Krajowa Izba Rozliczeniowa S.A.

CERTIFICATION POLICY OF KIR S.A.
FOR
QUALIFIED CERTIFICATES

Version 2.1

Document history

Version Number	Status	Author	Issue Date
1.0	Document approved by the Management Board of KIR S.A.	Elżbieta Włodarczyk	14 November 2002
1.1	Document approved by the Management Board of KIR S.A.	Elżbieta Włodarczyk	27 February 2003
1.2	Document approved by the Management Board of KIR S.A. - previous version effective as from 28 February 2010	Elżbieta Włodarczyk	29 January 2004
2.0	Document approved by the Management Board of KIR S.A. - version effective as from 1 March 2010	Elżbieta Włodarczyk	1 March 2010
2.1	Document approved by the Management Board of KIR S.A. - version effective as from 1 March 2010	Elżbieta Włodarczyk	10 January 2013

LIST OF CONTENTS

1. INTRODUCTION

"The Certification Policy of KIR S.A. for Qualified Certificates", hereinafter referred to as the Policy, shall specify detailed solutions, including technical and organisational, indicating the manner, the scope, and the terms and conditions for developing and applying qualified certificates, hereinafter referred to as certificates. An identifier of this Policy that has been registered in the National Identification Cards Registry is the following: 1.2.616.1.113571.1.1.

Krajowa Izba Rozliczeniowa S.A. NIP: 526-030-05-17, registered by the District Court for the City Warsaw, XIII Commercial Division of the National Court Register under the registration number of 0000113064, is a qualified entity to provide certification services within the meaning of the Digital Signature Act of 18 September 2001 (Journal of Laws No. 130, item 1450 as amended), hereinafter referred to as the "Digital Signature Act"), entered in the register of qualified entities providing certification services under number 6, pursuant to Decision No. 7/014499/03 of the Minister of Economy, Labour, and Social Policy.

Certification services are also offered by field units of KIR S.A. The list of units of KIR S.A. together with their working hours is available at the web site of KIR S.A. at www.elektronicznypodpis.pl. Some of actions relating to the provision of certification certificates, including issuance of certificates and their revocation KIR S.A. may commission to be performed by outside entities, also referred to as "Partners".

Any correspondence relating to the provision of certification services shall be sent to the office address of KIR S.A.:

Krajowa Izba Rozliczeniowa S.A.
ul. Pileckiego 65
02-801 Warszawa, Poland
with an annotation "certificates"

tel. +48 801 500 207
e-mail: bok@kir.com.pl

or to the address of field units of KIR S.A., as well as electronically to the addresses provided at the website of KIR S.A.

2. DEFINITIONS

Operator - an employee authorised by KIR S.A. who is involved in registration of subscribers and acceptance of applications for issuance, suspension, and cancellation of certificates.

Certification Services Recipient - a natural, legal person, or an organisational unit without corporate existence that has concluded an agreement with KIR S.A. for the provision of certification services.

Subscriber - a natural person whose personal data have been entered into the certificate.

Private Key - data used for affixing a digital signature within the meaning of the Digital Signature Act.

Public Key - data used to verify the digital signature within the meaning of the provisions of the Digital Signature Act.

Key Pair - a private key and its accompanying public key.

3. APPLICATION SCOPE OF THE CERTIFICATION POLICY

The Policy is applied to issue and manage qualified certificates of public keys issued by KIR S.A. pursuant to an agreement for the provision of certification services concluded with a certification services recipient.

4. PROVISION OF CERTIFICATION SERVICES

4.1. Certification Services Provision Agreement

Certification services are provided pursuant to an agreement for provision of certification services hereinafter also referred to as the "Agreement".

The certification services provision agreement may be concluded with a natural person, a legal person, or an organisational unit without corporate existence. Based on the Agreement the certification services recipient shall indicate subscribers for whom it orders certificates.

4.2. Purpose of Certificates

Certificates that have been issued in accordance with this Policy shall be used for verification of secure digital signatures and identification of subscribers.

Certificates that are issued in accordance with the terms and conditions specified herein, are qualified certificates within the meaning of the Digital Signature Act of 18 September 2001 (Journal of Laws No. 130, item 1450). A secure digital signature that has been verified with the use of a qualified certificate has the same legal consequences as the own hand.

4.3. Obligations of KIR S.A.

KIR S.A. undertakes in particular to:

- issue certificates in response to properly submitted orders to KIR S.A. for certificates;
- reliably verify the identity of subscribers at the moment of delivering the private key carrier at the latest;
- reliably generate key pairs for subscribers on technical components that make up part of the safety device for affixing signatures held or to be used by subscribers;
- reliably verify requests for the issuance of certificates, in case they are not produced by KIR S.A.;
- reliably verify identities of persons requesting cancellation or suspension of a certificate and their rights to demand certificate suspension or cancellation;
- cancel or suspend certificates in response to a properly submitted request;
- publish a list of suspended or cancelled certificates at www.elektronicznypodpis.pl;
- protect subscribers' data;
- protect its private keys in accordance with this Policy;
- perform other obligations provided for under law.

Additional obligations of KIR S.A. may be stipulated by an Act of Law.

4.4. Obligations of the Subscriber

The Subscriber shall be in particular required to:

- use certificates in accordance with their purpose indicated in a given certificate;
- use certificates for the purpose of affixing secure digital signatures only within the certificate validity period indicated therein;
- protect its private key;

- advise about a certificate cancellation request in cases provided for in the Act, the Agreement, information that a subscriber has been provided with, or in the Policy.

The Agreement may specify a more detailed scope of the subscriber's responsibilities, provided it is known to it. The subscriber may also be advised of its detailed scope in writing or in information sent electronically.

4.5. Obligations of Trusted Parties

A trusted party shall be understood to mean a natural person, a legal person or an organisational unit without corporate existence who undertakes actions or any decision in trust to data signed with or certified electronically with the use of a public key contained in a certificate issued by KIR S.A. or a certification statement of KIR S.A.

Trusted parties shall be obliged to:

- use certificates in accordance with their purpose;
- verify the secure digital signature or electronic certificate at the moment of verification or at any convenient time;
- verify the signature or electronic certificate with the use of a secure device for verification of a digital signature while observing the relevant safety measures, including checks of the list of suspended and cancelled certificates, the lists of suspended and cancelled electronic certificates and the certification path.

4.6. Liability of KIR S.A.

KIR S.A. shall be held liable for any damage caused by failure to perform or default performance of its obligations within the scope of provided services, unless failure to perform or default performance of such obligations has been caused by the circumstances for which KIR S.A. is not held liable and which it could not have prevented despite exercising best efforts.

KIR S.A. shall not be held liable for damage resulting from the use of certificates outside the scope specified in the certification Policy that has been indicated in the certificate, including in particular, damage resulting from the excess of the highest threshold value of transactions, if such value has been disclosed in the certificate.

KIR S.A. shall not be held liable for damage resulting from untrue data disclosed in the certificate, entered upon request of a person affixing a digital signature or a certification services recipient.

KIR S.A. shall not be held liable for damage caused by outdated data entered into the certificate, if they were true at the time of certificate issuance.

KIR S.A. shall be held liable for storing and archiving data relating to the issuance, suspension and cancellation of a specific certificate.

KIR S.A. shall be held liable for security of infrastructure keys used in the process of issuing, suspending, and cancelling certificates.

The Agreement may specify a more detailed scope of liability incurred by KIR S.A.

4.7. Liability of the Certification Services Recipient

The certification services recipient shall be primarily held liable for the correctness and completeness of data disclosed in the request for certificate issuance and in the request for certificate suspension or cancellation.

The Agreement may specify a more detailed scope of liability incurred by the certification services recipient.

4.8. Financial Liability

The total liability under certification services provided by KIR S.A. may not exceed EUR 1,000,000. The amount of non-recurring compensation due under improper use of the certificate issued by KIR S.A. may not exceed EUR 250,000.

4.9. Fees

Fees for the provision of certification services are specified in the certification services price list published at the web site of KIR S.A. www.elektronicznypodpis.pl, the Agreement, an offer or any other document containing price proposals.

4.10. Audit

Within the scope specified in the Digital Signature Act of 18 2001, KIR S.A. shall be subject to audit by the minister competent for economy.

4.11. Compromise of the Private Key of KIR S.A.

In the event the private key of KIR S.A. that is used for signing certificates and the list of suspended and cancelled certificates has been compromised, all the hitherto issued certificates shall be automatically invalidated.

4.12 Discontinuance of Provision of Certification Services with Regard to Qualified Certificates by KIR S.A.

KIR S.A. shall have the right to discontinue issuance of qualified certificates. In such event all subscribers and certification services recipients shall be informed about it with a 90-day notice. Pursuant to the requirements of the Digital Signature Act, all qualified certificates that have been issued by KIR S.A. and related documents shall be delivered to a minister competent for economy or an entity indicated by the minister. Subscribers using certificates and prospective users shall have not right to make any claims against KIR S.A.

5. DESCRIPTION OF THE MANNER OF CREATING AND TRANSMITTING DATA THAT SHALL BE APPENDED WITH ELECTRONIC ATTESTATIONS

5.1. Secure Devices for Affixing Signatures

Secure devices for affixing digital signatures are used to generate certificates, certification authority certificates, lists of cancelled and suspended certificates. These devices are used only to provide certification services hereunder. Secure devices for affixing signatures used by KIR S.A. have a certificate that is required by law and statements made by equipment suppliers and manufacturers of software. Secure devices for affixing signatures that are used by KIR S.A. to generate certificates and lists of cancelled and suspended certificates are protected against unauthorised access. Access to devices is provided to authorised persons only. Each attempt at accessing a specific device, irrespective of its outcome, and actions related to generation of data used for affixing a digital signature or electronic attestation are monitored and recorded in the IT system used for provision of certification services.

Keys that protect data used for electronic attestation of certificates, lists of cancelled certificates and certification authority certificates are divided into parts according to a threshold pattern (m, n), where "m" is 2, while "n" is 5. Each of the parts is stored in separate key module held by persons authorised by KIR S.A. or in safes. Data for submitting electronic attestations are disclosed in full in a technical component only.

5.2. Infrastructure Keys

Infrastructure keys are used for:

- ensuring integrity of the transmission of data relating to the provision of certification services (requests for certificate issuance, suspension or cancellation, information on errors resulting from the process of certificate issuance, suspension or cancellation);
- ensuring integrity of event logs kept at KIR S.A.;
- ensuring integrity of data relating to the provision of certification services archived at KIR S.A.;
- securing access to the software and devices for affixing signatures used for the provision of certification services.

5.3. Generation of Certificates, Certification Authority Certificates and the Certificate Revocation Lists

KIR S.A. generates certificates and certificate revocation lists electronically confirming data contained in them with the use of secure devices for affixing signatures. KIR S.A. uses encryption algorithms for generating certificates and certificate revocation lists and the shortcut functions are specified in Section 14 of the Policy. The format and structure of certificates and certification authority certificates have been specified in Section 9 hereof. The format of certificate revocations lists has been specified in Section 10 hereof.

5.4. Generation of the Key Pair on Behalf of the Subscriber

KIR S.A. may generate a pair of keys on a technical component that makes up part of the secure device for affixing subscriber's signatures. In such case generation of data is performed on the basis of generators implemented in the technical component. A private key is not copied, or stored in any other way outside the technical component. Access to data stored on a technical component is secured against unauthorised use.

KIR S.A. may issue a certificate pursuant to a certification request prepared by a third party.

6. CERTIFICATE VALIDITY PERIOD

The maximum validity period of the subscriber's certificate is 2 years. The beginning of the certificate validity period may be from time to time determined with a certification services recipient or a subscriber. KIR S.A. may, upon request of a certification services recipient or subscriber, issue a certificate having any validity period of the subscriber's certificate, provided, however, that such period may not be longer than 2 years.

7. PRINCIPLES OF IDENTIFICATION AND AUTHENTICATION

This section governs the procedures of identification of subscribers who request KIR S.A. for certificate issuance and identification procedures applied to persons who request cancellation, suspension, or generation of another certificate.

7.1. Issuance of the First Certificate

Prior to the issuance of the first certificate for a specific subscriber a certification services recipient shall sign an agreement for provision of certification services and shall deliver to KIR S.A. an order that contains data necessary for certificate preparation. A sample of the order has been made available at the web site of KIR S.A. at www.elektronicznypodpis.pl.

Issuance to a subscriber of a carrier with a pair of keys to which KIR S.A. has issued a certificate shall require its personal appearance in an office of KIR S.A. or at the Partner's co-operating with KIR S.A. in certificate issuance.

To receive a certificate the subscriber shall have to present:

- an identity document;
- a document confirming assignment of the tax identification number (NIP), if it has been entered in the certificate;
- a file with a request for certificate issuance (if a pair of keys is generated individually by the subscriber).

KIR S.A. may expect presentation of other documents, in case of request for entering in the certificate subscriber's data other than the given name and surname and the personal identification number (PESEL) or the tax identification number (NIP).

In the event whereby the subscriber individually generates the pair of keys then presentation of the file with a certificate issuance request shall additionally be required for certificate issuance. The file contains a public key for which a certificate is to be generated, the subscriber's data, and an electronic signature generated with the use of a private key that makes up one pair with the public key.

7.2. Subscriber's Identifier

Based on the data received during registration, an identifier shall be created in accordance with the pattern below allowing identification of the subscriber related to the public key entered in the certificate.

The subscriber's identifier may contain the following elements:

Meaning	Value
name of country	Two-letter abbreviation of the country
common name	Subscriber's identifying name
surname	Subscriber's surname plus, possibly, its family name
given names	Subscriber's names
pseudonym	Name under which the subscriber is known or which it wishes to use
serial number	Subscriber's PESEL personal identification number and/or NIP tax identification number
organisation	Name of the certification services recipient with which the subscriber is connected
organisational unit	Name of the organisational unit with which the subscriber is connected
province	Name of the province
name of the town	Name of the town
postal address	Postal address

The subscriber's identifier shall be created on the basis of a subset of the above attributes provided that the identifier must be not empty and unique within a specific technical infrastructure at KIR S.A.

Certificates may be issued to various categories of subscribers. There is a minimum set of attributes defined under each category that are included in the subscriber's identifier:

- Category I - name of the country, surname, given name (names), serial number;
- Category II - name of the country, own name, serial number;

- Category III - name of the country, pseudonym.

KIR S.A. makes the reservation that it may decline issuance of the certificate that contains the subscriber's identifier in accordance with Category III.

7.3. Generation of Another Certificate

If the subscriber has a valid qualified certificate whose validity period is about to expire, the certification services recipient or subscriber, provided it has a relevant authorisation, may request generation of another qualified certificate.

When the subscriber collects the new certificate personally at the office of KIR S.A. or its partner verification of the subscriber's identity and its right to receive the certificate is performed in the same way as in case of the first certificate.

If the subscriber requests issuance of a new certificate using the Internet then its identity is verified on the basis of the current qualified certificate with which the request for certificate renewal has been signed. A detailed description of the certificate renewal process via the Internet is available at the web site of KIR S.A. at www.elektronicznypodpis.pl

7.4. Generation of Another Certification Following Cancellation of the Previous Certificate or Expiry of its Validity Period

The process of generating another certificate following cancellation of the previous one or generation of another certificate when the validity period of the certificate held by the subscriber has expired shall be performed in the same manner like in the case of request for the first certificate. Verification of the subscriber's identity shall be done in the same manner line in case of the first registration. If the certificate has not been cancelled due to a change of the subscriber's identity, then the new certificate may contain the previously assigned identifier.

7.5. Request for Certificate Cancellation or Suspension

The request for cancellation or suspension of a certificate shall be made by the subscriber or a third person, provided its data have been included in the certificate or another person, if it is so provided by the Act of Law, the Agreement or other obligations of KIR S.A.

The certificate that has been cancelled may not be then recognised as valid.

KIR S.A. shall cancel a certificate it has issued if:

- the certificate has been issued based on untrue or outdated data;
- default on the obligations provided for in the Digital Signature Act has been established;
- the subscriber has not provided the proper protection for data used for affixing a digital signature again unauthorised access;
- it has been requested by the subscriber or a third person indicated in the certificate or another person authorised to make such request;
- KIR S.A. has discontinued provision of services relating to certificates, and its rights and obligations shall not be taken over any other qualified entity providing certification services;
- it has been so requested by the minister competent for economy;
- the subscriber has lost its full capacity to enter into legal transactions.

In the event of a reasonable suspicion that there are allegations to cancel the qualified certificate, KIR S.A. shall suspend the certificate and immediately undertake actions necessary to clarify such doubts.

Authorisation to request cancellation of the certificate may be provided for in the agreement.

The agreement may provide for cases of certificate cancellation other than those listed above.

In a specific event, KIR S.A. may cancel the certificate upon request of the certification services recipient, even if it is not separately authorised to do so, if:

- the certificate has been issued pursuant to the Agreement concluded together with it, and
- it has presented and submitted to KIR S.A. written evidence of notifying the subscriber about its intention to request cancellation of the certificate at KIR S.A.

A request for certificate cancellation or suspension may be submitted:

- personally in the offices of KIR S.A., during business hours of KIR offices;
- by telephone to an info desk given on the web site of KIR S.A. at www.elektroniczypodpis.pl during business hours of the info desk;
- 24h at the web site of KIR S.A. at www.elektronicznypodpis.pl.

A request for certificate cancellation or suspension shall contain at least:

- the given name and surname of the requesting person;
- PESEL number of the requesting person or number and series of the identity document in the absence of PESEL number;
- data from the certificate (e.g. serial number, subscriber identifier, the period of validity);
- the reason for certificate status change.

A specimen of the request for certificate cancellation/suspension is available at the web site of KIR S.A. at www.elektronicznypodpis.pl.

Positive verification of the following shall be the basis for acceptance of the request for certificate cancellation or suspension submitted personally:

- identity of the person requesting cancellation/suspension, pursuant to a personal identity card or a passport and its right to cancel/suspend the certificate;
- data contained in the request for certificate cancellation/suspension.

Positive verification of the following shall be the basis for accepting the request for certificate cancellation/suspension submitted by telephone or via the Internet:

- the given name and surname of the requesting person;
- PESEL number of the requesting person or number and series of the identity document in the absence of PESEL number;
- data from the certificate (e.g. serial number, subscriber identifier, the period of validity);
- the password of the requesting person.

In the event whereby any data are incorrect, the request for cancellation/suspension of the certificate shall be rejected.

In the event of a reasonable suspicion that there are allegations to cancel the certificate, KIR S.A. shall suspend the certificate and immediately undertake actions necessary to clarify them.

In case of a request for suspension, when all the listed information is correct, KIR S.A. shall cancel the certificate for a period of 7 days.

7.5.1. Password for Certificate Suspension and Cancellation

The subscriber or another person authorised to request certificate cancellation/suspension shall be required to provide KIR S.A. with the passwords for certificate suspension and cancellation. The password, written down on a sheet of paper, shall be sealed in a non-transparent envelope. Failure to deliver the password shall make submission of the request to cancel or suspend the certificate via the Internet or by phone impossible.

The internal envelope shall additionally have the following information on it:

- the given name and surname of the authorised person;
- PESEL personal identification number.

In the event whereby the password is submitted by a person other than the subscriber, such person shall be obliged to quote the legal basis authorising it to request certificate cancellation or suspension.

Envelopes containing passwords shall be stored at KIR S.A., accessible only by persons who are authorised at KIR S.A. to suspend and cancel certificates.

The certification services recipient and the subscriber shall have the right to change the previously given passwords.

8. METHODS, THE MANNER OF CREATION AND PROVISION OF CERTIFICATES AND CERTIFICATE REVOCATION LISTS

8.1. Encryption Algorithms

KIR S.A. shall issue qualified certificates to subscribers for data used for signature verification that come from the following encryption algorithms:

- RSA;
- DSA;
- ECDSA;
- ECGDSA.

Identifiers and detailed minimum requirements for encryption algorithms have been specified in Attachment 6 to this Policy.

8.2. Processing of Certificate Issuance Requests

Having received an order for a certificate KIR S.A. shall proceed to issue the certificate pursuant to the data contained in the order. KIR S.A. shall generate a pair of keys and record the generated certificate on a technical component dedicated for the subscriber notified in the order.

An operator, who on behalf of KIR S.A. has confirmed the subscriber's identity at the time of certificate delivery to the subscriber, shall certify such confirmation with its own hand and giving its PESEL personal identification number on the confirmation.

8.3. Issuance of Another Certificate

In the event whereby the subscriber sends a request for the issuance of another certificate by means of telecom transmission, having received the request from the subscriber KIR S.A. shall check:

- if the subscriber has a valid certificate;
- if the data disclosed in the request are the same as in the valid certificate;
- the digital signatures appended with the request file.

KIR S.A. shall compare fields in the new request for certificate issuance with the current certificate. Fields that are to be compared include:

- the subscriber's identifier;
- the certification policy's identifier;
- application of the public key;
- the key length and algorithm.

In case of incompatibility, the request shall be rejected. The subscriber shall be informed about rejection of the request in a message about an error.

8.4. Issuance of the Certificate by KIR S.A.

By issuing a certificate, KIR S.A. shall electronically confirm the data used to verify the signature with the data about the subscriber, using a secure device for affixing signatures for this purpose. Electronic confirmation made by KIR S.A. below the certificate is generated with the use of an RSA encryption algorithm and an SHA-1 hash function the identifiers and characteristics of which are defined in Section 14 of the Policy. Data used for affixing electronic confirmation used by KIR S.A. have the length of2048 bits.

8.5. Certificate Cancellation

In the event of positive verification of the request for cancellation/suspension of the certificate KIR S.A. shall cancel/suspend the certificate. Cancellation/suspension of the certificate shall be done at the time the certificate is entered into the Certificate Revocation List. Information on cancellation/suspension of the certificate shall be put on the Certificate Revocation List (CRL). KIR S.A. shall notify the subscriber and, possibly, another person about cancellation/suspension of the certificate.

8.6. Change of the Certificate Status After Suspension

The certificate that has been suspended may next be cancelled or recognised as valid.

A change in the certificate status into a valid one may be made only upon request that has been personally submitted at KIR S.A. A specimen of the request for a status change is available at the web site of KIR S.A. at www.elektronicznypodpis.pl. The status change into invalid shall be made in the manner specified in Section 7.5 of this Policy.

If within 7 days as from the date of certificate suspension there has been no request submitted for the change of its status, then the certificate shall be cancelled.

If certificate cancellation is effected after its previous suspension, then the certificate cancellation date shall be the same as the certificate suspension date.

Verification of the identity of a person submitting the request for a status change of the suspended certificate and the request itself shall be performed in the same manner as in case of submission of a request for certificate cancellation/suspension.

8.7. Certificate Revocation Lists

Following certificate suspension or cancellation, KIR S.A. shall generate a certificate revocation list. The list shall contain:

- indication of the time of its creation;
- indication of the publication time of the next certificate revocation list;
- serial number of the suspended/cancelled certificate;
- indication of certificate suspension/cancellation time;

- reason for certificate suspension/cancellation.

After the previous certificate suspension has been cancelled, information about such certificate shall be removed from the certificate revocation list.

Information about cancelled certificates the validity period of which assigned by KIR S.A. has expired may not be removed from the certificate revocation list.

A detailed description of the structure of the certificate revocation list has been defined in Section 10 hereof.

8.8. Publications and Repository

Information concerning certification services provided by KIR S.A., information about the manner of Agreement conclusion, processing orders and renewals of certificates shall be made available to all interested parties at the web site of KIR S.A. at www.elektronicznypodpis.pl or in the offices of KIR S.A.

Certificate revocation lists shall be generated by KIR S.A. not less frequently than every 12 hours or after certificate suspension or cancellation. List updates shall be made not later than within 1 hour from certificate suspension or cancellation.

Current CRLs generated by KIR S.A. shall be available free of charge to all interested parties at the web site of KIR S.A. at www.elektronicznypodpis.pl

All certificates issued by KIR S.A. shall be stored at KIR S.A. at least throughout the period required under the Act.

9. DESCRIPTION OF ELECTRONIC STRUCTURES OF DATA INCLUDED IN CERTIFICATES

The contents of certificates and certification authority certificates generated by KIR S.A. have been described in ASN.1 notation specified in ISO/IEC 8824 - Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1) issued by International Organization for Standardization.

Certificates and certification authority certificates issued by KIR S.A. are made up of three parts:

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

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

Field Name	Meaning of the Field	Contents
version	certificate version marking	2
serialNumber	certificate serial number	unique certificate number under the qualified certificate issuance system
signature	identifier and parameters of the signature used by KIR S.A. for electronic certification of a given certificate	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identifier distinguishing an entity providing certification services that has issued a certificate	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= marking of the centre responsible for certificate generation; entry number in the register
validity	marking of the beginning and end of the validity of a certificate issued by KIR S.A.	certificate generation time and end of the certificate validity period down to a single second

subject	identifier of an entity related to the public key included in the certificate	value that is referred to in Section 7.2 of the Policy
subjectPublicKeyInfo	value of the public key together with an algorithm identifier with which the key is associated	the public key presented by the subscriber
extensions	standard and non-standard extensions	in accordance with the table below

Permitted extensions of the certificate have been shown in the table below:

Standard/ non-standard extension	**Extension name**	**Critical/ Non-critical**	**Meaning of the Extension**	**Contents**
Non-standard Extensions	*authorityKeyIdentifier*	non-critical	identifier of the public key used for verification of the issued certificate	identifier
	subjectKeyIdentifier	non-critical	identifier of the certificate containing the subscriber's specific public key	identifier
	keyUsage	critical	specifies the way the public key is used	nonRepudiation
	certificatePolicies	critical	specifies the certification policy in accordance with which a given certificate is issued	- identifier (1.2.616.113571.1.1) and the policy description - statement that the certificate is a qualified certificate issued by a qualified entity providing certification services
	subjectAltName	critical/ non-critical	another, supplementary name of the certificate owner, e.g. electronic mail address	Pursuant to the subscriber's indication or an entity signing an agreement for the provision of certification services
	basicConstraints	critical	allows checking whether the certificate owner is an end-user or an entity issuing certificates	empty sequence
	cRLDistributionPoints	non-critical	specifies addresses at which the current CRL is published	http://www.kir.com.pl/certyfikacja_kluczy/CRL_OZKx.crl lub http://www.elektronicznypodpis.pl/crl/crl_ozkx.crl; where x means marking of the centre/IT system of KIR S.A. responsible for certificate issuance
	subjectDirectoryAttributes	non-critical	additional attributes related to the certificate owner	this field may include: - the position; - the electronic mail address.
	qcStatement	critical	statement of the qualified certificate issuer	- a limit for a transaction that may be confirmed on a non-recurring basis with the certificate; - indication on whose behalf the certificate owner acts (permitted values: a) on its own behalf; b) as a representative of another natural person, a legal person, or an organisational unit without corporate existence; c) acting as a member of the authority or an authority of a legal persons or an organisational unit without corporate existence;

				d) as a public administration authority Presented declarations are not obligatory.

10. LIST OF ELECTRONIC STRUCTURES OF DATA INCLUDED IN THE REVOCATION LISTS

The contents of certificates and certification authority certificates generated by KIR S.A. have been described in ASN.1 notation specified in ISO/IEC 8824 - Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1) issued by International Organization for Standardization.

The certificate revocation list is made up of three parts:

- contents of the certificate *(tbsCertList);*
- identifier of the digital signature algorithm *(signatureAlgorithm);*
- digital signature *(signature).*

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

Field Name	Meaning of the Field	Contents
version	marking of the version of the certificate revocation list	1
signature	identifier and parameters of the signature used by KIR S.A. for electronic certification of a given certificate	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identifier distinguishing an entity providing certification services that has issued a certificate	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= marking of the centre responsible for certificate generation; entry number in the register
thisUpdate	issuance date of the certificate revocation list	CRL generation time down to a single second
nextUpdate	planned date of another list	planned time of another CRL down to a single second
revokedCertificates	certificate revocation list	- certificate serial number - data and time of certificate cancellation/suspension - certificate cancellation/suspension code
crlExtension	extensions of the certificate revocation list (status: non-critical)	- identifier of the entity's key to verify the signature under the certificate revocation list - number of the certificate revocation list

Permitted certificate cancellation/suspension codes include:

- *unspecified* - reason for certificate cancellation is not known;
- *keyCompromise* - certificate has been cancelled due to compromise or alleged compromise of data used for affixing the digital signature;
- *affiliationChanged* - certificate has been cancelled due to a change in the data included in the certificate;

- *superseded* - certificate has been cancelled because data used for affixing the digital signature have been superseded;
- *cessationOfOpertion* - certificate has been cancelled due to cessation of its use for the purpose for which it has been issued;
- *priviligeWithdrawn* - certificate has been cancelled due to a change in the data included in the certificate specifying the role of the certificate owner;
- *certificateHold* - certificate has been suspended.

In the event of the *certificateHold* code the certificate revocation list may contain additional non-critical extensions specifying possible instructions how to handle the suspended certificate:

- indication of the necessity to contact the certificate issuer to explain the reason for certificate suspension;
- indication of the obligatory rejection of the processed certificate.

11. MANNER OF MANAGING DOCUMENTS RELATING TO THE PROVISION OF CERTIFICATION SERVICES

KIR S.A. shall store and archive documents and electronic data, directly relating to the performed qualified certification services, in the manner that ensures safety of the stored documents and data. Access to documents and data relating to the provision of certification services shall be provided only to persons authorised by KIR S.A., who have been trained in personal data protection and admitted to their processing.

Documents and electronic data shall be kept in the personal data database of SZAFIR system that has been registered in the register maintained by the Inspector General for Personal Data Protection. Storage shall be carried in accordance with the use of technologies that ensure data integrity in accordance with the requirements provided for under the Personal Data Protection Act on August 29, 1997 (consolidated text, Journal 2002, no. 101, pos. 926, as amended), hereinafter referred to as the "Personal Data Protection Act ".

The following shall be stored and archived for a period of 20 years as from the moment of creation of a specific document and data:

- qualified certificates and certification authority certificates issued by KIR S.A.;
- certificate revocation lists for qualified certificates issued by KIR S.A.;
- lists of cancelled certification authority certificates issued by KIR S.A.;
- agreements for the provision of certification services;
- other documents in accordance with the legal requirements.

In the event whereby issuance of certificates by KIR S.A. has been discontinued, all the above-mentioned documents shall be delivered to the Minister of Economy or an entity indicated by it. Subscribers and recipients of certification services shall not incur any costs related to that.

12. CONFIDENTIALITY OF AND PERSONAL DATA PROTECTION

KIR S.A. shall ensure that all information relating to the provision of certification services that has not been explicitly recognised as not classified shall be subject to protection against its disclosure pursuant to the provisions established in the applicable regulations of law.

The following information held by KIR S.A. shall be subject to protection:

- internal procedures relating to the provision of certification services;

- private keys of the infrastructure of KIR S.A. used for the provision of certification services;
- passwords for certificate suspension and cancellation;
- archives, entries of the logs on functioning of the teleinformation system used for the provision of certification services;
- data on subscribers relating to the issuance, cancellation, and suspension of subscribers' certificates.

All certificates issued by KIR S.A. shall be subject to protection in accordance with the requirements of the regulations governing personal data protection.

Processing of personal data at KIR S.A. shall be performed in accordance with the principles specified in the Personal Data Protection Act and its secondary regulations. Each person for whom a certificate has been issued shall be entitled to rights provided for under the Personal Data Protection Act.

13. TECHNICAL AND ORGANISATIONAL PROTECTION

13.1. Physical Protection

Premises where data are processed that are related to the issuance, suspension, or cancellation of certificates and where certificates are generated, suspended and cancelled shall be subject to physical protection pursuant to the requirements of the Digital Signature Act and the Personal Data Protection Act. Applied protective measures shall protect against:

- premises being accessed by unauthorised persons;
- consequences of natural disasters and fortuitous events;
- fire;
- infrastructure failure;
- flooding, theft, burglary, and assault.

Applied measures of physical protection shall, among others, include:

- premises access control system;
- fire-protection system;
- class SA3 alarm system.

14.2. Technical Protection

13.2.1. Security of the Teletransmission Network

Access to the teleinformation system that is used for the provision of certification services, shall be secured in accordance with the requirements specified in the Digital Signature Act and the secondary regulations that follow from that Act.

13.2.2. Technical Components

When data necessary for affixing signatures by subscribers are generated by KIR S.A. such action is performed in technical components dedicated for that purpose. All data that allow re-engineering of the generated private key shall be automatically destroyed directly after the generation process of data for affixing digital signatures has been completed.

13.3. Back-up Centre

In the event of a failure of the primary centre that houses the infrastructure that is used for the provision of certification services thus making provision of certification services impossible, operations of the system shall be taken over by a back-up system located in the back-up location. In the event of a breakdown, the backup system shall take over operations relating to certificate cancellation, suspension, and publication of certificate revocation lists on an ongoing basis.

13.4. Security Relating to Staff

The staff who are involved in the provision of certification services have qualifications required under the Digital Signature Act, and in particular knowledge of the public key infrastructure and personal data processing.

14. IDENTIFIERS AND REQUIREMENTS FOR ENCRYPTION ALGORITHMS AND HASH FUNCTIONS

1.	RSA	{join-iso-ccitt(2) ds.(5) module (1) algo-rithm(8) encryptionAlgorithm(1) 1}	- minimum length of the key understood as module p*q is 1020 bits; - length of prime numbers p and q, making up the module may not differ by more than 30 bits.
2.	DSA	{iso(1) member-body(2) us(840) x9-57(10040)x9cm(4) 1}	- minimum length of the key understood as module p, it 1024 bits; - minimum length of parameter q, being the divisor of the number (p-1), is 160 bits.
3.	ECDSA	{iso(1) member-body(2) us(840) ansi-X9-62(10045) ecdsa-with-SHA1(1)}	- minimum length of parameter g is 160 bits; - minimum co-efficient r_0 is 10^4; - minimum class is 200.
4.	ECGDSA		- minimum length of parameter g is 160 bits; - minimum co-efficient r_0 is 10^4; - minimum class is 200.
5.	SHA-1	{iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWAlgo-rithm(2) 26}	
6.	RIPEMD-160	{iso(1) identifiedOrganization(3) tele-trust(36) algorithm(3) hashAlgorithm(2) 1}	