Krajowa Izba Rozliczeniowa S.A.

CERTIFICATION POLICY OF KIR S.A.
for
TRUSTED NON-QUALIFIED CERTIFICATES

Version 1.4

Document history

Version Number	Status	Date of Issue
1.0	Document approved by the Management Board of KIR S.A. – version effective until 30 September 2012	19 December 2011
1.1.	Document approved by the Management Board of KIR S.A. – version effective until 19 December 2013	1 October 2012
1.2.	Document approved by the Management Board of KIR S.A. – version effective until 24 April 2014	20 December 2013
1.3.	Document approved by the Management Board of KIR S.A. – version effective until 20 November 2014	18 April 2014
1.4.	Document approved by the Management Board of KIR S.A. – version effective as from 20 November 2014	13 November 2014

LIST OF CONTENTS

1. INTRODUCTION

The “Certification Policy of KIR S.A. for Trusted Non-Qualified Certificates”, hereinafter referred to as the “Policy” sets forth general rules for provision of certification services, including technical and organisational solutions that indicate the manner, the scope, and the terms and conditions for creating and applying certificates. The Policy defines the process of providing certification services and its participants. A detailed description is included in the “Code of Certification Procedure at KIR S.A. for Trusted Non-Qualified Certificates”, hereinafter referred to as the “Code”. Definitions of the terms used in the Policy have been defined in the Code.

Certification services concerning issuance of trusted non-qualified certificates, hereinafter referred to as “certificates” are provided by Krajowa Izba Rozliczeniowa S.A., hereinafter referred to as “KIR S.A.”, also by its field branches. A list of branches of KIR S.A. together with their office hours is available at the website of KIR S.A. www.elektronicznypodpis.pl.

2. APPLICATION SCOPE OF THE CERTIFICATION POLICY

The Policy is used for issuing and managing certificates issued by KIR S.A. A certificate shall be understood to mean an electronic file electronically certified by KIR S.A., in which the public key is assigned to the subscriber and allows its identification.

Certificates that have been issued in accordance with the Policy are not qualified certificates within the meaning of the Digital Signature Act of 18 September 2001 (Journal of Laws No. 130, item 1450, as amended). A digital signature verified with the use of such certificates does not have legal consequences equalling those of a hand-affixed signature.

Certificates described in the Policy are generated by the certification centre SZAFIR Trusted CA operated by KIR S.A.

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

Responsibility of KIR S.A., including financial, responsibility of the subscriber, the recipient of certification services, and the trusted party has been set forth in the Code.

2.1. Standard certificate

These certificates are used for protecting information sent electronically. They may be used for encrypting data and authenticating and identifying parties to communication. These certificates may be used for securing electronic mail and for logging into the systems or services, authorising the subscriber during establishment of secure connections.

In the process of issuing this type of certificates the operator KIR S.A. shall verify the subscriber's identity and the right to obtain such certificate. The certificate is delivered to the subscriber most often with a pair of keys generated on a carrier defined by the subscriber. Data included in the certificate allows identifying the subscriber that uses the certificate.

The Policy's distinguished name 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)
```

2.2. Certificate for signing codes

Certificates for signing codes are used for confirming authenticity and origins of binary codes. Based on the data included in the certificate it is possible for define the author or an entity that provides the code for a program or application.

In the process of issuing this type of certificates the operator KIR S.A. shall verify the subscriber's identity and the right to obtain such certificate and shall confirm reliability of the data entered into the certificate.

Data included in the certificate allow identification of an entity that uses the certificate.

The Policy's distinguished name for certificates for code signing looks as follows:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-kod(4)
```

2.3. VPN certificate

A VPN certificate allows identification of routers in both local and Internet networks. It allows creating virtual private networks by setting up encrypted connections.

In the process of issuing this type of certificates the operator KIR S.A. shall verify the subscriber's identity and its right to obtain a certificate. The process may also include verification, whether a network device is held by the recipient of certification services.

The Policy's distinguished name for VPN certificates looks as follows:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-VPN(5)
```

2.4. SSL certificate

An SSL certificate allows confirming authenticity of www servers and setting up secure connections using SSL and TSL protocols. A certificate may contain data of a single www server or associated servers within a single domain.

In the process of issuing this type of certificates the operator KIR S.A. shall verify the subscriber's identity and its right to obtain a certificate. The process includes verification, whether the server or domain are held by the recipient of certification services.

The Policy's distinguished name for SSL certificates looks as follows:

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

2.5. Test certificate

These certificates are used for checking co-operation with the system or the subscriber's IT solution.

In the process of issuing this type of certificates the operator KIR S.A. shall verify the subscriber's right to obtain such certificate. In case, when test certificate is to serve to examine the possibility of setting up secure connections, then process includes also verification, if www server or domain are at the disposal of recipient of certification services.

The Policy's distinguished name 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)

2.6. ELIXIR certificate

These certificates are used for protecting information transmitted within ELIXIR and EuroELIXIR systems operating by KIR S.A. They can be used for data encription and authentication and identification of communicating parties. Such certificates are issued only to participants in ELIXIR and EuroELIXIR systems.

In the process of issuing this type of certificates the operator KIR S.A. shall verify the subscriber's right to obtain such certificate. In case, when test certificate is to serve to examine the possibility of setting up secure connections, then process includes also verification, if www server or domain are at the disposal of recipient of certification services.

The Policy's distinguished name 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)
```

2.7. Standard Server Certificate

The Standard Server Certificate allows confirming authenticity of servers, including those operating in the organisation's internal network. The certificate may contain data of a single server or associated servers within a single domain.

In the process of certificate issuance, the operator KIR S.A. shall verify the subscriber's identity and its right to obtain such certificate. The process comprises verifications, whether the server or the domain shall be available for the recipient of certification services.

The Policy's identifier for Standard Server certificates 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).
```

3. PROVISION OF CERTIFICATION SERVICES

Conclusion of an agreement on provision of certification services consisting in the issuance of certificates, hereinafter also referred to as the "Agreement" shall be the basis for certificate issuance.

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

Placement of an order and verification of the subscriber's identity and his right to receive the certificate shall be the basis for issuance of the first and subsequent certificates, including certificate renewal. The manner of verifying identity and the right to receive the certificate shall depend on the certificate type and whether it is the first, or another certificate for a specific subscriber. Details concerning issuance of the certificate have been provided in the Code.

Revoking, suspending, or reactivating of the certificate may only be performed with regard to a certificate the operational period of which has not expired and it may be performed upon a request of the subscriber, an entity whose date is included in the certificate, the recipient of certification services, another authorised person or individually by KIR S.A. Details concerning a change in the certificate status have been provided in the Code.

4. SUBSCRIBER

The subscriber is primarily obliged to protect the private key it holds that is linked with the public key included in the certificate issued to it by KIR S.A. In the event of establishing or allegation that a private key's security has been compromised, the subscriber and the recipient of certification services shall be obliged to submit a request to KIR S.A. for suspension or revocation of the certificate.

5. TRUSTED PARTY

A trusted party shall be obliged to use certificates in accordance with their intended purpose and to verify an electronic or digital signature and signature data at the time of verification or at any other reliable moment using the list of suspended and revoked certificates for certificates and issuer certificates that are included in the proper certification path. Prior to undertaking any actions trusting in certificate the trusted party shall become acquainted with the provisions of the Code.

6. AMENDMENTS TO POLCIES, PUBLICATIONS

KIR S.A. shall have the right to periodic updates of the Policy. After KIR S.A. has approved amendments thereto, an updated Policy shall be disclosed at www.elektronicznypodpis.pl. Information concerning certification services provided by KIR S.A., including information about the manner in which Agreements are concluded, orders for and renewals of certificates is made available to all interested parties at the web site of KIR S.A. or outlets of KIR S.A.

Lists of suspended and revoked certificates are generated by KIR S.A. not less frequently than every 24 hours or following suspension or cancellation of the certificate. Lists are updated not less than within 1 hour from suspension or revocation of the certificate.

7. FEES

Fees for the provision of certification services are set forth in the price list of certification services disclosed at the website of www.elektronicznypodpis.pl, the Agreement, the offer, or any other document that contains price proposals.