

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.

RootCA Certificate Policy

Certificates of the Signet-RootCA, TELEKOMUNIKACJA POLSKA CA, and Signet-PublicCA Certification Authorities

Table of contents

1	Preface	2
1.1	<i>Document identification</i>	2
1.2	<i>Change history</i>	2
1.3	<i>Contact data</i>	2
2	Introduction.....	3
3	Provisions of the Certification Policy	3
3.1	<i>Applicability</i>	3
3.2	<i>Obligations of the parties</i>	3
3.2.1	Obligations of the subscriber.....	3
3.2.2	Obligations of the relying party.....	4
3.3	<i>Responsibility</i>	4
3.4	<i>Interpretation and the applicable law</i>	4
3.5	<i>Publication and the Repository</i>	5
3.6	<i>Information protection</i>	5
3.7	<i>Intellectual property rights</i>	5
4	Identification and authentication	5
4.1	<i>Registration</i>	5
4.2	<i>Certificate renewal</i>	5
4.3	<i>Certificate suspension and revocation</i>	5
5	Operational requirements	6
5.1	<i>Certificate issue request</i>	6
5.2	<i>Certificate renewal</i>	6
5.3	<i>Certificate acceptance</i>	6
5.4	<i>Certificate suspension and revocation</i>	6
6	Technical procedures of security control	7
6.1	<i>Key pair generation</i>	7
6.2	<i>Protection of the RootCA private keys</i>	7
6.3	<i>Security of the RootCA computer systems</i>	7
7	Profiles of the certificates and CRLs	7
7.1	<i>Certificate profiles</i>	8
7.1.1	RootCA certificate profile	8
7.1.2	CA TELEKOMUNIKACJA POLSKA cross-certificate profile (secure corporate mail)	9
7.1.3	Signet-PublicCA certificate profile	11
7.2	<i>Certificate Revocation List (CRL) profile</i>	12

1 Preface

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 (“RootCA”) of CC Signet.

The certification services described herein are provided by the Signet Certification Center (“CC Signet”) operated by Telekomunikacja Polska S.A. with its registered office address of 00-672 Warszawa, ul. Twarda 18 (“TP”).

1.1 Document identification

Title	RootCA Certificate Policy — Certificates of the Signet-RootCA, CA TELEKOMUNIKACJA POLSKA, and Signet-PublicCA certification authorities
Reservation	Certificate issued in compliance with the “RootCA Certificate Policy” document. Certificate issued by RootCA in the CC Signet hierarchy.
Version	1.0
OID (Object Identifier)	1.3.6.1.4.1.27154.1.1.1.10.1.1.0
Implementing entity	CC Signet - RootCA
Issue Date	04.12.2006
Expiration date	Until revoked
Certification Practice Statement relevant to the Policy	Certification Practice Statement of the Signet Certification Center 1.3.6.1.4.1.27154.1.1.1.1.1.0

1.2 Change history

Version	Date	Change description
1.0	04.12.2006	The first version of the document.

1.3 Contact data

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

Telekomunikacja Polska S.A.
Centrum Certyfikacji Signet
ul. Czackiego 13/15
00-043 Warszawa
E-mail: kontakt@signet.pl

2 Introduction

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

The private key associated with the public key disclosed in a certificate issued by RootCA 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 certification services.

Signet-RootCA does not issue certificates to end users.

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

The RootCA computer 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 RootCA and operating CAs directly subordinate to RootCA.

The certificates issued hereunder constitute “certificate credentials” (*zaświadczenia certyfikacyjne*) for the purpose of the Polish Digital Signature Act of 18.09.2001, because they associate the digital-signature verification data (i.e. the public key) with the certification service provider.

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 RootCA is signed by RootCA itself (self-signed certificate).

The certificates of subordinate CAs are signed by RootCA.

3.2 Obligations of the parties

3.2.1 Obligations of the subscriber

A Certification Authority which is a RootCA 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 140-1 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 RootCA 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 RootCA 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 services based on a certificate issued hereunder, the relying party must properly verify the certificate. Within the verification process, the relying 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 signature of the previous certificate in the path, assuming the first certificate in the path as the trustworthy starting point. In the verification process, the relying party should use the resources and procedures provided by CC Signet.

As a minimum, the relying party must verify the certification path and the current RootCA'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 RootCA. Also, CC Signet is responsible for publishing current information about any revocations of certificates issued by RootCA.

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 certification services, CC Signet publishes all certificates issued by RootCA in the publicly available information Repository.

The detailed organization of the Repository and descriptions of the methods of accessing such information are available 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 RootCA 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

The proprietary rights to this Policy belong solely to Telekomunikacja Polska S.A.

4 Identification and authentication

During contacts with RootCA, 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 RootCA subscribers, i.e. certification authorities of CC Signet, is compliant with the detailed internal procedures.

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

4.2 Certificate renewal

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

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 issue request

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 RootCA under the registration process. Selected information from the request is disclosed in the certificate, depending on the certificate profile.

RootCA 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 RootCA administrator, on a magnetic medium. Upon acceptance by the subscriber, the certificate is also published in the Repository.

5.2 Certificate renewal

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

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

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

5.3 Certificate acceptance

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 RootCA. 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 RootCA. Such request must be approved by the Policy Approval Committee.

6 Technical procedures of security control

RootCA, 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 key pair (private key and public key) must be associated with the RSA algorithm and generated by the CA (the subscriber) holding the key.

The private keys of CAs subordinate to RootCA may be generated, used, authorized, access-controlled, and destroyed only in a hardware cryptographic module with a certified security level of at least FIPS 140-1 Level 3 (or equivalent under another test method).

The public key is delivered to RootCA 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 RootCA private keys

The private key of RootCA is generated, stored, and used only in the secure environment of a hardware cryptographic module with a certified security level of FIPS 140-1 Level 4. 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 RootCA systems are protected physically against unauthorized access and electromagnetically against tapping and intrusion.

6.3 Security of the RootCA computer systems

CC Signet provides its services using computer systems protected in compliance with the applicable Security Policy. 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 profiles of certificates and Certificate Revocation Lists (CRLs) issued hereunder.

For the basic fields of the certificate and CRL, the “Attribute” column provides the field/attribute name as per the standard X.509 v. 3.

The attribute values for the **Issuer** and **Subject** fields are provided in the order from the catalog tree root, as per the standard X.500.

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 provides the field/attribute value or, after the ‘#’ character, a description of the method of determining the field value, with comments.

7.1 Certificate profiles

7.1.1 RootCA certificate profile

The RootCA certificate has the following structure:

Attribute	Value
version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by Signet-RootCA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for digitally signing the certificate)
issuer	C = PL, O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - RootCA # distinguished name of the CA issuing certificates hereunder
validity	# certificate validity period
not before	# certificate issue date
not after	# certificate issue date + 25 years
subject	C = PL, O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - RootCA # 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

Extension	Critical extension	Value
(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	-	# identifier of the CA key, for verification of the certificate signature
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
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_rootca.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji RootCA". Certyfikat wystawiony przez RootCA w hierarchii CC Signet. #(Certificate issued in compliance with the "RootCA Certificate Policy" document. Certificate issued by RootCA in the CC Signet hierarchy.)

7.1.2 CA TELEKOMUNIKACJA POLSKA cross-certificate profile (secure corporate mail)

The CA TELEKOMUNIKACJA POLSKA certificate has the following structure:

Attribute	Value
version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by Signet-RootCA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for digitally signing the certificate)
Issuer	C = PL, O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - RootCA # distinguished name of the CA issuing certificates hereunder

validity	# certificate validity period
not before	# certificate issue date
not after	# certificate issue date + 15 years
subject	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet OU = CA TELEKOMUNIKACJA POLSKA # 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	-	# identifier of the CA key, for verification of the certificate signature
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
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/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.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_rootca.pdf

Extension	Critical extension	Value
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji RootCA". Certyfikat wystawiony przez RootCA w hierarchii CC Signet. #(Certificate issued in compliance with the "RootCA Certificate Policy" document. Certificate issued by RootCA in the CC Signet hierarchy.)

7.1.3 Signet-PublicCA certificate profile

The CC Signet - CA TP certificate has the following structure:

Attribute	Value
version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by Signet-RootCA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for digitally signing the certificate)
Issuer	C = PL, O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - RootCA # distinguished name of the CA issuing certificates hereunder
validity	# certificate validity period
not before	# certificate issue date
not after	# certificate issue date + 15 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

Extension	Critical extension	Value
(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	-	# identifier of the CA key, for verification of the certificate signature
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
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.signet.pl/crl/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_rootca.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji RootCA". Certyfikat wystawiony przez RootCA w hierarchii CC Signet. #(Certificate issued in compliance with the "RootCA Certificate Policy" document. Certificate issued by RootCA in the CC Signet hierarchy.)

7.2 Certificate Revocation List (CRL) profile

A CRL has the following structure:

Attribute	Value
version	1 # list compliant with X.509 v. 2
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for digitally signing the list)
issuer	C = PL O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = Signet - RootCA # distinguished name of the CA issuing certificates hereunder
thisUpdate	# list publication date and time (GMT in the UTCTime format)
nextUpdate	# list publication date and time + 365 days (GMT in the UTCTime format)
revokedCertificates	# list of revoked certificates, with the following syntax:

Attribute	Value
serialNumber	# serial number of the revoked certificate
revocationDate	# certificate revocation date and time (GMT in the UTCTime format)
reasonCode 2.5.29.21	# certificate revocation reason code, as per the description below

The **reasonCode** field is a non-critical extension of the **revokedCertificates** field, specifying the reason of revocation or indicating that the certificate is suspended. The following code values are allowed:

- unspecified (0) — unspecified
- keyCompromise (1) — the key has been compromised
- cACompromise (2) — the CC key has been compromised
- affiliationChanged (3) — change of the subscriber data
- superseded (4) — the key has been superseded (renewed)
- cessationOfOperation (5) — the certificate has ceased to be used for its purpose

The CRL contains the following extensions:

Extension	Critical extension	Value
cRLNumber 2.5.29.20	NO	# CRL number assigned by Signet-RootCA
authorityKeyIdentifier 2.5.29.35	NO	
keyIdentifier	-	# identifier of the CA key, for verification of the CRL signature

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