres for which security plans have been prepared describing:

1) general information concerning location of the buildings;
2) general information concerning physical protection of the buildings;
3) division of buildings into zones;
4) the applied protection measures for individual zones, including zones where telecommunication and IT systems are operated to provide trust services.

Generation, suspension, revocation, and issuance of certificates shall also be performed at local offices of KIR.

5.1.2. Physical Access

The rules applicable to access control to the premises are provided by the Procedure of managing access by persons and vehicles to the premises of KIR.

Pursuant to an agreement physical protection of KIR has been given to a licensed agency having staff (including licensed physical protection guards) and hardware resources that allow full performance of tasks that relate to the nature of the facility and its size. Superiors in all shifts of guards who protect the facility have qualifications of physical protection.

The premises of KIR are logically divided into zones with different levels of access and proper technical and organisational 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-Condition

Power to the buildings of KIR is supplied from the two independent power-supply lines. In the event of power outage in the two supply sources, power generating units shall be switched on. Telecommunication and IT devices used in processing are powered from the so-called guaranteed power supply source that is secured by UPSs that ensure continued power supply. The buildings have

UPSs operating in a parallel arrangements ensuring redundancy which provides for continuity of power supply even if one of the UPSs is down.

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

1) general;
2) specific that maintains constant temperature and humidity in the server room.

5.1.4. Flood Hazard

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

5.1.5. Fire Protection

The building is equipped with fire-protection systems that allow early fire detection (SAP), limiting its spreading (fire partitions), protection an escape route against smoke, a permanent fire-extinguishing system located in the premises that are most critical for operations of KIR.

The building has the following security solutions in place:

1) passive protection, i.e. the building has been equipped with fire-protection wall barriers;
2) active protection, i.e.:
    a) the signalling and alarm system equipped with detectors allowing early detection of fire and buttons that allow forwarding the alarm signal from each floor in the building to the fire signalling centre,
    b) early smoke detection system,
    c) permanent fire-extinguishing equipment (gaz FM 200) that is used for fighting fires in their first phase,
    d) escape route lighting – there are escape route lights installed in the building that are equipped with batteries that support lights for at least two hours.

5.1.6. Information Carriers

Information carriers that contain copies of current data are stored in the strong cabinets that are located in the protected premises that are used for operations. Strong cabinets are accessed by employees who perform the function of operators of the key certification system. Carriers with archived data are stored in fire-proof safes in the premises with the top protection level in the primary and back-up centre. Access to the safes have employees who perform the function of a Security Inspector.

5.1.7. Destruction of Redundant Carriers and Information

Destruction of magnetic and optical carriers is performed by a commission. Data on magnetic carriers is removed in the manner that prevents its reading, and if removal of data is impossible, carriers are physically destroyed in the way that makes accessing data saved in them impossible.

Optical carriers are physically destroyed in the way that makes accessing data saved in them impossible.

Destruction of carriers shall be performed in the manner that ensures obtaining a minimum 2nd security class in accordance with the standard DIN 32 757-1.

Destruction of carriers shall be recorded in a scrap report. The scrap report shall contain:

1) destruction completion date;
2) description of the object of destruction;
3) description of the time span for destruction of archived data;
4) signatures of persons performing and attending the destruction process

The scrap report shall be kept by a Security Inspector of the Szafir telecommunication and IT system not shorter than for 3 years. A copy of the scrap report shall be forwarded to the Information Security Administrator who shall keep it not shorter than for 3 years.

5.1.8. Back-up Copies and Back-up Location

In the event of failure of the primary location that houses the infrastructure that is used for the provision of trust services preventing provision of trust services, operations of the system shall be taken over by a back-up system located in the back-up location. In the event of failure, the back-up system shall take over work relating to revocation, suspension of certificates and publication of the list of suspended and revoked certificates on an on-going basis.

5.2. Organisational Security Measures

The system used for the provision of trust services is operated by employees of KIR who are responsible for operations of telecommunication and IT systems, and in particular:

1) persons who act as a system Security Inspector whose responsibilities include supervision over implementation and application of all security procedures governing operations of telecommunication and IT systems used in the provision of trust services;
2) operators who receive orders, requests for suspension/ revocation / unsuspension of certificates, who issue certificates;
3) system administrators whose responsibilities include installing, configuring, and managing systems and telecommunication and IT networks used for the purposes of provision of trust services, hereinafter referred to as “administrators”;
4) person who acts as an Information Security Administrator whose responsibilities included supervision over compliance with the requirements set forth in the personal data protection law;
5) persons who act as supervisors of physical and telecommunication and IT security at KIR.

5.3. Staff Supervision

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

5.3.1. Qualifications, Experience, Authorisation

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

1) cryptography, electronic signatures, electronic seals and the public key infrastructure;
2) mechanisms protecting networks and telecommunication and IT systems;
3) personal data protection;
4) automatic data processing in networks and telecommunication and IT systems;
5) hardware and software used for electronic data processing;
6) forgeries of own hands and documents establishing identity;
7) operation of application and secured cryptographic devices used for the purposes of provision of trust services.

5.3.2. Staff Screening

Before assigning an employee with any of the roles described in Clause 5.2 KIR shall perform its screening. Screening shall be done with regard to:

1) an employment certificate from the previous employer (it applies to new employees);
2) diplomas and certificates confirming the employee's educational background;
3) professional qualifications and experience;
4) employee statement of good conduct .

Confirmation of a clean record in the National Criminal Register is done during work performance at least once a year.

5.3.3. Training

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

Technical personnel are regularly trained in the use of the IT infrastructure organised by manufacturers or providers of technical solutions.

5.3.4. Repetition of Training

Training is repeated depending on the needs and prior to implementation of significant changes in service provision.

5.3.5. Frequency of Rotation of Positions and Its Sequence

The CPS does not provide for the frequency and sequence of how positions should rotate.

5.3.6. Sanctions for Unauthorised Actions

In the event whereby unauthorised actions performed by an employee have been detected or all there are allegations about them, a Security Inspector may take a decision on blocking such employee's access to the system. Further explanatory actions are carried on pursuant to the internal regulations of KIR S.A. and provisions of law.

5.3.7. Contracted Employees

There are not actions at KIR envisaged that would involve provision of trust services by persons not employed at KIR.

5.3.8. Documentation of the Staff

Operators and administrators have access to operating procedures, applications' user's manuals that are used in the certification authorities and which are necessary for the performance of responsibilities of an Operator or administrator.

5.4. Procedures for Recording Events and Audit

KIR shall maintain a register of all events that are related to the provision of trust services. Events are registered to ensure security and exercise supervision over correct operations of the system. They also provide for accountability of actions performed by employees who carry out actions relating to the provision of trust services. Registers of events are kept electronically and in a hard copy. All registers of events shall be properly secured and made available for the purposes of an audit. A Security Inspector shall be a person responsible for keeping the register of events.

5.4.1. Types of Recorded Events

Registration shall comprise:

1) events directly related to the provision of trust services, and in particular: generation of CA keys, acceptance of a certificate issuance request, generation of keys and certificates for subscribers, revocation of certificates, generation of CRLs, etc.;
2) actions related to customer and subscriber service: acceptance and execution of agreements, requests, issuance of certificates, delivery of certificates, invoicing, etc.;
3) system events (logs) from the servers and working stations that are part of the certificate generation system;
4) events relating to system technical support: errors and alarms, a register of entered changes into the system, user support.

Register of events are recorded electronically. Records shall contain an event identifier, the date and time of its occurrence, event type, and detailed description.

5.4.2. Frequency of Events Inspection (Logs)

System logs are subject to constant, daily inspection. Key elements of the system are controlled automatically in real time. An inspection report shall be saved in the system log book. Logs shall be reviewed periodically (once a month). All recorded irregularities must be explained, and a relevant report shall be put into the system log book.

Access to the registers of events has a Security Inspector, an Audit Inspector, and a System Administrator only.

5.4.3. Period of Storing Registers of Recorded Events

The registers of events shall be kept on discs of servers and working stations in the form of files, databases, records of system logs. The register of events directly relating to the provision of trust services shall be available throughout the entire period of operations of the CA. After operations of the CA have been completed the registers shall be available in the archives for a period of 7 years.

System logs and event log books are periodically archived and available in the archives for a period of 7 years.

5.4.4. Protection of the Recorded Events

The registers of events shall be kept on disk arrays. Disk arrays are configured in the manner that prevents the loss of data because of disk failure and are monitored on a continued basis. Security Inspectors and administrators have access to the registers. Each record in the database of the key certification system is electronically signed or sealed thus ensuring record integrity.

5.4.5. Procedures of Making Back-Up Copies of the Recorded Events

The registers of the system of the certification authority are copies in real time into a back-up location with the use of mechanisms offered by the disk array. Once a month all registers shall be electronically signed by a Security Inspector, recorded on optical carriers, and put into safes. There shall be two copies of the registers made, with one remaining in the primary location, and the other in the back-up one. Access to the safes have persons who perform the function of a Security Inspector.

5.4.6. System of Collecting Data for the Purposes of the Audit (Internal vs. External)

Program modules of the key certification system and servers shall automatically make records in the registers of events. Other events shall be registered manually in relevant databases. For the purposes of an internal audit data shall be made available on-line or from archived records kept in the safes.

5.4.7. Notification of Entities Responsible for the Occurring Event

Elements of the certification system and supporting systems are subject to continued supervision by monitoring systems and technical staff. Information on a detected threat or a hazard in security shall be directly forwarded to the administrator and Security Inspector. Depending on the level and importance

of such hazard persons responsible for operations of components such event relates to shall be notified. Notification may be done electronically or by telephone.

5.4.8. Assessment of Susceptibility to Threats

KIR shall analyse susceptibility to threats on a current basis that relate to procedures and systemic solutions. An internal audit of the system oraz analiza ryzyka is performed periodically. To minimise susceptibility to threats business continuity procedures are updated and tested. The Security Inspector shall be responsible for the susceptibility analysis.

A risk analysis is conducted at least annually. The risk analysis shall include:

1) foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of data related to certificate issuance and certificate management processes;
2) an assessment of the likelihood and potential harm, given the materiality of the data and certificate management processes;
3) assessing the sufficiency of policies, procedures, information systems, applied technologies implemented and used to address the threats.

5.5. Data Archiving

KIR shall keep and archive documents and data in an electronic form directly relating to the provided trust services for 20 years from the moment of certificate issuance, and in case of CRLs - for a minimum 7 years from the moment when a specific list has been generated. Storing and archiving shall be performed in compliance with the requirements specified in the personal data protection law. Documents and data in an electronic form (with the exclusion of the archived CRLs and certificates) shall not be made available outside.

5.5.1. Types of Archived Data

Archiving shall include:

1) orders;
2) agreements for the provision of trust services;
3) confirmations of certificate issuance;
4) certificates;
5) CRLs;
6) registers of events of the key certification system;
7) system logs of the servers;
8) system logs of the firewall;
9) system log books.

5.5.2. Archiving Period

Paper and electronic documents referred to 1) – 4) Clause 5.5.1 shall be kept for 20 years. Data referred to 5) – 9) Clause 5.5.1 exist only in electronic form and shall be kept for 7 years.

5.5.3. Archives Protection

Archived data stored electronically shall be kept in fire-proof safes. The safes shall be put in the primary location and the back-up one in the top security zone. Access to the safes shall have persons who perform the function of a Security Inspector.

5.5.4. Procedures of Creating Back-Up Copies

Back-up copies shall be created to protect data and to recover the system after a failure. Copies of data from the key certification system shall be created in real time with the use of synchronous replication of disk resources that are stored in the disk arrays. Additionally, a full back-up of the databases is created once a day. Each location shall have carriers with the back-up copies of the system and application software.

Detailed procedures of creating back-up copies are governed by internal procedures of KIR.

5.5.5. Required Time-stamping of Archived Data

There shall be no time-stamping of the archived data.

5.5.6. Data Archiving System (Internal vs. External)

KIR can outsource archiving of data in paper form associated with the provision of trust services. Archiving shall take place in a company with considerable experience in this area and meets the relevant criteria with regard to personal data. The company has implemented quality management systems and information security in accordance with the requirements of PN-EN ISO 9001: 2009 and BS ISO / IEC 27001: 2014 in terms of customer service in the process of storage, scanning and destroying records.

5.5.7. Procedures of Verifying and Accessing Archived Data

Access to the archives is vested on authorised persons only. The access to the data may ask only authorised persons in KIR and defined in the agreement between the companies. Access to the archived registers of events kept in the safes is vested only on persons who perform the function of the Security Inspector. Carriers in the archives are reviewed every 2 years. Data integrity is verified. Data from the carriers that are older than 2 years shall be recorded on new carriers, older shall be destroyed in accordance with relevant procedures.

5.6. Replacement of the Key

Replacement of the keys of the certification authorities shall be done in a way that ensures compliance with the established minimum validity period of subscribers' certificates. Well ahead of the expiry of a certificate of a specific certification authority there is a new independent infrastructure of the public key created within which a new pair of keys is generated and a certificate of a new certification authority. Until a certificate of the old certification authority has expired two certification authorities shall operate. The new certification authority shall assume the role of an expiring authority and shall perform all actions

relating to the support of certificates: generation, suspension, and revocation of subscribers' certificates, and generation of CRLs. The expiring certification authority shall support only revocation and suspension of certificates issued within its infrastructure and shall generate CRLs until it has ceased its operational activities (certificate expiry).

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

A new certificate of the certification authority shall be published at www.elektronicznypodpis.pl and distributed in the systems and software (e.g. in Internet browsers). Information on a change of the keys may be published in mass media.

5.7. Compromising of the Key and Launching After Failures or Natural Disasters

If a private key of the certification authority used for generation of certificates has been compromised, a CRL shall be generated containing a certificate that relates to the compromised private key.

KIR shall exercise its best efforts to ensure continued and failure-free operations of the certification authority. The technical infrastructure of the certification authority, inter alia, has a doubled hardware and software configuration outside the primary location, a back-up power supply (power generator) in both locations and other safety measures that provide for continued operations in the event of any failure. In the event of a failure of the primary location that prevents provision of the basic functionality of the certification authorities, they shall be launched in the back-up location within 24 hours from find out about the failure.

KIR shall have and regularly review a Business Continuity Plan (PCD) that includes information on:

1) the purpose and scope of the PCD;
2) business continuity strategy, including:
    (a) a list of critical processes and required recovery times (RTOs);
    b) prioritization of critical processes;
    c) business continuity strategy for IT infrastructure;
    (d) policies in the event of an Emergency;
    (e) incident management
    f) documenting activities;
3) PCD documentation and principles of updating/accessing and storing
4) PCD reviews
5) PCD audits
6) PCD testing
7) training and awareness raising

8) accountability

9) Crisis management structure

10) State of Emergency and State of Crisis, including criteria for initiating/acting/terminating a State of Emergency and criteria for initiating/acting/terminating a State of Crisis; crisis communications.

The PCD shall be tested in accordance with the adopted PCD Test Plan. Each time after tests have been conducted, a report shall be prepared and sent to appropriate units of KIR.

5.7.1. Procedures of Handling Incidents and Responding to Hazards

KIR has a set of procedures for handling incidents and unforeseeable events. All incidents shall be reviewed in detail by relevant organisational units and remedial measures shall be implemented. Details have been provided for in an internal procedure of KIR.

5.7.2. Procedures of Recovering Computing Resources, Software, and/or Data

KIR has a set of operating procedures to be used in the event of a necessity to recover resources. Each location has resources allowing recovery of the certification authority's full functionality. In particular, these include:

1) back-up of the data;

2) back-up of the keys of certification authorities;

3) copies of cryptographic cards with shared secrets and operators cards;

4) carriers with the software of the key certification system;

5) operating procedures of the certification authorities.

Recovery procedures are included in PCD.

5.7.3. Actions in the Event Whereby the Private Key of a Registration Authority has been Compromised

Compromising of the key of the certification authority is a crisis situation and is part of the PCD. If the private key has been compromised, KIR shall undertake the following actions:

1) revokes the certificate of the certification authority and puts it on CRLs,

2) notifies the certification authority about certificate revocation using available communication including notifying affected software vendors by creating a notification on relevant platforms,

3) generates a new key of the certification authority and new certificates of the subscribers.

Detailed actions in the event whereby the key has been compromised are described in the internal procedures of the PCD.

5.7.4. Ensuring Business Continuity After Disasters

In case of disasters and other unpredictable circumstances KIR has the PCD. Procedures of the PCD strictly define the way of conducting actions necessary for restoring operations. Tests of the PCD procedures are held periodically.

5.8. Completion of Operations of the Certification Authority or the Registration Authority

KIR shall have the right to discontinue issuance of certificates. In such event, all subscribers and contractor authorities shall be informed accordingly with a 90-day notice. Subscribers using certificates, contractor authorities, and trusted parties shall have no right to make any claims against KIR, provided, however, that KIR shall still perform its obligations with respect to processing of requests for certificate suspension or revocation and publication of the list of suspended and revoked certificates. Otherwise, contracting authorities shall have the right to reimbursement of part of the payment for the certificate in proportion of its usage period.

6. TECHNICAL SECURITY PROCEDURES

Below are described the procedures governing generation and management of cryptographic keys of the certification authorities, the operators, and subscribers. This chapter also includes a description of technical solutions that have been applied to ensure security of the keys and high level of the infrastructure security.

6.1. Generating and Installing A Pair of Keys

6.1.1. Generating A Pair of Keys of the Certification Authorities and Subscribers

Generation and installation of the keys is performed in accordance with the internal procedure of KIR that governs the rules of generation and management of the CA keys.

The Szafir Root and Szafir Root CA2 are superior authorities, whereas the Szafir Trusted CA2 and Szafir Trusted CA3 act as an operational authority.

Each of root CA authority has two pairs of RSA keys and the self-signed certificate of the public key. A certified key is used for certification of the public keys of the operational centres and generation of lists of the revoked certificates (CRL and ARL). The second pair of keys is used for securing communication within the infrastructure of the Root CA PKI. The keys of the root CA are generated within a separate environment: the CA server is an engine dedicated only for supporting processes relating to the superior CA and is equipped with a cryptographic module that meets the security standards according to FIPS-140-2 level 3. Generation of keys and operations relating to the use of the private key shall be performed in the cryptographic module only. In order to prevent the emission of electromagnetic radiation, all operations using the root certification authorites' master keys are performed in a data centre equipped with appropriate physical barriers (Faraday cage).

The operational certification authority generates certificates for the end users. The operational certification authority has two pairs of RSA keys, of which one public key has been certified by the

superior authority. The role the Szafir Trusted CA is to generate certificates of the public keys of subscribers and publication lists of the revoked certificates (CRL). The second pair of keys is used for securing communication within the infrastructure of the sub CA. The keys of each operational certification authority are generated within a separate environment: the certification authority server is an engine dedicated only for supporting processes relating to the root certification authority and is equipped with a cryptographic module that meets the security standards according to FIPS-140-2 level 2 and level 3. Generation of keys and operations relating to the use of the private key shall be performed in the cryptographic module only.

A committee made up of employees of KIR is established to generate keys. All activities are made under the auditor supervisory. All activates and their completion time are registered in the document registering the activities. After the generation procedure has been completed, together with relevant reports the document is signed by the committee and filed into the archives.

Keys of the Operators are used for signing subscribers' requests for certification of keys. They are also used for authorisation of the Operators in the system and securing communication between the client application and the program module of the Registration Authority. Keys of the Operators are recorded on cryptographic cards and issued to authorised employees under supervision of the Security Inspector.

The subscriber may itself generate a pair of keys and present the public key for certification in the form of a PKCS#10 request. Keys for subscribers may also be generated by the operational certification authority, both in the cryptographic cards or in the form of files. Keys generated in files are password protected.

For TLS certificates KIR does not generate private keys on behalf of subscribers, but it may do so for other types of certificates.

6.1.2. Delivery of the Private Key to the Subscriber

If keys are generated in the sub CA, the private and public key shall be forwarded to the subscriber together with a public key certificate. During the first registration in the Szafir Trusted CA, the subscriber shall have to appear personally in the registration authority to verify their identity and collect the carrier with the private key, or – if the Agreement so provides - process of identity verification and provision of the private key may also be done in the offices of the contracting authority , after an on-site service of the Operator has been purchased. If the keys have been issued in a cryptographic card, access to the private key shall be secured with the PIN/PUK codes that the subscriber shall assign individually after receiving the card. The registration authority may also generate the subscriber's keys in the form of a PKCS#12 file that is password protected.

6.1.3. Delivery of the Public Key to the Certification Authority

If the certification authority generates a pair of keys there is no necessity for the subscriber to deliver a public key. If the keys are generated by the subscriber, it shall deliver its public key to the registration authority in the form of an electronic request signed with the private key that complies with the PKCS#10 standard. Keys to be certified shall be delivered from the registration authorities to the certification

authority through an encrypted communication channel in the form of electronic requests signed with a key by an authorised registration inspector.

Applications may also be delivered electronically using the ACME protocol.

6.1.4. Delivery of the Public Key of the Certification Authorities to Trusted Parties

Keys of the certification authorities shall be made available to trusted parties in the form of certificates that comply with the X.509v3 standard. A certificate of the superior CA is a self-signed certificate, whereas a certificate of the sub CA is signed by the appropriate superior CA. Certificates of the certification authorities are published at the website of KIR www.elektronicznypodpis.pl

Certificates of the certification authorities are also distributed in the in-house program of KIR that is used for supporting the electronic signature, electronic seals and in Internet browsers.

6.1.5. Length of Keys

Keys of the certification authorities have the following length:

Certification Authority (CA)	Length of the Key
Szafir Root CA	2048 bits RSA
Szafir Root CA2	2048 bits RSA
Szafir Trusted CA	2048 bits RSA
Szafir Trusted CA2	2048 bits RSA
Szafir Trusted CA3	4096 bits RSA

Keys of the subscribers may be 2048 or 4096 RSA bits long.

Certificates of the subscribers shall be issued for RSA keys having the length of 1024, 2048, 3078, 4096 bits and ECC for keys 256 bits (ECDSA from secp256r1) and SHA-1 or SHA-256 hash functions.

TLS Certificates shall be issued for RSA keys having the length at least of 2048 bits and SHA-256 hash functions.

6.1.6. Generating Parameters of the Public Key and Quality Check

The process of generating keys in the certification authority is performed using a pseudo-random number, while applying strong cryptographic algorithms. To ensure high quality keys prime numbers are subjected to the Miller-Rabin primality test. KIR does not impose any limits concerning the parameters of key generation for subscribers generate the key on their own and submit it for certification. It is, however, recommended that the key should satisfy the requirements set in the document called EESSI-SG Algorithms and Parameters for Secure Electronic Signatures. The CA shall check if the key that has been presented for certification satisfies the requirements set forth in Clause 6.1.5.

6.1.7. Application of the Keys (By Key Usage Field for X.509 v.3 Certificates)

The key usage is defined by the KeyUsage field (OID: 2.5.29.15) with extensions of standard certificates.

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

Certificates of subscribers may also have the ExtKeyUsage field (OID: 2.5.29.37). It defines detailed application of the key.

The ExtKeyUsage field (OID: 2.5.29.37) may also occur in subscribers' certificates. It specifies the specific use of the key. In Szafir Trusted CA3 certificate, used to certify subscribers' keys, there is an ExtKeyUsage field (OID: 2.5.29.37) having the values clientAuth, emailProtection.

Szafir Root CA2 private keys are not used to sign certificates, except for:

1. self-signed certificates representing the root certification authority (self-signed certificate);
2. operational certification authority's certificates, cross certificates;
3. infrastructure certificates (administrative role certificates, internal certificates of operational devices of the certification authority);
4. certificates for verification of OCSP responses.

6.2. Protection of the Private Key and Technical Control of the Cryptographic Module

Private keys of the certification authorities are protected in the manner that prevents their unauthorised use, loss, or disclosure. Keys are generated and stored in a secure environment that is protected by cryptographic modules. Keys are subject to divisions into secrets, access to secrets is vested only upon appointed and trusted employees of KIR. Keys of subscribers may be generated by the certification authority in the form of PKCS#12 files that are password protected or on cryptographic cards protected by PIN/PUK codes.

6.2.1. Standards for the Cryptographic Module

Hardware modules used in the certification authority meet the following standards:

Module protection the root certification authority keys – FIPS-140-2 level 3.

Module protection the operational certification authority keys – FIPS-140-2 level 2 and level 3.

6.2.2. Private Key Division

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

A chart of the private key division:

Certification Centre	Total Number of Secrets [n]	Number of Secrets Necessary for Using the Key [m]
Root certification authority	6	3
Operational certification authority	5	2

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

A secret holder shall be held responsible for due protection of the secret. In the event of loss, theft, damage to the card or any other situation that compromises the secret's security the Security Inspector shall have to be immediately notified accordingly.

6.2.3. Depositing of the Private Key

KIR does not provide services of depositing and storing private keys of subscribers. The keys of certification authorities are not deposited outside KIR.

6.2.4. Back-Up Copies of the Private Key

A certification authority shall create back-up copies of the keys and store them in the back-up location. Copies of the cards with share secrets shall be deposited in the certification authority's safes, and access to safes shall be granted to Security Inspectors only. PINs to the cards shall be kept in sealed envelopes deposited in the safes located in other premises. Disk files in a close safety environment of cryptographic modules are stored on servers in the encrypted form with a 3DES algorithm. A full set of materials used

for recovering a private key of the certification authority shall not be kept in a single place. In the event of a necessity to recover the key from back-up copies a procedure of entering the key into the module is performed as described in Clause 6.2.6.

6.2.5. Private Key Archiving

KIR does not archive private keys of the certification authorities. Following expiry of the certificates of the public keys of the certification authorities and discontinuance of operations, the private keys of the certification authorities shall be destroyed. KIR does not archive private keys of the subscribers.

6.2.6. Uploading a Private Key to the Cryptographic Module or its Downloading

Uploading a private key to cryptographic modules is done in the following situations:

1) launch of the certification authority during the system start-up;
2) recovery of the key of the certification authority in the back-up location;
3) replacement of the cryptographic module.

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

6.2.7. Storing of 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. There is no possibility to read the value of the private key from the module, this key never leaves the module. Operations that require using the private key are performed in the cryptographic module.

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

6.2.8. Private Key Activation

Once uploaded into the module, the key shall be active. Signing operations shall be performed in separate sessions. The program module of the certification authority that uses a private key must be authenticated to perform the signing operations. Only a program module that uses the infrastructure keys may perform such operations. Following authentication an active session is open and data for signing or sealing are sent to the module.

6.2.9. Deactivation of the Private Key

After the operation of signing the data in the module has been completed the session between the module and software shall be closed. Execution of another signature requires opening a new session. Deactivation of the key in the module may be performed by the system administrator upon request of a Security Inspector or, if there is a need to perform deactivation (key is subject to a threat,

system has been shut down). Deactivation shall be performed by cleaning 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 operations of the certification authority have been completed, all elements used for recovering of the private key shall be destroyed.

Cards that contain co-shared secrets shall be cleaned with the use of utility software and next physically destroyed by cutting.

Destruction of the carriers and cards shall be performed by a specially formed committee. The fact of destroying the carriers and cards shall be confirmed by a report with signatures of the committee members.

6.2.11. Possibilities of the Cryptographic Module

Parameters of cryptographic modules are described in Clause in Clause 6.2.1.

6.3. Other Aspects of Key Management

The following clauses describe aspects relating to the validity period of certificates and archiving of keys.

6.3.1. Public Keys Archiving

The certification authority shall keep the archives of public keys. The purpose of archiving is to create a possibility of verifying electronic signatures and electronic seals after expiry of the validity period of a certificate of the authority and closure of its operations.

Keys of the certification authority shall be subject to archiving. Public keys shall be archived in the form of certificates. Archiving shall be done by a Security Inspector. Archiving shall be performed by recording files with certificates on optical carriers. Archived files shall be affixed with an electronic signature of a Security Inspector. Details of how to set up the electronic archives are described in Clause 5.5

The archiving period for public keys shall be:

Entity's public key	Archiving Period
Root certification authority	min. 7 years
Operational certification authority	min. 7 years

6.3.2. Validity Period of Certificates

Operational Period of Certificates

Certificate of an Entity	Validity Period
Root certification authority	20 years

Operational certification authority	10 years
Subscriber	maximum 1095 days since a certificate is generated, excluding Elixir and TLS certificates The maximum validity period of Elixir certificates is 762 days from the date of certificate generation. The maximum validity period of TLS certificates is 398 days from the date of certificate generation.

6.4. Activating Data

If a certificate and a pair of keys have been generated on a cryptographic card, then prior to the first use of the card, the subscriber shall be obliged to assign their own PIN and PUK code that protects access to the card.

In case whereby a pair of keys is recorded by KIR together with the certificate, before it is issued to the subscriber in the form of a file, then it shall be protected by a password assigned by KIR.

The subscriber or another person authorise to submit a request for certificate revocation / suspension shall be obliged to deliver to KIR passwords for certificate suspension and revocation. The password, written down on a sheet of paper, shall be put into a sealed non-transparent envelope. Failure to forward the password prevents submission of a request to revoke or suspend a certificate by the Internet or telephone.

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

1) first name and the surname of the authorised person;
2) PESEL of the authorised person or another personal identifier assigned by an authority to do so.

If the password is submitted by a person other than the subscriber, such person shall be obliged to give the legal grounds authorising it to request certificate revocation or suspension.

Envelopes with passwords shall be stored at KIR, whereas access to them shall have only persons authorised at KIR to suspend and revoke certificates.

The person authorised to request certificate revocation or suspension shall have the right to change the previously given password.

6.4.1. Generation and Installation of Activating Data

Assigning codes by the subscriber to protect the card with the pair of keys and the certificate should be performed with the use of application for card management that has been delivered by KIR together with the card.

A password to protect the file with the keys and the certificate shall be generated at random by KIR in the process of generating the pair of keys and recorded in a save envelope.

6.4.2. Activating Data Protection

The PIN and PUK codes that have been assigned by the subscriber shall be known to the subscriber only.

The password to the file with the pair of keys and the certificate shall be known to the subscriber only.

It is the subscriber's responsibility to protect the PIN and PUK codes for the card and the password protecting access to the file with the keys.

Disclosure of the PIN and PUK codes or the password to the file with the keys to other persons should be a condition for requesting certificate suspension or revocation.

6.4.3. Other Aspects Relating to Activating Data

Copies of the passwords to protect access to the files with the pairs of keys shall not be stored at KIR. KIR does not have any codes or data that allow recovering the PIN and PUK codes that protect access to the card and which were assigned by the subscriber.

6.5. Supervision Over Computer System Security

For provision of the trust service hardware and specialist software shall be used that makes up a closed computer system. The system has been executed in the way that satisfies the requirements set forth in the document called CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

6.5.1. Technical Requirements Concerning Specific Security Measures for Computer Systems

Servers and working stations of the system shall be specially prepared to operate in the certification system (hardening of the operating systems) and protected with anti-virus software. Management of the accounts in the system shall be multi-level and performed at the level of the domain/operating system, application of the system managing certificates, and databases. User accounts shall be assigned in accordance with the rules described in the internal documents of KIR. KIR enforces multi-factor authentication for all accounts associated with the issuance of certificates.

6.5.2. Assessment of Security of Computer Systems

Assessment of security of the computer systems shall be performed on the basis of WebTrust Principles and Criteria for Certification Authorities.

6.6. Life Cycle of Technical Security Measures

6.6.1. System Development Supervision

Supervision over system development shall be exercised by a Security Inspector. He shall approve the system configuration and the planned changes to the software and hardware. Before it is approved for a production environment, each change shall be tested in a testing environment. After passing rigorous

acceptance tests, it may be implemented in the production environment. Any changes in the system shall be recorded in the system documentation and registered in the register of events.

Computer hardware and cryptographic modules are selected in such way to be able meet an assumed functionality and security standards.

6.6.2. Security Management Supervision

KIR has extended internal procedures for security management. There is constant monitoring of system security performed at many levels. Examined is the integrity of software, network traffic, configuration of the system and security devices. A system inspection report is regularly prepared. Supervision over system security is exercised by professionals from KIR.

6.6.3. Supervision Over of the Life Cycle of Security Measures

The CPS does not impose a life cycle of the security measures that have been applied. Security measures shall be replaced in the event of a need to apply other than those that are currently used, amendments in legal regulations, or if technologically they are outdated and do not comply with the current standards and norms.

6.7. Supervision Over Computer Network Security

Access to the communication and IT system in which trust services are provided shall be protected at the level specified in the law for qualified trust services.

Supervision over security of the computer networks of KIR is exercised by qualified staff.

With respect to computer network security, KIR shall apply the best market practices, including among others complying with the current guidelines of the CAB Forum Network and Certificate System Security Requirements.

7. CERTIFICATE PROFILE AND CRLs

7.1. Certificate Profile

Certificates issued by KIR are made up three parts:

- tbsCertificate;
- signatureAlgorithm;
- signature.

The first part of the certificate (*tbsCertificate)* is made up of the following primary fields:

Field	Field Meaning	Content
version	marking of certificate version	3
serialNumber	certificate serial number	unique certificate number under the certificate issuance system (greater than zero (0) containing at least 64 bits of output from a CSPRNG)
signature	identifier and signature parameters applied by KIR to create the electronic seal	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }

issuer	identifier distinguishing an entity that provides trust services that has issued the certificate	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= Szafir Trusted CA2 C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= Szafir Trusted CA3
validity	marking of the beginning and end of the validity of the certificate issued by KIR	time of certificate generation and end of the certificate validity period with an accuracy of up to a second
subject	identifier of the subscriber related to the public key placed in the certificate	value that is referred to in Clause 3 of the Certification Practice Statement
subjectPublicKeyInfo	value of the public key with the algorithm identifier with which the key is associated	public key presented by the entity
extensions	standard and non-standard extensions	in accordance with the table below

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

Extension Name	Critical/ Non-Critical	Extension Meaning	Content
authorityKeyIdentifier	non-critical	identifier of the public key used to verify the issued certificate	160 bit SHA-1 hash function
subjectKeyIdentifier	non-critical	certificate identifier containing the hash of the public key included in the certificate	160 bit SHA-1 hash function
keyUsage	critical	determines the scope of use of the public key included in the certificate	digitalSignature – for electronic signature execution, nonRepudiation – related to execution of non-repudiation service, keyEncipherment – for key encipherment
extendedKeyUsage	non-critical	determines the permitted scope of application of the public key included in the certificate	clientAuthentication – verification of the customer's certificate, serverAuthentication – verification of the server's certificate, emailProtection – for electronic mail protection
certificatePolicies	non-critical	determines the certification policy, in accordance with which a specific certificate has been issued	- identifier compliant with Clause 7.1.6
subjectAltName	critical/non-critical	complementary subscriber's name	E.g. electronic mail address; This field includes the domain name (FQDN - Fully- Qualified Domain Name) only in the case of TLS certificates. For TLS certificates the field is required.
basicConstraints	critical	allows 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	
cRLDistributionPoint	non-critical	indication of the URL where CRLs are published	
authorityInfromation Access	non-critical	indication of OCSP URL at which the validity status of the certificate may be checked	
Certificate Transparency – Signed Certificate Timestamp (SCT) oid 1.3.6.1.4.1.11129.2.4.2	non-critical	Signed stmap of the certificate	

In case of Standard certificates extension extendedKeyUsage includes the following values: clientAuthentication, emailProtecion.

In case of TLS certificates extension extendedKeyUsage includes the following values: serverAuthentication and clientAuthentication.

In case of test certificates extension extendedKeyUsage may include the following values: clientAuthentication, serverAuthentication, if the field subjectAltName includes domain name, otherwise extension may take values: clientAuthentication, emailProtecion.

In case of Elixir certificates extension extendedKeyUsage includes only clientAuthentication.

In case of Server certificates extension extendedKeyUsage includes only clientAthentication.

7.1.1. Version number(s)

All KIR certificates issued in compliance with X.509 v.3.

7.1.2. Certificate Extensions

Extension are created in accordance with RFC 5280. All extensions included in subscribers' certificates are included in the table in section 7.1. Certificate Profile.

7.1.2.1. KIR root certificate

The KIR root certificate (SZAFIR ROOT CA2) valid from 2015 to 2035 includes the following extensions

- basicConstraints (critical) – cA True (the pathLenConstraint field is not present);
- keyUsage (critical) – keyCertSign, cRLSign;
- subjectKeyIdentifier.

7.1.2.2. KIR subordinate Certificate

Szafir Trusted CA2 operational certification centre certificate valid from 2015 to 2025 includes the following extensions:

- basicConstraints (critical) – cA True (the pathLenConstraint field is not present);
- keyUsage (critical) – keyCertSign, cRLSign;
- authorityKeyIdentifier;
- subjectKeyIdentifier;
- certificatePolicies;
- cRLDistributionPoints;
- authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2.

Szafir Trusted CA3 operational certification centre certificate valid from 2015 to 2025 includes the following extensions:

- basicConstraints (critical) – cA True (the pathLenConstraint field is not present);
- keyUsage (critical) – keyCertSign, cRLSign;
- authorityKeyIdentifier;
- subjectKeyIdentifier;
- certificatePolicies;
- cRLDistributionPoints;
- authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2.
- extendedKeyUsage – clientAuth, emailProtection

7.1.3. Algorithm Identifiers

The following requirements apply to the subjectPublicKeyInfo field in a certificate or precertificate.

In case of a certification authority that generates certificate in compliance with the Policy, the authority shall create electronic seal with an RSA algorithm having 2048 or 4096 bit keys and an SHA-1 hash function.

Certificates of the subscribers shall be issued for RSA keys having the length of 2048, 3078, 4096 bits and ECC for keys 256 bits (ECDSA from secp256r1) and SHA-256 hash functions.

TLS Certificates shall be issued for RSA keys having the length at least of 2048 bits and SHA-256 hash functions.

7.1.4. Name Forms

Certificates contain indication of the subject of the certificate issuer and the subject of the certificate prepared in accordance with Clause 3.1.1.

7.1.5. Limitations Imposed on Names

TLS certificates may not contain IP addresses in the *subject* and *subjectAltName* fields. Additionally, TLS certificates in the *subject and subjectAltName* fields may not contain domain names that are not registered in the DNS system.

Domain names can be included only in TLS certificates and test certificates to test TLS connections.

7.1.6. Identifier of the Certification Policy

The identifier of the policy for standard certificates looks as follows:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-standard(3)

The identifier of the policy for TLS certificates issued before the 31st of August 2020 looks as follows:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-TLS(6)

The identifiers of the policies for TLS certificates issued after the 1st of September 2020 look as follows:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-TLS(6)

and additionally one of the following identifier of compliance with Baseline Requirements Certificate Policy for the Issuance and Management of Publicly - Trusted Certificates:

- for TLS DV certificates:

  joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)

- for TLS OV certificates:

  joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)

The identifier of the policy for test certificates looks as follows:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-test(7)

The identifier of the policy for Elixir certificates looks as follows:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-ELIXIR(8)

The identifier of the Server certificate policy looks as follows:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-Server(9).

7.1.7. Use of Extensions Not Allowed in the Certification Policy

KIR does not envisage putting in certificates other extensions than those referred to in Clause 7.1.2 of the CPS.

7.1.8. Policy qualifiers syntax and semantics

Certificates issued by KIR contain a certification policy qualifier placed in the policyInformation extension (certificatePolicies).

7.1.9. Processing of Semantics for the Critical Extensions of the Certification Policy

KIR does not define requirements in this respect.

7.2. Profile of the CRL

The list of suspended and revoked certificates is made up of three parts:

- tbsCertList;
- signatureAlgorithm;
- signature.

The first part of the CRL (*tbsCertList)* is made up of the following primary fields:

Field	Field Name	Content
version	marking of the version of the list of suspended and revoked certificates	2
signature	identifier and signature parameters applied by KIR to create the electronic seal	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identifier distinguishing an entity that provides trust services that has issued the certificate	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= Szafir Trusted CA
thisUpdate	issuance date of the list of suspended and revoked certificates	time of CRL generation with an accuracy of up to a second
nextUpdate	planned time of issuing another list	planned time of generation of another CRL with an accuracy of up to a second
revokedCertificates	list of suspended and revoked certificates	– certificate serial number – certificate revocation/suspension date and time – certificate revocation/ suspension code
crlExtension	extended list of suspended and revoked certificates:	– key identifier of the entity to verify 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 certificate revocation/ suspension codes are:

- *unspecified* – the reason for certificate revocation is unknown The reason unspecified is represented in the CRL by omitting the reasonCode;.
- *keyCompromise* – indicates that it is known or suspected that the subscriber's private key has been ,compromised.
- *cACompromise* – indicates that the certificate has been revoked due to compromise or suspected compromise of the certification authority key
- *affiliationChanged* – indicates that the subscriber's name or other subscriber identity information contained in the certificate has changed, but there is no reason to suspect that the subscriber's private key has been compromised;

- *susperseded* – indicates that the certificate is being replaced for the following reasons:, the Subscriber has requested a new certificate or the certification authority has reasonable evidence that the validation of the authorization or domain control for any fully qualified domain name or IP address in the certificate is no longer reliable, or the certification authority has revoked the certificate for reasons of compliance with the Baseline Requirement or the Policy or Code;
- *cessationOfOpertion* – indicates that, for example, the website for which the certificate was issued was closed before the end of the certificate's validity period or the Subscriber no longer owns it before the end of the certificate's validity period ub does not control the domain indicated in the certificate;*privilegeWithdrawn* – indicates that there was a violation on the part of the Subscriber that did not lead to the compromise of the private key, for example, the Certificate Subscriber provided misleading information in the certificate application or failed to meet its material obligations under the terms of use.
- *certificateHold* – certificate has been suspended. Status cannot be assigned for a certificate for which such status is excluded according to Baseline Requirement

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

- indication of a necessity to contact the certificate issuer to clarify the reason for certificate suspension;
- indication of obligatory rejection of the reviewed certificate.

The *signatureAlgorithm* field contains an identifier of the algorithm used by the certification authority to create an electronic seal under the CRL. In case of certification authorities that generate certificates in compliance with the CPS, it is an RSA algorithm having 2048 bit keys and an SHA-1 or HAS-256 hash function.

The *signature* field contains an electronic seal created by the issuer of a CRL – a certification authority. For data included in the tbsCertificate field a value of the hash function is generated that shall be enciphered with the private key of the certification authority.

CRLs are published at the website of 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 the OCSP protocol (Online Certificate Status Protocol) in accordance with RFC 6960. The OCSP service is provided by all certification authorities described in the CPS. Each of the certification authorities uses a dedicated certificate to create OCSP responses. The service is provided as an Authorized Responder. Responses of the responder are authenticated with the use of a special certificate that has been issued for that purpose by the authority and the status of which is authenticated by the responder. Certificates of the responders include the extendedKeyUsage extension that corresponds to the value of id-kp-ocspSigning (OID 1.3.6.1.5.5.7.3.9) and the extension No Check (OID 1.3.6.1.5.5.7.48.1.5). Each of the certification authorities uses a dedicated certificate to create OCSP responses.

A certification authority that provides the OCSP service puts information on the manner of accessing the service in the issued certificates. Such information is included in AuthotityInfoAccess 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  }
```

An access method to OCSP (OID id-ad-ocsp) has been put in the accessMethod field, while in the accessLocation field, there is an URI to the OCSP service.

7.3.1. Certificate Status Query

The OCSP server accepts queries about the certificate status the syntax of which is compliant with RFC 6960:

```
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 the syntax of which is 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 on 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 is not in the CRL,

1 – revoked – certificate has been issued by KIR and has been revoked, it is in the CRL,

2 – unknown – certificate status is not known.

In case of status 1 (revoked) information on the time and reason for revoking is put in the revocationTime and revocationReason fields of the RevokedInfo structure. The revocationReason field may assume values of CRLReason 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),
        removeFromCRL(8)
        privilegeWithdrawn(9)
}
```

7.3.3. Version Number

Responses of the OCSP service 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.

8. COMPLIANCE AUDIT AND OTHER ESSESSMENTS

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

8.1. Issues Covered by Audit

Issues covered by audit include:

1) controls concerning management of the key's life cycle;
2) controls concerning the certificate's 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 Assessment

An external audit shall be performed at least once a year in accordance with the schedule approved in an agreement with the auditor. Internal audits shall be carried out in accordance with the plan that is effective at KIR for audits comprising certification authorities.

8.3. Identity / Qualifications of the Auditor

External audits are carried out by a company that is authorised to perform such compliance audits. It should be a company that has proper experience in conducting compliance audits and employs a sufficient number of properly trained staff.

8.4. Relation Between the Audited and the Audited Unit

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

8.5. Actions Undertaken to Removal Defects Detected During the Audit

Any information about defects detected during the audit shall be forwarded to persons managing the certification authority of KIR or a Security Inspector. Such persons shall immediately undertake actions aimed at removing defects.

8.6. Informing About Audit Results

Information about audit results in the form of an audit report or a summary of such report shall be published at the website of KIR.

KIR once every quarter shall carry out an internal audit performed by authorised employees of KIR. During the audit the correctness of processes related to issuance and management of certificates shall be checked on the basis of a random sample of at least 10% of the TLS certificates issued in a given quarter.

9. OTHER BUSINESS AND LEGAL ISSUES

9.1. Fees

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

9.1.1. Fees for Certificate Issuance and Its Renewal

KIR shall charge fees for certificate issuance and its renewal. The amount of such fess depending on the certificate type is set in the price list of trust services, the Agreement, the offer, or in another document that contains price proposals.

9.1.2. Fee for Access to Certificates

Fees for access to certificates are not charged by KIR.

9.1.3. Fees for Revocation or Information About Certificate Status

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

9.1.4. Fees for Other Services

As regards provision of trust services KIR may also charge other fees, provided they shall be introduced to the price list of trust services. They may include, among others, fess for:

- training and consultation;
- cards;
- readers;
- software.

9.1.5. Reimbursement of Fees

Reimbursement of fees is permitted under regulations of Polish law in case KIR has not performed its agreement concluded with a contracting authority or its has performed unduly.

9.2. Financial Liability

KIR shall be held liable for damage related to services that are governed by the CPS.

An 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 reviewing such filing.

KIR shall be held liable only for damage that has been caused during the validity period of the certificate that such damage relates to.

KIR undertakes to pay compensation, if it confirms that damage has been caused by operations by KIR and included within the scope of responsibilities of KIR The amount of paid compensation shall not be higher than the amount of damage that has been demonstrated and recognised and may not exceed the amounts specified in Clause 9.8.

9.2.1. Financial Liability

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

9.2.2. Other Assets

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

9.2.3. Extended Scope of the Warranty

The CPS does not provide for any requirements in that respect.

9.3. Business Information Confidentiality

Agreements, personal data, any information relating to the provision of trust services, and also obtained in the course of their provision shall be confidential. They shall be protected by the following provisions, respectively:

1) the Act on Prohibiting Unfair Competition of 16 April 1993. (Journal of Laws of 2020, item 1913, as amended) to the extent applicable to the enterprise secrets, and also

2) RODO.

9.3.1. Scope of confidential information

Protected shall be information that is held by KIR:

1) internal procedures concerning provision of trust services;
2) private keys of the infrastructure of KIR used for the provision of trust services;
3) passwords for suspending and revoking of certificates;
4) archives, logs of the operations of the telecommunication and IT system used for the provision of trust services;
5) data of subscribers or other entities involved in issuing, revoking, and suspending of certificates.

9.3.2. Information That is Not Confidential Information

Information that is not confidential information is all information that has not been marked as confidential by subscribers, trusted parties, or KIR.

Data recorded in the certificate shall be deemed as not covered confidentiality.

9.3.3. Responsibility for Protection of Confidential Information

KIR shall be responsible for protecting confidential information it has been entrusted with.

9.4. Personal Data Protection

Personal data of the subscribers and persons authorised by the recipients of trust services provided to KIR shall be subject to protection in line with the requirements on personal data protection.

Processing of personal data at KIR shall be done pursuant to the rules provided in the personal data protection law and its secondary regulations. Every person to whom a certificate has been issued shall have rights provided from these regulations.

9.4.1. Privacy Rules

Protection of privacy of the subscribers and persons authorised by recipients of trust services is of specific importance for KIR.

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

Personal data of persons authorised by the recipients of trust services shall be processed solely and to the extent necessary for the performance of the agreement on the provision of trust services.

Processing of personal data of the subscribers for the purposes of promotion of services of KIR shall be done on the basis of separate consent issued by the subscribes. The subscribers shall be informed about a voluntary nature of such consent and a possibility of its withdrawal.

Each person shall have 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 that indicated in Clause 9.4.2 shall not be considered as private.

9.4.4. Responsibility for Protection of Private Information

Krajowa Izba Rozliczeniowa S.A. 02-781 Warszawa ul. rtm. W. Pileckiego 65 is a controller of the subscriber's personal data, in the meaning of RODO, and shall be held liable for the protection of personal data.

9.4.5. Reservations and Authorisation to Use Private Information

In compliance with the requirements of the personal data protection law KIR may entrust personal data processing to a third party.

9.4.6. Disclosure of Information in Compliance with a Court or Administrative Order

Pursuant to the requirements of the personal data protection law KIR shall be obliged to provide personal data to entities that may submit such requests in accordance with mandatory regulations of law.

9.4.7. Other Circumstances of Information Disclosure

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

9.5. Intellectual Property Protection

Copyright to this document is held by Krajowa Izba Rozliczeniowa It may be used solely for the purposes of using certificates. Any other uses, including the entire or part of the document shall require a written consent of Krajowa Izba Rozliczeniowa, provided that KIR expresses its consent to copying and publishing this document in its entirety.

A contracting authority shall be held fully liable for the data disclosed by them in the certificate. KIR does not verify data provided by subscribers in terms of its merits, and does not verify the use of the registered trademarks, either. Further to that KIR shall not be held liable for their default.

Certificates of the certification authorities of KIR, i.e. Szafir Root CA and Szafir Trusted CA are the property of KIR. KIR shall grant licenses to software or hardware manufacturers for making copies of certificates of the certification authorities and for placing them in the software, especially in certificate warehouses or on hardware.

9.6. Representations and Warranties

9.6.1. Obligations and Warranties of KIR with Respect to Non-Qualified Trust Services

KIR undertakes to:

1) issue certificates in response to correct certificate orders submitted to KIR;

2) reliably verify 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 subscribers;
4) reliably verify requests for issuance of certificates, if they are not produced by KIR;
5) reliable verify identity of persons requesting certificate revocation or suspension and their rights to request certificate suspension or suspension;
6) revoke and suspend certificates in response to the correctly submitted requests;
7) provide information on suspended and revoked certificates at the website;
8) protect processed personal data about subscribers;
9) protect its private keys used for generation of certificates and lists with suspended and revoked certificates in accordance with the CPS;
10) perform other obligations provided under law;
11) register and verify reports concerning reliability of certificates issued by it and which are submitted by subscribers, recipients of services or trusted parties.

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

KIR shall be liable for damage caused by failure to perform or undue performance of its obligations with respect to the provided services, unless such failure to perform or undue performance of such obligations has resulted from the circumstances for which KIR is not held liable and which it could not have prevented despite exercising reasonable care.

KIR shall be responsible for storing and archiving data relating to issuance, suspension, and revocation of a specific certificate.

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

The Agreement may define a more detailed scope of the responsibilities of KIR.

9.6.2. Obligations and Warranties of the Registration Authority

Since all registration authorities are organisational units of KIR they do not provide any other additional warranties or are not charged with any other additional obligations.

9.6.3. Obligations and Warranties of the Subscriber

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

9.6.4. Obligations and Warranties of the Trusted Party

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

9.6.5. Obligations and Warranties of Other Entities

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

9.7. Exclusions from Liability Under the Warranty

KIR shall not be held liable for damage resultant from the use of certificates outside the scope defined in the Policy that has been indicated in the certificate, including in particular liability for damage resulting from exceeding the threshold value of a transaction, if such value has been disclosed in the certificate.

KIR shall not be held liable for damage resultant from incorrect data included in the certificate, entered pursuant to a request of the subscriber or the contracting authority , and also that the verification of which has been based on their statements or that has been entered in accordance with the submitted documents that have been forged or presented untrue or non-valid data.

KIR shall not be held liable for damage resultant from non-valid data entered in the certificate, if at the moment of certificate issuance it has been true.

KIR shall not be held liable for consequences, including suffered damage, of using the software the executable code of which has been signed with a certificate for signing the code issued by KIR.

KIR shall not grant any warranty to users of the software or hardware in which certificates of the certification authorities of KIR has been placed pursuant to the license referred to in Clause 9.5 and shall not be held liable for damage resulting from the use of such software.

9.8. Limitation of Liability

If during provision of trust services there is damage occurring attributable to KIR, liability towards all parties may not exceed:

1) PLN 0 in total and for a single damage in case of test certificates;

2) PLN 100,000 in total and for a single damage in case of other non-qualified certificates.

Liability of KIR does not include opportunity costs and is limited to actual damage.

KIR shall only be responsible for damage that has been intentional or caused due to gross negligence, provided that KIR shall be held at default for damage caused by consumers who are contracting authority relating to improper performance of services rendered to them.

9.9. Compensation

Compensation shall be payable upon a recognised complaint, settlement, including a court settlement, or a judgement of a common court.

9.10. Term of the Document and Expiry of Its Validity

9.10.1. Term

This document shall be effective as from the moment it has been assigned an effective status and published on the website of KIR until another effective version has been published.

9.10.2. Expiry

Another version of the CPS that has been published shows its effective date that at the same time is the expiry date of the present CPS. Thus, the previous CPS shall lose its status as being effective.

9.10.3. Effects of Document Expiry

After this CPS has expired, users of the certificates issued by KIR shall comply with its provisions during the term of its effectiveness until the expiry of the certificate's validity period.

9.11. Individual Notices and Communication with Users

Commonly available means of communication, including written, telephone, and electronic shall be used for exchanges between KIR and users. The Parties may define in the Agreement special, additional methods of communication.

Certain types of communication exchange between KIR and users shall enforce strictly defined methods of communication, e.g. specific network protocols.

Information such as CRLs and current certificates of the certification authorities shall be made available for all those interested in a continuous manner. Any information about defaults on the private key of any of the certification authorities that is subject to this document shall be immediately made available to all those interested.

9.12. Implementing Amendments to the Document

9.12.1. Amendment Implementation Procedure

KIR shall verify the CPS once a year for compliance with applicable CA/Browser Forum requirements: Baseline Requirements and Mozilla Root Security Policy. If there is no need to change the document, it shall be reviewed to confirm compliance with the latest version of the CA/Browser Forum Baseline Requirements. Amendments to the CPS may be implemented depending on the needs, in particular as a result of discovering errors or due to necessary updates or in the wake of annually updates implementing the latest version www.cabforum.org requirements. Amendments may also result from suggestions submitted by interested persons.

Proposals of changes may be submitted by internal mail of KIR by authorised employees of KIR, and also other interested persons by electronic mail to the contact addresses of KIR or by traditional mail.

Interested persons who may submit proposals of amendments to be implemented in the CPS are:

1) auditors;
2) contracting authorities;
3) subscribers;
4) employees of KIR, especially a Security Inspector;
5) legal institutions, especially in case of discovering conflicting provisions in the CPS that are contrary to the regulation of applicable law.

After amendments have been implemented, the document is updated, its publication date and the version number shall be changed. Each time, amendments shall have to be accepted by the Management Board of KIR.

9.12.2. Mechanisms and Dates of Notifying About Amendments and Expected Comments

Before material amendments are implemented all interested parties shall be informed accordingly by being sent information about intended amendments or by putting such information up at the website of KIR.

The interested parties may send comments to amendments within 10 business days from reception or publication of the same. Amendments relating to comments, provided they are substantial, must be published again and subjected to the above procedure of informing the interested parties.

In other cases, a new version of the CPS with amendments shall be subject a procedure of approval at KIR until it has been given an “effective” status.

Amendments notified by those interested may be accepted in their entirety, accepted with corrections or rejected after expiry of the date for submitting responses to another version of the document.

Amendments that do not require informing those interested and which may be implemented without notifying them include:

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

This kind of amendments are not subject to an amendment procedure.

9.12.3. Circumstances Requiring a Change of the Identifier

A change of the identifier (OID) may occur in the event of a change of an entity that manages the certification authorities.

9.13. Dispute Resolution Procedures

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

9.14. Governing Law and Jurisdiction

Polish law shall be governing law, and disputes shall be resolved by a common court of competent and actual jurisdiction in Poland.

9.15. Compliance with Applicable Law

KIR operates all of its business in compliance and pursuant to law applicable in Poland.

9.16. Miscellaneous Provisions

The CPS does not provide for any requirements in that respect.

9.16.1. Completeness of the Terms and Conditions of the Agreement

The Parties shall be bound by the provisions of the Agreement, the CPS, and the Policy.

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 written consent.

If the operations consisting in the provision of services included by this CPS have ended, KIR may transfer the rights to use the private key and issue and publish a CRL onto another entity without consent of the contracting authority , the subscriber, or the trusted party.

9.16.3. Severability of Provisions

In the event of doubts or discrepancy between the provisions of the Agreement, the Policy, and the CPS that cannot be removed, the Agreement shall prevail having priority before the CPS and the Policy.

In the event whereby provisions of any of the above documents do not comply with law resulting in their invalidity, the valid provisions included other documents shall remain effective.

9.16.4. Enforceability Clause

Temporary non-exercising of the rights of KIR, as well as failure to use them against one or more of the contracting authorities or subscriber, may not be construed as a waiver, or permanent abandoning of their use and shall not affect the contents and interpretation of the CPS or the Policy.

9.16.5. Force Majeure

Circumstances of force majeure shall be understood as extraordinary events that are external, impossible to predict, such as disasters, fires, floods, explosions, social unrests, acts of war, acts of state authorities, power supply failure or failure or a telecommunication connection which, in part or in whole, prevent satisfaction of obligations included in the Agreement, the CPS, or the Policy or make performance of such obligations in accordance with the terms and conditions specified therein difficult.

KIR shall not be held liable for any default on its obligations, if this has been caused by force majeure.

9.17. Other Provisions

The CPS does not specify any other provisions.