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

Certificates for SSL servers

version 1.2

Document metric

Document title	Certificate Policy - Certificates for SSL Servers
Reservation	Certificate issued in compliance with the "Certificate Policy — Certificates for SSL servers" document. Compliant with CA/Browser Forum Baseline Requirements - subject identity validated. Not a qualified certificate for website authentication as defined by the eIDAS.
Version	1.2
Document status	approved
Approval date	31.10.2017
Number of pages	16

Approved by:

Version	Approver
1.1	Policy Approval Committee

Change history:

Version	Date	Change description
1.0	22.12.2016	The first version
1.0a	06.06.2017	Corrections in Chapter 7: adaptation of the CRL certificate profile to the current requirements of the CA Forum browser and RFC 6818:3. Pursuant to Decision 1/2017, the Chairperson of the Policy Approval Committee is not introduced the new version or OID.
1.1	04.08.2017	Change of document template, change of document number Chapter 2.3: Added provision about responsibilities in CC Signet. Chapter 2.2.3: Adding the provision about compliance CC Signet with the legal regulations currently in force in Poland Chapter 3.1: Changes in registration process description. The process has been modified by adding the new requirement relevant to requestor's office address and changing the name of the unit where the certificate is installed into optional . Chapter 3.1: Added the provision about IP verification ability out of www.ripe.net site. Chapter 3.1: Added the provision about the issuance of certificates which contain the new functional domain name. Chapter 4: Added the point „Approval of certificate request" Chapter 5.1: Added the new part about public key Change document template, change document number.
1.1	31.10.2017	Addresses correction in CDP and CPS

Table of contents

1 Introduction 4
1.1 Document 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 5
2.2.3 Obligations of the Signet Certification Center 6
2.3 Responsibilities of the Signet Certification Center 6
2.4 Fees 7
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 8
3.1 Registration 8
3.2 Key replacement 9
3.3 Suspension of certificate 9
3.4 Canceling a suspension of certificate 9
3.5 Revocation of certificate 9
3.6 Renewal of certificate 9
3.7 Certificate modification 10
4 Operational requirements 10
4.1 Submitting a certificate request 10
4.2 Approval of certificate request 10
4.3 Issuing the certificate 10
4.4 Acceptance of the certificate 10
4.5 Suspension of certificate 11
4.6 Cancelling a suspension of certificate 11
4.7 Revocation of certificate 11
4.8 Renewal of certificate 12
5 Technical security measures 12
5.1 Key generation 12
5.2 Protection of keys belonging to the certificate holder 12
5.3 Activation of keys 12
5.4 Removal of keys 12
6 Ability to adapt the provisions of the Policy to the user requirements 13
7 Certificate profiles and Certificate Revocation Lists (CRL) 13
7.1 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 creation, use and protection of certificates for securing SSL servers of natural and legal persons (companies), hereinafter referred to as "Subscribers", who entered into an agreement for services covered by the Policy, hereinafter referred to as "the Agreement", with 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 Document identification

Title	Certificate Policy - Certificates for SSL servers
Reservation	Certificate issued in compliance with the “Certificate Policy — Certificates for SSL servers" document. Compliant with CA/Browser Forum Baseline Requirements - subject identity validated. Not a qualified certificate for website authentication as defined by the eIDAS)
Version	1.2
OID	1.3.6.1.4.1.27154.1.1.10.10.5.1.2 2.23.140.1.2.2 (if certificate is issued for legal person) or 2.23.140.1.2.3 (if certificate is issued for natural person)
Implementing entity	Signet - Public CA
Issue date	31.10.2017
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, any change is applicable to the certificates issued after the date of the given version of the Policy. 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 under the Policy are intended to protect SSL servers of Subscribers. The recipient of services, i.e. the holder of certificate issued in accordance with the Policy, is a person with the e-mail address indicated in the request for certificate.

In particular, a SSL server administrator can be the certificate holder.

Certificates used for authentication of web servers and setting up a secure connection in SSL protocol are issued under the Policy.

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 Certification Center issues certificates used for authentication of web servers and setting up a secure connection in SSL protocol under the Policy.

The validity period of issued certificates is 1, 2 or 3 years.

The certificates issued hereunder are not qualified certificate for website authentication for the purposes of the Reg. (UE) No 910/2016 (hereinafter referred to as "eIDAS") and are not used to verify electronic signatures.

2.2 Obligations of parties

2.2.1 Obligations of the certificate holder

Before submitting a request for certificate, the future holder is required to read the Policy and the Certification Practice Statement. Submitting a request is equivalent to acceptance of the terms and conditions of the certificate issuance service hereunder.

The certificate holder must securely store the private key associated to the public key contained in his/her certificate.

If the certificate holder loses control of such private key or if the private key is revealed (or believed to be revealed), he/she must notify the certificate issuer without delay by submitting the certificate revocation request.

The certificate holder is responsible for trueness of the data provided in the certificate request.

The certificate holder shall notify the certificate issuer of any changes in the information contained in his or her certificate or indicated in the request for certificate.

2.2.2 Obligations of the relying party

The relying party must verify public key of trusted CA (Certification Authority). If during the verification the warning "Untrusted issuer" is displayed, then the Signet Root CA certificate must be downloaded and installed in trusted root certificate store of used system or application software. 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.

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

The certification services are provided by Signet CC in compliance with the legal regulations in force in Poland.

Signet Certificate declares that the SSL certificate profile of certificates issued under the Policy and every procedure of theirs life cycle management comply with requirements published in the current version of "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates" ("Requirements") document of CA/Browser Forum available at https://cabforum.org. In the case of a discrepancy between the provisions of the Policy and the Requirements , apply provisions of the Requirements.

Signet Certification Center shall act according to the Policy and the CPS, in particular carry out the procedures for management of certificate lifecycle in accordance with the rules described in the Policy, the Certification Practice Statement and the Agreement.

The current version of Requirements is fully compliant with the legal regulations currently in force in Poland. If any provision of the Requirements would conflict with the laws in force in Poland, Signet CC may modify it to the minimum extent required, modify the record in the Policy and notify the CA/Browser Forum of the conflict.

In accordance with the requirements of the Policy, certificates can be issued only pursuant to the Agreement (not applicable to certificates issued for internal purposes of Orange Polska SA).

Before entering into an agreement with a legal person, Signet Certification Center is required to unequivocally establish the existence of the company/institution on whose behalf the agreement is to be concluded and the authorizations of the natural person who represents it (based on the presented documents and/or publicly available reliable sources of information), in accordance with the procedures of customer verification of Orange Polska SA.

The Registration Authority Operator is responsible for carrying out the procedures of verification of identities of natural person requesting for certificates in accordance with the rules presented in the Certification Practice Statement, Chapter 3.1 "Pre-Registration" and Chapter 3 of the Policy.

Signet Certification Center provides the ability to verify the status of certificates issued under the Policy and requesting for the revocation or suspension on 24x7 basis.

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 CC is not responsible for trueness of the information provided in the certificate request. The scope and method of verification of the information provided in the certificate request are described in Section 3 below.

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 the Repository of Signet Certification Center in accordance with the Policy.

Signet CC may delegate to other entities or institutions some of its competencies in respect to registration of Service Recipients. In such case, the division of responsibility between Signet CC and such entity is regulated by the agreement. Signet CC is responsible to the Service Recipients for acts of such entities as for its own acts.

Notwithstanding any limitations on its liability to Certificate Holders and Relying Parties, Signet CC understands and acknowledges that the Application Software Suppliers who have a Signet Root CA Certificate distribution agreement in place with the Signet CC do not assume any obligation or potential liability for potential damages arising with connection of the Trust Services provided by Signet CC under the Policy.

2.4 Fees

Services related to the issuance of certificates under the Policy shall be paid for in accordance with the Agreement.

The certificate revocation services and the revocation information are free of charge.

2.5 Publishing the issued certificates and revocation information

Signet Certification Center publishes Certificate Revocation Lists 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/.

Certificates issued under the Policy shall not be published in the 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 and published immediately 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 laws applicable on the territory of the Republic of Poland. 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 does not provide any information obtained under the Policy to third parties. The obligation does not apply to requests for information made by the Polish authorities with proper powers under the applicable law.

Signet Certification Center does not provide certificates issued under the Policy to any third parties.

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 adoption and verification of a new certificate request is carried out by the Registration Authority serving Signet - Public CA in the PKI hierarchy Signet Certification Center. After successful completion of the registration process, the certificate is issued by the Certificate Authority.

The registration procedure requires the following data and documents to be provided to the Signet Certification Center:

a. address of the server (IP address and/or domain name) for which the certificate is requested

b. residence address of Applicant (at least country and location)

c. name of the organizational unit in which the server is installed (optional)

d. e-mail address (compliant with the SMTP standard) of the Administrator responsible for the server

e. the public key to be included in the certificate.

The following are verified during registration:

- the Applicant identity and residence address, based on the presented documents and/or publicly available reliable sources of information, in accordance with the procedures of customer verification of Orange Polska SA.
- the Applicant's authorizations to receive the particular type of certificate.
- the correctness of the server address:
  - in case of a certificate for a domain address:
    - verification whether the domain address is an web address (ends with one of the registered marks for *top-level domains*);
      and
    - verification whether the domain whose name is placed in the request for certificate is given to the Subscriber - based on the provided attestation issued by the organization managing the particular namespace, or on the basis of publicly accessible WHOIS services;

      Signet CC does not issue Certificates containing a new gTLD under consideration by ICANN. prior the new gTLD is approved for operation.
  - in case of a certificate for an IP address:
    - verification whether the specified web address does not belong to reserved addresses;
      and
    - verification whether the specified IP address belongs to the class assigned to the Subscriber - on the basis of information obtained in Réseaux IP Européens

(www.ripe.net), or other authorized Internet Registry appropriate for given region or country.

- possession of a private key associated with the key included in the request (the request must comply with the PKCS#10 standard).

Verification of access to the private key associated with the public key in the request for certificate involves checking whether the cryptographic syntax of the electronic request in PKCS#10 standard is correct.

The Applicant's access to the e-mail account address placed in the certificate is verified indirectly, by sending the issued certificate to the address.

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 4.1.

3.3 Suspension of certificate

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

Applicant authentication and verification of the authorization to submit a request for suspension of certificate issued under the Policy is carried out in accordance with the procedure stated in the Agreement.

3.4 Canceling a suspension of certificate

In the course of the procedure of cancellation of certificate suspension the applicant is authenticated and the authorization to submit requests for the operation is checked.

Applicant authentication and verification of the authorization to submit a request for cancellation of suspension of certificate issued under the Policy is carried out in accordance with the procedure stated in the Agreement.

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 the authorization to submit a request for revocation of certificate issued under the Policy is carried out in accordance with the procedure stated in the Agreement.

3.6 Renewal of certificate

Certificate is renewed by issuing a new certificate in which all the data are the same as in the renewed certificate, except for the validity period. Depending on technical conditions and the specificity of the renewal process for respective customers, Signet Certification Center can decide whether the renewal process is carried out for the currently used key pair, or whether it is necessary to generate a new key pair.

The conditions for renewal of certificates issued under the Policy should be set out in the Agreement.

3.7 Certificate modification

Data modification in issued certificate is not possible. If the change of the data contained in the certificate is requires, it is necessary to submit a request for revocation of the certificate and the request for a new certificate with the revised data, in accordance with the principles described above.

4 Operational requirements

4.1 Submitting a certificate request

The basis for issuing a certificate is as follows:

- Agreement signed by the Subscriber,
- Service Order signed by the Subscriber in accordance with the template set out in the Agreement,
- Request containing Applican's public key to be certified.

Additional requirements for registration may be specified in the Agreement.

The basis for the issuing a certificate for internal purposes of Orange Polska is a written request of the person authorized to represent the Business Owner of Signet CC.[1]

4.2 Approval of certificate request

Before certificate is issued, public key contained in the certificate request is checked against Signet CC internal register of previously revoked certificates and rejected requests. If public key matches the register, the request is rejected and the Applicant is obliged to submit new request with different public key.

4.3 Issuing the certificate

Before issuing a certificate, Signet CC checks whether the identification data and documents referred to in Sec. 3.1 above were obtained not earlier than 24 months before the certificate issuance date. If this is not the case, Signet CC requests / retrieves the current data.

Certificate is issued after Signet Certification Center receives the signed documents listed in Chapter 4.1 and no later than 3 working days after transfer of the correct request for certificate in an electronic form if the key pair is generated by the future certificate holder.

After the issuance the certificate is sent to its holder in the manner agreed by the Parties.

4.4 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

[1] For writing in this case it is also considered a signed electronic document verified with a qualified electronic signature certificate or with an electronic signature certificate issued by any Certificate Authority in the Signet Certification Centre hierarchy.

contained in the certificate. If the certificate holder fails to make reservations within 24 hour, it shall be considered to be the confirmation that the data in the certificate are consistent with the data in the 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 accepts a certificate with data inconsistent with the certificate request, he/she shall be responsible for any consequences of using such certificate, attributable to such inconsistency.

4.5 Suspension of 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. The certificate is suspended immediately after the successful completion of the verification of the request, but no later than within 24 hours of its submission. If during this time verification of the request carried out in accordance with the applicable procedure is not completed, the request is canceled.

The procedure of requesting for suspension of certificate issued under the Policy should be stated in the Agreement.

4.6 Cancelling a suspension of certificate

Suspension of certificate may be cancelled when a written request is received. The requester must be authenticated as described in section 3.4 above. A positive verification of the rights to demand the cancellation of suspension of certificate leads to cancellation of certificate suspension. The certificate suspension is cancelled immediately after the successful completion of the verification of the request, but no later than within 24 hours of its submission. If during this time verification of the request carried out in accordance with the applicable procedure is not completed, the request is canceled.

The procedure of requesting for cancelling the suspension of certificate issued under the Policy should be stated in the Agreement.

4.7 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. The certificate is revoked immediately after the successful completion of the verification of the request, but no later than within 24 hours of its submission. If during this time verification of the request carried out in accordance with the applicable procedure is not completed, Signet Certification Center suspends the certificate and then follows-up the investigation to determine the status of the request.

The procedure of requesting for revocation of certificate issued under the Policy should be stated in the Agreement.

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

- receiving a written request for revocation from an authorized third party;
- obtaining information that the data contained in the certificate have 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.

In case of a justified suspicion that the certificate should be revoked, Signet CC shall suspend the certificate, notify the certificate holder, and investigate the situation.

4.8 Renewal of certificate

A certificate issued hereunder may be renewed. Certificates may be renewed only when all of the following conditions are met:

1. The request is submitted before the current certificate expires,
2. The information content of the certificate contained in the registration data has not changed,
3. The current certificate has not been revoked,
4. The current keys are not registered as compromised keys.

If any of the above-mentioned conditions are not met, the certificate holder must apply for a new certificate in accordance with the registration procedure described in Chapter 3.1.

Detailed description of procedures of renewal of the certificate issued in accordance with the Policy should be set out in the Agreement.

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:

Minimal key length (modulus of p*q)	Key generation method	Key generating entity
2,048 bits	no requirements	Certificate holder

Signet CC confirms that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between 216+1 and 2256- 1. The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

5.2 Protection of keys belonging to the certificate holder

The certificate holder is responsible for the protection of the private key from the moment of its generation.

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

This Policy imposes no particular requirements on the method of destroying a private key associated with a public key included in a certificate issued hereunder.

When a certificate issued in accordance with the Policy expires and is not renewed, the private key associated with the public key contained in the certificate should be removed from the device in accordance with the instruction manual of standard software used to manage the device. Where possible, the private key should be destroyed.

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

If required by the nature of the provided service, the following changes of profiles of certificates issued under the Policy are possible at a written request of the responsible person indicated in the Agreement:

- changing the **cRLDistributionPoint** extension value into the value specified in the request for certificate, or adding new **distributionPoint** attributes;
- adding extensions not listed in Chapter 7.1, but specified in the request for certificate; the extension should be marked as non-critical.

Custom-profile certificates are issued after prior acceptance of the profile by the Policy Approval Committee and updating the Policy with the information about the modified profile.

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 commends (beginning with #).

7.1 Certificate profile

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	1.2.840.113549.1.1.11#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 # distinguished 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	# certificate issuance date and time + 1, 2 or 3 years (GMT in the UTCTime format)

subject	C = # two-letter country code of the Applicant in accordance with ISO 3166-1
	L = # the name of Applicant's location
	O = # the name of the organization specified in the request (if the registrant of the domain name or IP address is a natural person, it may contain his or her name and surname)
	OU = # the name of the organizational unit specified in the request (optional field)
	CN = # optional field, currently discouraged. If present, this field contain a single **iPAddress** or **dNSName** that is one of the values contained in the Certificate's **subjectAltName** extension.

subjectPublicKeyInfo	
algorithm	rsaEncryption # identifier of the algorithm associated with the certificate holder's public key
subjectPublicKey	# public key of the certificate holder

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

Extension	Critical Extension	Value
keyUsage **2.5.29.15**	YES	80h
(0) digitalSignature	**-**	**1 # key for electronic signature**
(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	1.3.6.1.5.5.7.3.1 #id-kp-serverAuth 1.3.6.1.5.5.7.3.2 #id-kp-clientAuth (optional - for a server operated as both a SSL client and SSL server,)
authorityKeyIdentifier **2.5.29.35**	NO	-
keyIdentifier	-	# identifier of the CA key, for verification of the certificate signature
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	# key identifier of the certificate holder, placed in the following field: subjectPublicKeyInfo
basicConstraints **2.5.29.19**	NO	-
cA	-	FALSE

Extension	Critical Extension	Value
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder[2]
iPAddress		# device IP address (optional field, may occur multiple times)
dNSName		# device domain name (optional field, may occur multiple times)
rfc822Name	-	# e-mail address of the certificate holder (may occur multiple times)
cRLDistributionPoint 2.5.29.31	NO	
distributionPoint	-	http://crl.signet.pl/crl/publicca.crl
certificatePolicies 2.5.29.32	NO	
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.10.10.5.1.2; 2.23.140.1.2.2 # compliant with CA/Browser Forum Baseline Requirements - organization validated. or 2.23.140.1.2.3 # compliant with CA/Browser Forum Baseline Requirements - individual validated.
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/docs/pc_ssl_1_2.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji – Certyfikaty dla serwerów SSL". Zgodność z podstawowymi wymogami CA/Browser Forum – tożsamość Podmiotu potwierdzona. (#Certificate issued in compliance with the "Certificate Policy — Certificates for SSL servers" document. Compliant with CA/Browser Forum Baseline Requirements - subject identity validated.)

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, OU = Signet Certification Authority, CN = Signet - Public CA # distinguished 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 and suspended certificate list with the following syntax:
serialNumber	# serial number of revoked certificate
revocationDate	# date and time of certificate revocation (GMT in UTCTime format)

[2] The extension must contain at least one **iPAddress** or **dNSName** field

Attribute	Value
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 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