Polska wersja tego dokumentu znajduje się tutaj

IMPORTANT NOTICE: This English translation is provided for reference. The only official version of this document is its original Polish version, available under the link above.

Signet Root CA Certificate Policy

Certificates of the Signet Root CA and Signet – Public CA Certification Authorities

version: 1.1

Document metric

Document title	Signet Root CA Certificate Policy - Certificates of the Signet Root CA and Signet – Public CA Certification Authorities
Version	1.1
Document status	approved
Approval date	02.06.2017
Number of pages	13

Approved by:

Version	Approver
1.1	Policy Approval Committee

Change history:

Version	Date	Comments
1.0	15.04.2013	The first version of the document.
1.1	02.06.2017	Document review and incorporation of eIDAS and Polish Trust Services Act stipulations. Document update due to organizational changes at Orange Polska S.A. (company name change in sec. 1.3; sec. 3.7). Introduction of SHA2 in certificates of operational Certificate Authorities (amendment to sec. 7.1.2, sec. 7.2).

Table of contents

1 Introduction

This Certificate Policy ("Policy") sets forth the detailed (in technical and organizational terms) methods, scopes, and conditions of protection, creation, and use of certificates issued by the superordinate certification authority Signet Root CA ("Root CA") .

Trust services described in the Policy are provided by Signet Certification Center (hereinafter referred to as Signet CC) managed by Orange Polska S.A. based in 02-326 Warsaw at Al. Jerozolimskie 160.

1.1 Policy ID

Policy title	Signet Root CA Certificate Policy - Certificates of the Signet Root CA and Signet – Public CA Certification Authorities
Reservation	Certificate issued in compliance with the "Signet Root CA Certificate Policy" document. Certificate issued by Signet Root CA in the CC Signet hierarchy.
Version	1.1
OID (Object Identifier)	1.3.6.1.4.1.27154.1.1.3.10.1.1.1
Implementing entity	Signet Root CA
Issue date	02.06.2017
Expiration date	Until revoked
Certification Practice Statement	CPS CC Signet 1.3.6.1.4.1.27154.1.1.1.1.1.2

1.2 Contact data

For more information on the Signet CC services, please contact us at:

Orange Polska S.A.
Signet Certification Center
ul. Piotra Skargi 56
03-516 Warszawa
E-mail: kontakt@signet.pl

2 Introduction

The Signet Certification Center is not a qualified trust service provider.

The Signet Certification Center operates in accordance with the generally applicable law in the Republic of Poland, in particular:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Off. J. of UE L 257 of 28.08.2014),
- Polish Trust Services and Electronic Identification Act of 5.09.2016 (JoL. 2013, sec. 1579).

This Policy is applicable to the process of certificate issuance by Root CA. Root CA issues certificates exclusively for Certification Authorities (CAs) providing trust services in the CC Signet hierarchy, including the self-signed certificate for Root CA.

The private key associated with the public key disclosed in a certificate issued by Root CA may be used by the certificate holder, i.e. the relevant CA, for the following purposes:

- digitally signing the issued certificates
- digitally signing the certificate revocation lists (CRL) containing information about certificate revocation
- digitally signing the infrastructure keys used for providing the trust services.

Signet Root CA does not issue certificates to end users.

CC Signet complies with the procedure of detailed verification of the information certified hereunder.

The Root CA information system can be accessed only through commands entered manually from the CA operator console. The system is not connected to any logical network extending beyond the room in which the system is installed.

3 Provisions of the Certificate Policy

3.1 Applicability

The certificates issued hereunder are issued only for Root CA and operating CAs directly subordinate to Root CA.

The certificates issued hereunder are not qualified certificated as defined in eIDAS Regulation.

The CA certificates confirm the organizational affiliation and possession of the private key corresponding to the public key disclosed in the certificate.

The certificate of Root CA is signed by Root CA itself (self-signed certificate).

The certificates of subordinate CAs are signed by Root CA.

3.2 Obligations of parties

3.2.1 Obligations of the subscriber

A Certification Authority which is a Root CA subscriber is obliged to generate its private key and then to store it securely.

The private key may be generated, used, authorized, access-controlled, and destroyed only in a hardware cryptographic module with a certified security level of at least FIPS 140-2 Level 3 (or equivalent under another test method).

Before using the certificate for the first time, the subscriber must verify the compliance of the certificate contents with the submitted request and verify the certification path. The Root CA certificate constituting the trust point in the verification process should be either obtained off-line, directly from CC Signet, or authenticated by comparing its hash value against the value obtained from CC Signet through a trusted channel.

In case of actual or suspected loss of control of the private key, the subscriber must notify the certificate issuer without delay.

Also, subscriber must notify the certificate issuer without delay about any change of the information disclosed in the certificate or submitted in the registration process.

The data published in the certificates issued by the CAs hereunder is verified according to the Certificate Policy applicable to the given CA.

3.2.2 Obligations of the relying party

The relying party is obliged to obtain the Root CA certificate in a secure manner and to verify its hash value against the value published by CC Signet. The methods of getting access to the CA certificates and to the information necessary to verify them are described in the Certification Practice Statement.

As part of establishing the trust in a service based on a certificate issued hereunder, the trusting party must properly verify the certificate. Within the verification process, the trusting party must verify the whole certification path. A certification path is an ordered sequence including CA certificates and the verified certificate, created so that each next certificate in the path can be verified as based on the previous certificate in the path, assuming the first certificate in the path as the trustworthy starting point. In the verification process, the trusting party should use the resources and procedures provided by Signet CC.

As a minimum, the relying party must verify the certification path and the current Root CA's CRL published by CC Signet.

The Certification Practice Statement defines the available services and methods of verification of the certificate validity. The relying party is obliged at least to use the Certificate Revocation List ("CRL") published by CC Signet and to verify the certification path from the trusted CA to the certificate issuer.

3.3 Responsibility

CC Signet is fully responsible for trustworthiness of information provided in the CA certificates issued by Root CA. Also, CC Signet is responsible for publishing current information about any revocations of certificates issued by Root CA.

3.4 Interpretation and the applicable law

To the extent of certificates issued hereunder, CC Signet operates in compliance with the Certification Practice Statement and with this Policy. In case of doubt, the provisions of those documents shall be interpreted in compliance with the superior legal regulations in force in Poland.

3.5 Publication and the Repository

Within its trust services, CC Signet publishes all certificates issued by Root CA in the publicly available information Repository.

Details of the organization of Repository and a description of methods for accessing the information can be found at http://www.signet.pl/repository .

In case of revocation of a CA certificate, the information to that effect is published without delay by creating a new CRL. CRLs are published by Root CA not less frequently than every 365 days.

3.6 Information protection

The information collected and processed hereunder is protected in compliance with the legal regulations.

CC Signet guarantees that any third party can access only the information disclosed in the certificate. The above guarantee does not apply to disclosing information on demand of competent authorities in compliance with the law.

3.7 Intellectual property rights

Proprietary rights to the Policy are owned exclusively by Orange Polska SA.

4 Identification and authentication

During contacts with Root CA, a subscriber is not subject to the standard procedures of certificate registration, renewal, suspension, and revocation defined in the Certification Practice Statement.

4.1 Registration

The process of registration of the Root CA subscribers, i.e. certification authorities of CC Signet, is compliant with the detailed internal procedures.

The procedures of Root CA subscriber registration are opinioned and approved by the CC Signet Policy Approval Committee.

4.2 Renewal of certificate

CC Signet does not provide any procedure for renewing a certificate issued hereunder. The issuance procedure of subsequent certificate is the same as for the first certificate.

4.3 Certificate suspension and revocation

CC Signet does not provide any procedure for suspending a certificate issued hereunder.

A certificate may be revoked, subject to verification of the requester's authorization to make such request.

Such verification includes identification and authentication of the requester in compliance with the detailed internal procedure of CC Signet.

5 Operational requirements

5.1 Certificate application

Certificates are issued only on request of a CA, subject to the conditions set forth herein.

Filing such a request is equivalent to the requester's consent to issuing the certificate.

The certificate may be issued only following positive verification of the request by Root CA under the registration process. Selected information from the request is disclosed in the certificate, depending on the certificate profile.

Root CA may supplement the information provided in the request to ensure compliance herewith or may reject the request, notifying the requester that the submitted information is not compliant herewith.

The issued certificate is delivered to the subscriber off-line, in person by the Root CA administrator, on a removable medium. Upon acceptance by the subscriber, the certificate is also published in the Repository.

5.2 Renewal of certificate

A period is envisaged before expiration of the Root CA certificate during which such certificate may not be used to certify new subscribers. For Root CA, such period is 2 years.

During that period, Root CA shall sign any new subscribers' certificates with a new private key.

It means that during that period, two Root CA certificates will be valid at the same time.

5.3 Acceptance of the certificate

Upon obtaining the certificate, the subscriber must verify the correctness of the data disclosed in the certificate and to notify the issuer without delay about any discrepancies or other defects of the certificate.

The obligations of both parties become effective at the moment of acceptance of the issued certificate by the subscriber.

In absence of any objections submitted to CC Signet by the subscriber within 24 hours of the certificate delivery, the certificate shall be deemed accepted.

5.4 Certificate suspension and revocation

CC Signet does not provide any procedure for suspending a certificate issued hereunder.

The subscriber may submit a request for certificate revocation. Such request shall be verified according to internal procedures of Root CA. If the verification is positive, the certificate shall be revoked.

Certificate revocation is irreversible.

A subscriber's certificate may also be revoked on a justified request of Root CA. Such request must be approved by the Policy Approval Committee.

6 Technical procedures of security control

Root CA, as a part of CC Signet, maintains a detailed register of events related to the service security.

The compliance of the CC Signet operations with the Certification Practice Statement, internal procedures, and this Policy, is periodically verified by an auditor independent from CC Signet.

6.1 Key pair generation

This policy requires that the RSA key pair (private key and public key) must be generated by the CA (the subscriber) holding the key.

The private keys of CAs subordinate to Root CA may be generated, used, authorized, access-controlled, and destroyed only in a hardware cryptographic module with a certified security level of at least FIPS 140-2 Level 3 (or equivalent under another test method).

The public key is delivered to Root CA in the form of a standard PKCS#10 request.

The CA holding the key shall be solely responsible for security of the private key.

6.2 Protection of the Root CA private keys

The private key of Root CA is generated, stored, and used only in the secure environment of a hardware cryptographic module with a certified security level of FIPS 140-2 Level 3. The private key leaves the secure environment of the hardware module only in the encrypted form, divided into parts remaining under control of several different persons, in compliance with the secret sharing procedures.

Additionally, the Root CA systems are protected physically against unauthorized access and electromagnetically against tapping and intrusion.

6.3 Security of the Root CA ICT systems

CC Signet provides its services using ICT systems protected in compliance with the Security Policy applicable for Orange Polska S.A.. The general procedures and systems used to protect the CC Signet resources are described in the Certification Practice Statement.

7 Profiles of the certificates and CRLs

This section describes the certificate profiles and the Certificate Revocation Lists (CRL) for certificates issued hereunder.

The 'Attribute' column includes the names of respective fields and attributes in accordance with X.509 standard in version 3 for the basic fields of certificate and CRL.

Attribute values in the **Issuer** and **Subject** fields are given in the order from the root of the directory tree, according to X.500 standard.

For the certificate and CRL extensions, the “Extension” column provides the extension/attribute name and the respective object identifier. The “Critical extension?” column identifies whether the given extension is critical.

The 'Value' column includes the values of respective fields and attributes, or descriptions of how the field value is specified and commends (beginning with #).

7.1 Certificate profiles

7.1.1 Signet Root CA certificate profile

The Signet Root CA certificate has the following structure:

Attribute	Value
version	2 # certificate consistent with X.509 version 3
serialNumber	# a number assigned by Signet Root CA, unique within the authority
signature	1.2.840.113549.1.1.11#SHA256 with RSA encryption (identifier of the algorithm used for electronic confirmation of the certificate)
issuer	C = PL, O = Telekomunikacja Polska S.A., OU = Signet Certification Authority, CN = Signet Root CA # distinguished name of the CA issuing the certificates hereunder
validity	# Certificate validity period
not before	# certificate issue date
not after	# certificate issue date + 25 years

subject	C = PL, O = Telekomunikacja Polska S.A., OU = Signet Certification Authority, CN = Signet Root CA # distinguished name of the CA certified hereunder
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 # rsaEncryption — identifier of the algorithm associated with the subscriber's public key
subjectPublicKey	# subscriber's public key (4096 bits)

The certificate contains the following extensions compliant with X.509:

Extension	Critical Extension	Value
keyUsage **2.5.29.15**	YES	06h
(0) digitalSignature	-	0
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	**-**	**1 # key for signing certificates**
(6) crlSign	**-**	**1 # key for signing CRLs**
(7) encipherOnly	-	0
(8) decipherOnly	-	0
authorityKeyIdentifier **2.5.29.35**	NO	-
keyIdentifier	-	# key identifier of the authority for verification of electronic certificate authentication
subjectKeyIdentifier **2.5.29.14**	NO	# identifier of the subscriber's key provided in the **subjectPublicKeyInfo** field
basicConstraints **2.5.29.19**	YES	-
CA	-	TRUE

7.1.2 Signet - Public CA cross-certificate profile

The Signet - Public CA certificate has the following structure:

Attribute	Value
version	2 # certificate consistent with X.509 version 3
serialNumber	# a number assigned by Signet Root CA, unique within the authority
signature	1.2.840.113549.1.1.11 #SHA256 with RSA encryption #identifier of the algorithm used for electronic signature of the certificate

Issuer	C = PL, O = Telekomunikacja Polska S.A., OU = Signet Certification Authority, CN = Signet Root CA # distinguished name of the CA issuing the certificates hereunder
validity	# Certificate validity period
not before	# certificate issue date
not after	# certificate issue date + 12 years
subject	C = PL, O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - Public CA # distinguished name of the CA certified hereunder
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 # rsaEncryption — identifier of the algorithm associated with the subscriber's public key
subjectPublicKey	# subscriber's public key (2,048 bits)

The certificate contains the following extensions compliant with X.509:

Extension	Critical Extension	Value
keyUsage **2.5.29.15**	YES	06h
(0) digitalSignature	-	0
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	**-**	**1 # key for signing certificates**
(6) crlSign	**-**	**1 # key for signing CRLs**
(7) encipherOnly	-	0
(8) decipherOnly	-	0
authorityKeyIdentifier **2.5.29.35**	NO	-
keyIdentifier	-	# key identifier of the authority for verification of electronic certificate authentication
authorityInfoAccess **1.3.6.1.5.5.7.1.1**	NO	#method of access to the issuer information
ocsp **1.3.6.1.5.5.7.48.1**	-	http://ocspca.signet.pl # HTTP URL of the Issuing CA's OCSP responder
calssuers **1.3.6.1.5.5.7.48.2**	-	http://www.signet.pl/repository/signetrootca/rootca_der.crt # HTTP URL of the Issuing CA's certificate
subjectKeyIdentifier **2.5.29.14**	NO	# identifier of the subscriber's key provided in the **subjectPublicKeyInfo** field

Extension	Critical Extension	Value
basicConstraints 2.5.29.19	YES	-
CA	-	TRUE
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://crl.signet.pl/public/rootca.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	2.5.29.32.0 #anyPolicy
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_signet_rootca_1_1.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certificate issued in compliance with the "Signet Root CA Certificate Policy" document. Certificate issued by Signet Root CA in the CC Signet hierarchy.

7.2 Certificate Revocation Lists (CRL)

The Certificate Revocation List has the following structure:

Attribute	Value
version	1 # list consistent with X.509 version 2
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption or 1.2.840.113549.1.1.11 #SHA256 with RSA encryption #identifier of the algorithm used for electronic authentication of CRL
issuer	C = PL O = Telekomunikacja Polska S.A., OU = Signet Certification Authority, CN = Signet Root CA # distinguished name of the CA issuing the certificates hereunder
thisUpdate	# date and time of list publishing (GMT in UTCTime format)
nextUpdate	# list publication date and time + 365 days (GMT in the UTCTime format)
revokedCertificates	# revoked certificate list with the following syntax:
serialNumber	# serial number of revoked certificate
revocationDate	# date and time of certificate revocation (GMT in UTCTime format)
reasonCode 2.5.29.21	# one of the revocation reason codes, as described below the table

ReasonCode field is a non-critical extension of the CRL **revokedCertificates** field, which allows to specify the reason for revocation or to indicate that the certificate is suspended.

The code can take the form of one of the following values:

- unspecified (0) - unspecified;
- keyCompromise (1) - key compromised;
- cACompromise (2) - CC key compromised;

- affiliationChanged (3) - change of the subscriber data
- superseded (4) - key superseded (renewed);
- cessationOfOperation (5) - certificate is no longer used for its purpose;

The Certificate Revocation List includes the following extensions:

Extension	Critical Extension	Value
cRLNumber 2.5.29.20	NO	# CRL number assigned by Signet Root CA
authorityKeyIdentifier 2.5.29.35	NO	-
keyIdentifier	-	# key identifier of the authority for verification of electronic authentication of CRL

Signet Root CA generates a new CRL not later than by 12 hours before the expiration time of the most recent list.