

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.

Certificate Policy

Signet CC Trusted Functions

Version 1.5

Document metric

Document title	Certificate Policy - Signet CC Trusted Functions
Reservation	Certificate issued in compliance with the "Certificate Policy – Signet CC Trusted Functions" document.
Version	1.5
Document status	approved
Approval date	14.11.2017
Number of pages	16

Approved by:

Version	Approver
1.5	Policy Approval Committee

Change history:

Version	Date	Change description
1.0	26.02.2007	The first version of the document.
1.1	24.11.2011	Taking into account changes in the defined trusted functions at Signet CC. Adding requirements for the application for electronic signature with the use of certificates issued in accordance with the Policy. Updating the link to the Certification Practice Statement version.
1.2	14.11.2013	Adding optional authorityInfoAccess extension in certificates. Increasing the minimum allowed length of RSA key to 2048 bits. Updating the effective Certification Practice Statement version. Updating the contact details.
1.3	12.06.2015	Updating the company name (change from "TELEKOMUNIKACJA POLSKA SA" to "Orange Polska SA") and contact information. Adding authorityInfoAccess = ocsp extension in issued certificates.
1.4	07.08.2017	Document review and incorporation of eIDAS and Polish Trust Services Act stipulations. Change of document template, document update due to change in organizational structure of OPL.
1.5	13.11.2017	User Notice, CDP and CPS link update.

Table of contents

1	Introduction.....	4
1.1	Policy identification	4
1.2	Change history	4
1.3	Service recipients and applicability of the certificates.....	4
1.4	Contact data.....	5
2	Basic principles of certification	5
2.1	Issued certificates.....	5
2.2	Obligations of parties	5
2.2.1	Obligations of the certificate holder	5
2.2.2	Obligations of the relying party	6
2.2.3	Obligations of the Signet Certification Center.....	6
2.3	Responsibilities of the Signet Certification Center.....	6
2.4	Fees	6
2.5	Publishing the issued certificates and revocation information	7
2.6	Information protection	7
2.7	Intellectual property rights.....	7
3	Identity verification and authentication	7
3.1	Registration	7
3.2	Key replacement.....	8
3.3	Suspending a certificate.....	8
3.4	Reinstating a certificate.....	8
3.5	Revocation of certificate.....	8
3.6	Renewal of certificate	8
4	Operational requirements	9
4.1	Submitting a certificate request	9
4.2	Issuing the certificate	9
4.3	Acceptance of the certificate	9
4.4	Suspending a certificate.....	9
4.5	Reinstating a certificate.....	9
4.6	Revocation of certificate.....	10
4.7	Renewal of certificate	10
4.8	Recovering the private key.....	10
5	Technical security measures	10
5.1	Key generation.....	10
5.2	Protection of keys belonging to the certificate holder	11
5.3	Activation of keys	11
5.4	Removal of keys	11
6	Ability to adapt the provisions of the Policy to the user requirements	11
7	Certificate profiles and Certificate Revocation Lists (CRL)	11
7.1	Certificate profiles	12
7.1.1	Authentication certificate profile.....	12
7.1.2	Encryption certificate profile.....	13
7.2	Certificate Revocation Lists (CRL)	15

1 Introduction

This Certificate Policy, hereinafter referred to as the Policy, sets out the specific (technical and organizational) solutions that indicate the method, scope and terms of protection, development and use of certificates for staff of Orange Polska SA who are employed at trusted functions in Signet Certification Center.

Certification 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 Warsaw at Al. Jerozolimskie 160, postcode 02-326.

1.1 Policy identification

Title	Certificate Policy - Signet CC Trusted Functions
Reservation	Certificate issued in compliance with the "Certificate Policy – Signet CC Trusted Functions" document.
Version	1.5
OID	1.3.6.1.4.1.27154.1.1.10.10.4.1.5
Implementing entity	Signet - Public CA
Issue date	14.11.2017
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 Change history

Unless stated otherwise, the changes apply to certificates issued after the date of issue of the particular Policy version. Each certificate issued by Signet Certification Center includes a link to the full text of the Policy in force for the particular certificate.

1.3 Service recipients and applicability of the certificates

Certificates issued in accordance with the Policy are intended for natural persons at one of trusted functions in Signet CC. The following trusted functions that can be held by one or more persons have been identified in Signet CC:

- Policy Approval Committee
- Security Inspector
- Public Key Infrastructure Administrator
- System Administrator
- Registration Inspector
- Registration Authority Operator
- Repository Administrator
- Archivist

The scope of responsibility and powers for each function is defined in the Certification Practice Statement and in internal documentation of Signet Certification Center.

Certificates used for the following purposes are issued under the Policy:

- sender authentication, ensuring the integrity of information sent by e-mail, website access authentication and electronic signatures;
- encryption of e-mail messages.

1.4 Contact data

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

Orange Polska S.A.
Centrum Certyfikacji Signet
ul. Piotra Skargi 56
03-516 Warszawa / POLAND
E-mail: kontakt@signet.pl

2 Basic principles of certification

2.1 Issued certificates

Signet Certificate Center issues the following types of certificates under the Policy:

- annual certificates used to authenticate senders of electronic messages, user authentication in relation to access to information systems and applications of Signet CC, ensuring the integrity of information sent by e-mail, and electronic signatures (hereinafter referred to as authentication certificates). Those certificates are assigned to a specific natural person;
- annual certificates used to encrypt electronic messages (hereinafter referred to as encryption certificates). Those certificates are assigned to a specific email address, and may be shared by a group of persons authorized use the address.

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

If an encryption certificate is assigned to an e-mail account accessible by one person only, that person is the holder of the certificate. The holder of encryption certificates shared by a group of persons is the Chairman of the Policy Approval Committee; the persons authorized to use the certificate are hereinafter referred to as users of encryption certificate.

2.2 Obligations of parties

2.2.1 Obligations of the certificate holder

Before receiving a certificate, the future holder or the user is required to read the Policy and Terms of Certification Services, to accept their conditions and to confirm it by personally signing a relevant statement.

The holder of authentication certificate is required for safely store the private key associated with the public key placed in the certificate.

The holder of authentication certificate is required to safely store the cryptographic token which contains the embedded private key associated with the public key placed in the certificate, and to protect the token PIN against disclosure.

The certificate holder should use electronic signature verified by a certificate issued in accordance with the Policy through an application that:

- uniquely identifies the data before signing by presenting their hash value,
- stores the history of activities related to saving of content.

Holders and users of encryption certificate are required for safely store their copies of the private key associated with the public key placed in the certificate. In particular, holders and users of certificates undertake to comply with the terms of use of cryptographic tokens, as set out in the relevant procedures.

Holders of certificates issued under the Policy are required to carefully store the passwords for certificate management and to protect them against disclosure.

- In the event of loss of control over the private key associated with the public key placed in the certificate, or a reasonable suspicion that such loss could take place, the certificate holder shall immediately notify the certificate issuer by submitting a request for revocation or suspension of the certificate.

2.2.2 Obligations of the relying party

The relying party must securely download the certificate of the trusted CA (Certification Authority) and verify its public key. 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. Certification path is an organized sequence of CA certificates and the certificate used to verify the signature, created in such a way that the data used to verify the electronic authentication and the name of the issuer of the first certificate on the path allow to show that for every two successive certificates the electronic authentication contained in the following one has been prepared by using the data for electronic authentication related to the previous one; the data used to verify the first electronic authentication are the trust point for the verifier. In the verification process, the trusting party should use the resources and procedures provided by Signet CC.

To determine the validity of a certificate, the relying party is required at least to use the OCSP service or the list of revoked certificates published by Signet CC and to verify the path of certificates from the trusted Certificate Authority to the authority that issued the certificate.

2.2.3 Obligations of the Signet Certification Center

Certification services are provided by Signet Certification Center in accordance with the laws in force on the territory of the Republic of Poland.

Signet Certification Center shall comply with the provisions of the Policy, in particular carry out the procedures of registration, renewal and revocation of certificates in accordance with the rules described in the Policy and Terms of Certification Services.

Signet Certification Center can store the private key associated with the public key placed in the encryption certificate. In this case, the storage period is at least 5 years from the date when the key is generated.

2.3 Responsibilities of the Signet Certification Center

Signet CC is responsible for consistency of the information contained in the certificate with the information provided in the certificate request.

Signet Certification Center is responsible for compliance with the applied procedures. In particular, Signet Control Center is responsible for publishing the current information about revocations of certificates in accordance with the Policy.

2.4 Fees

Both the services related to issuing and renewal of certificates associated with the Policy and the services related to revocation and suspension of certificates as well as provision of information about revocations are free of charge.

2.5 Publishing the issued certificates and revocation information

Signet Certification Center publishes lists of revoked and suspended certificates in a publicly accessible 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>.

Information about revocation, suspension and cancellation of suspension of certificates is published when a new Certificate Revocation List is created. The new Certificate Revocation List for certificates issued in accordance with the Policy is created within 1 hour after each revocation, suspension and cancellation of suspension of certificate, but no less frequently than every 24 hours.

Information about the validity of certificates issued under the Policy is also available through OCSP at <http://ocsp.signet.pl>.

2.6 Information protection

Information collected and processed under the Policy are protected to the extent and in the manner provided for by the applicable law. Information which could cause harm to the recipient of certification services or Signet Certification Center in the case of unauthorized disclosure is confidential.

Signet Certification Center ensures that it provides to third parties only the information contained in encryption certificates published in the Repository. The above restrictions do not apply to revealing information to competent Polish authorities in compliance with the law.

2.7 Intellectual property rights

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

3 Identity verification and authentication

This section describes the procedure of verification of identity of a person performing a certificate-management operation and the procedure of verification of such person's authorization to perform the given activity.

3.1 Registration

Registration, i.e. the process of acceptance and verification of a request for a new certificate, is conducted by the relevant Registration Authority at Signet Certification Center. A positively verified request requires approval by the Chairman of the Policy Approval Committee. If the registration process is completed positively, CA issues the requested certificate Signet - Public CA.

Registration of requests for encryption certificate shared by a group of persons is based on accepting a written request of the Chairman of the Policy Approval Committee; it contains the e-mail account address for which the certificate is to be issued and the list of its users. The list of certificate users may change in the certificate validity period at a written request of the Chairman of the Policy Approval Committee.

The following are VERIFIED during registration:

- authenticity of request;
- validity of the indicated e-mail address.

Registration of a request for authentication certificate is based on accepting a written request by the Manager of Signet Certificate Center; it contains the following information:

1. the name of the future certificate holder;
2. the name of the trusted function held in Signet Certification Center;

3. the e-mail account address that is to be placed in the certificate;
4. the name that uniquely identifies the certificate holder, which is to be placed in the certificate in the *subject* field, in the *pseudonym* attribute - applies to certificates which do not include the name of the certificate holder.

The following are VERIFIED during registration:

- authenticity of request;
- the fact that the future holder has the trusted function specified in the request - based on the information obtained from the person responsible for those functions in Signet Certification Center;
- the identity of the future holder - based on presented employee ID or identity document.

3.2 Key replacement

Keys can be replaced only by submitting a request for a new certificate with a new public key in accordance with the procedures described in Chapter 4.

3.3 Suspending a certificate

In the course of the certificate suspension procedure the applicant is authenticated and the authorization to submit requests for the operation is checked. Authentication and verification of authorization to submit requests involves:

- in the case of a request made by the certificate holder - verification of the applicant identity or verification of his or her electronic signature;
- in the case of a request made by a superior of the certificate holder - verification of professional relations between the applicant and the certificate holder.

3.4 Reinstating a certificate

Request for cancellation of suspension of authentication certificate may be made by the person at whose request the certificate was suspended. If the request for suspension of encryption certificate was submitted by its user, the request for cancellation of suspension may be made by the user or the certificate holder. The request must be made in person.

While submitting a request for cancellation of suspension the applicant must show his or her employee ID (or identity document) and clarify any doubts which were the basis for suspending the certificate to the person responsible for registration in Signet Certification Center.

3.5 Revocation of certificate

Revocation of certificate issued in accordance with the Policy requires submission of a proper request for revocation of certificate, authentication of applicant and verification of his or her authorization to make such a request.

Applicant authentication and verification of his or her authorization to revoke the certificate involves:

- in the case of a request made by the certificate holder - verification of the applicant identity or verification of his or her electronic signature;
- in the case of a request made by a superior of the certificate holder - verification of professional relations between the applicant and the certificate holder.

3.6 Renewal of certificate

Authentication and encryption certificates issued in accordance with the Policy may be renewed. Certificate is renewed by issuing a new certificate for a new public key, in which all the data are the same as in the renewed certificate, except for the validity period and the public key. Signet

Certification Center does not issue a new certificate for the public key contained in the certificate which is the basis for renewal.

A certificate may be renewed only within the validity period of the old certificate and only if the data the certificate is based upon remains unchanged. After the validity period or if the data is changed, the certificate holder must apply for a new certificate under the registration procedure contemplated in section 3.1 above.

4 Operational requirements

4.1 Submitting a certificate request

Certificates are issued under the Policy on the basis of a written request¹ of the future holder approved by the Chairman of the Policy Approval Committee.

4.2 Issuing the certificate

Certificates are issued no later than within 2 working days following the receipt of a valid request for certificate.

4.3 Acceptance of the certificate

Upon issuing the certificate, the holder must verify whether the certificate data is consistent with the certificate request.

If any discrepancy is detected, the certificate holder must notify Signet CC without delay, submit a request to revoke the defective certificate, and not use the private key associated with the public key contained in the certificate. In absence of any objections within 24 hours, the certificate shall be deemed verified against the data provided in the certificate request.

If the data contained in the certificate are inconsistent with the data indicated in the request, Signet Certification Center issues a new certificate with correct data to the holder free of charge.

If the certificate holder accepted the certificate containing data inconsistent with the data indicated in the request, he or she shall be responsible for any losses caused by the use of the certificate, if they occur as a result of the inconsistencies.

4.4 Suspending a certificate

Certificate issued under the Policy may be suspended. The requester must be authenticated as described in section 3.3 above. A positive verification of the rights to demand the suspension of certificate leads to the suspension of certificate.

If the suspension is not cancelled within 168 hours, the certificate shall be revoked.

4.5 Reinstating a certificate

Cancellation of suspension of certificate is possible only after personal appearance of the person who has requested for its suspension at Signet Certification Center.

¹ According to the Policy, a written form is considered to be a document bearing the personal signature of the applicant or his or her electronic signature verified by a qualified certificate or with an electronic signature verification certificate issued by a CA in the Signet Certification Center hierarchy. In particular, an e-mail message from the future user provided through the Chairman of the Policy Approval Committee with his electronic signature is a sufficient document.

If the request for suspension of encryption certificate was submitted by its user, the request for cancellation of suspension may be made by the user or the certificate holder.

The requester must be authenticated as described in section 3.4 above.

4.6 Revocation of certificate

A certificate issued hereunder may be revoked.

The requester must be authenticated as described in section 3.5 above. A positive verification of the rights to revoke the certificate leads to irreversible revocation of certificate.

Signet Certification Center can also revoke certificates in the following cases:

- receiving a written request for revocation from the holder or an authorized third party such as court, attorney, etc.,
- the information contained in the certificate has become invalid,
- if the certificate has been issued illegally or incorrectly, such as due to:
 - failure to meet the essential preconditions for certificate issuance,
 - providing false data for the certificate
 - errors in data entry or in the processing.

If there is a reasonable suspicion that there are reasons for revoking the certificate, Signet Certification Center shall suspend the validity of the certificate and notify the holder.

4.7 Renewal of certificate

Certificates issued under the Policy may be renewed. Certificates can be renewed only before the expiry date of the renewed certificate. After the validity period, the certificate holder must apply for a new certificate under the registration procedure contemplated in section 4.1 above 4.1.

A new key pair is generated under control of the holder during the certificate renewal; the public key is placed in the renewed certificate.

New key pairs are generated by Signet Certification Center during renewal of encryption certificates. The public key is placed in the renewed certificate, whereas the associated private key is archived.

4.8 Recovering the private key

At the request of the Head of Signet Certification Center or his or her superior, the private key associated with the key placed in an encryption certificate can be made available to a person indicated in the request. If the private key is provided to a person who is not employed at Signet Certification Center under employment contract, the request must be approved by the Director of level N +1, whose structure the Signet CC belongs to or by the Security Coordinator.

5 Technical security measures

5.1 Key generation

The Policy requires the key pair including the public key certified in accordance with the Policy to be associated with the RSA algorithm and to meet the following requirements:

- key length - (understood as a $p \cdot q$ module) - at least 2,048 bits;
- key generation method:
 - for authentication certificates - on a cryptographic token or card in Signet Certification Center;
 - for encryption certificates - the mechanisms of the Registration Office at Signet Certification Center.

5.2 Protection of keys belonging to the certificate holder

The certificate holder is solely responsible for protection of the private key used for authentication from the moment of its transfer to the certificate holder. The holder or user of encryption certificate is responsible for protecting the copy of the private key associated with the public key contained in the certificate located on his or her cryptographic card.

5.3 Activation of keys

The Policy does not provide for requirements in relation to the activation of private keys of the certificate holder.

5.4 Removal of keys

When an authentication certificate issued in accordance with the Policy expires, the private key associated with the public key placed in the certificate should be removed from the cryptographic token by using the software provided with the token, or the access to it should be locked in an irreversible way.

When an encryption certificate issued in accordance with the Policy expires, the private key associated with the public key placed in the certificate can be used to decrypt the data; however, it should still be stored in a secure manner. If the certificate holder no longer uses the private key, it can be removed or destroyed in the manner of his or her choosing.

If Signet Certification Center stores the copies of private keys associated with public keys placed in encryption certificates, the copy of the private key stored in a secure archive is destroyed no earlier than 5 years after generating the encryption certificate associated with the key.

6 Ability to adapt the provisions of the Policy to the user requirements

In justified cases, at the request of the future user approved by the Chairman of the Policy Approval Committee, a certificate issued under the Policy may have a profile with additional fields specified in the request, not listed in Chapter 7.1. None of the fields can be a critical extension within the meaning of x.509 certificate standard.

7 Certificate profiles and Certificate Revocation Lists (CRL)

Below are the profiles of certificates and Certificate Revocation Lists (CRL) issued in accordance with the Policy.

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 comments (beginning with #).

7.1 Certificate profiles

7.1.1 Authentication certificate profile

Authentication certificates issued in accordance with the Policy have the following structure:

Attribute	Value
version	2 # certificate consistent with X.509 version 3
serialNumber	# a number assigned by Signet - Public CA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption or 1.2.840.113549.1.1.11#SHA256 (identifier of the algorithm used for electronic confirmation of the certificate)
Issuer	C = PL, O = Telekomunikacja Polska, OU = Signet Certification Authority, CN= Signet - Public CA #specific name of the CA issuing the certificates hereunder
validity	# Certificate validity period
not before	# date and time of certificate issuance (GMT in UTCTime format)
not after	# date and time of certificate issuance + 365 days (GMT in UTCTime format)
subject	C = PL O = Telekomunikacja Polska. OU = Signet Certification Authority, CN = # first name and surname or name that uniquely identifies the certificate holder, specified in the request for certificate pseudonym = # repeated name that uniquely identifies the certificate holder, contained in the CN - if first name and surname are not provided (optional attribute)
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 #rsaEncryption - identifier of the algorithm associated with the public key of the certificate holder
subjectPublicKey	# public key of the certificate holder

Authentication certificates contain the following extensions in accordance with X.509 standard:

Extension	Critical Extension	Value
keyUsage 2.5.29.15	YES	80h # hexadecimal value
(0) digitalSignature	-	1 # key for electronic signature
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0

Signet Certification Center document

Extension	Critical Extension	Value
extendedKeyUsage 2.5.29.37	NO	1.3.6.1.5.5.7.3.2 #id-kp-clientAuth 1.3.6.1.5.5.7.3.4 #id-kp-emailProtection
authorityKeyIdentifier 2.5.29.35	NO	-
keyIdentifier	-	# key identifier of the authority for verification of electronic certificate authentication
authorityInfoAccess	NO	#method of access to the issuer information
accessMethod	-	1.3.6.1.5.5.7.48.2 # calssuers – issuer's certificate information
accessLocation	-	# URL address under which the issuer's CA certificate is available
accessMethod		1.3.6.1.5.5.7.48.1 # ocsp – OCSP service object identifier
accessLocation		# URL address of OCSP service
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder's key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-
cA	-	FALSE
subjectDirectoryAttributes 2.5.29.9	NO	
X520Title	-	# the name of the trusted function held by the certificate holder
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder
rfc822Name	-	# e-mail address of the certificate holder
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://crl.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NO	
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.4.1.5
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_zfccs_1_5.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Zaufane funkcje w CC Signet”. Nie jest kwalifikowanym certyfikatem w rozumieniu Rozp. eIDAS. #(Certificate issued in accordance with "Certificate Policy - Trusted Functions in Signet CC". It is not a qualified certificate within the meaning of eIDAS.)

7.1.2 Encryption certificate profile

Encryption certificates issued in accordance with the Policy have the following structure:

Attribute	Value
version	2 # certificate consistent with X.509 version 3
serialNumber	# a number assigned by Signet - Public CA, unique within the authority

Signet Certification Center document

signature	1.2.840.113549.1.1.5 #SHA1 or 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., OU = Signet Certification Authority, CN= Signet - Public CA #specific name of the CA issuing the certificates hereunder
validity	# Certificate validity period
not before	# date and time of certificate issuance (GMT in UTCTime format)
not after	# date and time of certificate issuance + 365 days (GMT in UTCTime format)
subject	C = PL O = Telekomunikacja Polska, OU = Signet Certification Authority, CN = # e-mail account address indicated in the request
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 #rsaEncryption - identifier of the algorithm associated with the public key of the certificate holder
subjectPublicKey	# public key of the certificate holder

Encryption certificates contain the following extensions in accordance with X.509 standard:

Extension	Critical Extension	Value
keyUsage 2.5.29.15	YES	30h # hexadecimal value
(0) digitalSignature	-	0
(1) nonRepudiation	-	0
(2) keyEncipherment	-	1 # key for key exchange
(3) dataEncipherment	-	1 # key for data encryption
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NO	1.3.6.1.5.5.7.3.4 #id-kp-emailProtection
authorityKeyIdentifier 2.5.29.35	NO	-
keyIdentifier	-	# key identifier of the authority for verification of electronic certificate authentication
authorityInfoAccess	NO	#method of access to the issuer information
accessMethod	-	1.3.6.1.5.5.7.48.2 # calssuers – issuer's certificate information
accessLocation	-	# URL address under which the issuer's CA certificate is available
accessMethod	-	1.3.6.1.5.5.7.48.1 # ocsp – OCSP service object identifier
accessLocation	-	# URL address of OCSP service

Extension	Critical Extension	Value
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder's key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-
cA	-	FALSE
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder
rfc822Name	-	# e-mail address of the certificate holder
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://crl.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.4.1.5
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_zfccs_1_5.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Zaufane funkcje w CC Signet”. Nie jest certyfikatem do weryfikacji podpisu elektronicznego. #(Certificate issued in compliance with the “Certificate Policy — Signet CC Trusted Functions” document. Not a certificate for verification of a digital signature.)

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 or 1.2.840.113549.1.1.11 #SHA256 with RSA encryption - specification of the algorithm used for electronic authentication of CRL
issuer	C = PL O = Telekomunikacja Polska, OU = Signet Certification Authority, CN= Signet - Public CA #specific name of the CA issuing the certificates hereunder
thisUpdate	# date and time of list publishing (GMT in UTCTime format)
nextUpdate	# date and time of list publishing + no more than 24 hours (GMT in 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;

Signet Certification Center document

- affiliationChanged (3) - change of data of certificate holder;
- superseded (4) - key superseded (renewed);
- cessationOfOperation (5) - certificate is no longer used for its purpose;
- certificateHold (6) - certificate has been suspended;

The Certificate Revocation List includes the following extensions:

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