



ORANGE POLSKA APPLICATION FOR THE MOZILLA ROOT CERTIFICATE PROGRAM UPDATED

General information about the CA's associated organization

CA Company Name	Signet Certification Center (Signet CC) “Signet CC” is a brand name of certification services provided by Orange S.A. (former Telekomunikacja Polska S.A – up to 31.12.2013);
Website URL	www.signet.pl (Signet CC website); www.orange.pl (company general website)
Organizational type	Signet CC is not an independent company or organization. It is an organizational unit in the structure of Orange Polska S.A. Orange Polska S.A is a public company traded on the Warsaw Stock Exchange, with a controlling stake owned by Orange S.A. (formerly France Télécom S.A.)
Primark Market / Customer Base	Orange Polska S.A. is a Polish national telecommunications provider. It operates the following services: PSTN, ISDN, GSM 900/1800 network, ADSL, IDSL, Frame Relay, ATM and Inmarsat. Provides retail services to end users and wholesale services for independent telecommunications operators. Parallel to its core business, the company rapidly increases the range of ICT services provided, including deployment of IT security solutions for its customers. Certification services of Signet Certification Center are offered as a security principle of more complex ICT services or as a standalone product.
Impact to Mozilla Users	Firefox is the most popular browser used by Internet users in Poland. On the other hand, Orange Polska is the leading Internet access service provider in Poland with the market share of ca. 1/3 for cable broadband and 1/4 for mobile access. Our customers, mostly using Firefox (or other products based on NSS by Mozilla), need to trust our Root CA to access and use certification services offered by Signet CC. By including our Root CA certificate into Mozilla products we want to give them confidence that our services are professional and recognized as trusted and also enable them to work seamlessly without disturbing messages about risks from untrusted Root CA. So, we want to show all our customers, external and internal, professional level of our services and high level of security. Public certification services of Signet CC include mainly SSL certificates. Implementation of S/MIME certificates in near future is not excluded.



Inclusion in other major browsers	Included into Microsoft Root Certificate Program since Nov. 2013 (please refer to http://social.technet.microsoft.com/wiki/contents/articles/20897.windows-and-windows-phone-8-ssl-root-certificate-program-november-2013.aspx). Applications for Apple Root Certificate Program and Android OS (Issue 71398 in android: http://code.google.com/p/android/issues/detail?id=71398) have been already sent.
CA Primary Point of Contact (POC)	Primary POC: Jerzy Rudowski (Signet CC Security Officer, Member of Policy Approval Committee) Orange Polska Centrum Certyfikacji Signet ul. Piotra Skargi 56 03-516 Warszawa POLAND POC direct email: jerzy.rudowski@orange.com Phone Number: +48 501 393 871 Alternative POC: Janusz Grabowski (Signet CC Security Business-Coordinator) Orange Polska Centrum Certyfikacji Signet ul. Piotra Skargi 56 03-516 Warszawa POLAND POC direct email: janusz.grabowski@orange.com Phone Number: +48 510 067 426 Email Alias: kontakt@signet.pl

Technical information about root certificate

Certificate Name	Signet Root CA
------------------	----------------

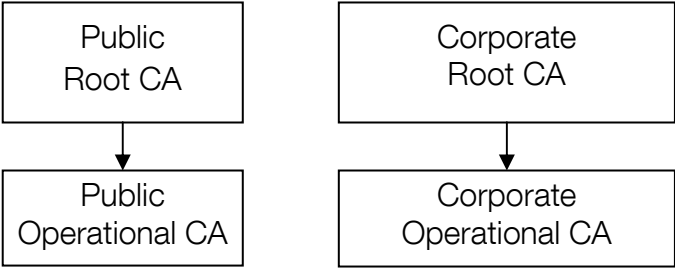


Certificate Issuer Field	CN = Signet Root CA OU = Signet Certification Authority O = Telekomunikacja Polska S.A. C = PL
Certificate Summary	This is the Root Certificate for Signet CC public certification services. This Root CA issued one certificate for operational CA. PKI of this undergoes periodic WebTrust audits. Currently only certificates for devices (SSL server or client certificates) are issued to public. S/MIME certificates may be introduced in the future. Issuing of code signing certificates is not planned. Establishing of other operational CAs is not excluded, but not expected in the near future.
Mozilla Applied Constraints	None
Root Cert URL	http://www.signet.pl/repository/signetrootca/rootca_der.crt ; http://www.signet.pl/repository/signetrootca/rootca_pem.crt
SHA1 Fingerprint	b2:bd:90:31:aa:6d:0e:14:f4:c5:7f:d5:48:25:8f:37:b1:fb:39:e4
Valid From	2013-05-06
Valid To	2038-05-06
Certificate Version	v3
Certificate Signature Algorithm	PKCS#1 SHA-256 with RSA encryption
Signing key parameters	RSA 4096 bits
Test Website URL (SSL) Example Certificate (non---SSL)	https://ssl-test.signet.pl ; test site linked to Signet CC repository
CRL URL	Signet Root CA CRL URL: http://crl.signet.pl/public/rootca.crl ; Signet – Public CA CRL URL for end-entity certificates: http://www.signet.pl/crl/publicca.crl Currently set value of nextUpdate field = thisUpdate +24h; (no more than 24h, as stated in Sec. 7.2 of every end-user Certificate Policy)



OCSP URL (Required now)	To be implemented in 2 nd half of 2014																										
Requested Trust Bits	Websites (SSL/TLS)																										
SSL Validation Type	OV – as stated in Secs. 2.23 and 3.1 of the “Certificate Policy – Certificates for Server and Devices” (http://www.signet.pl/docs/pc_csiu_1_7.pdf)																										
EV Policy OID(s)	N/A – not requesting EV treatment																										
Non-sequential serial numbers and entropy in cert	To be implemented soon (minor upgrade of PKI software of operational CA needed)																										
Response to Recent CA Communication(s)	<p>Responses to CA:Communications of May 2014:</p> <table border="1"> <thead> <tr> <th>Action #</th> <th>Response</th> <th>Relevant URL</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>#1: Current Audit</td> <td>N/A</td> <td>https://cert.webtrust.org/SealFile?seal=1665&file=pdf</td> <td>Signet root is not included yet</td> </tr> <tr> <td>#2: BR Audit</td> <td>E</td> <td></td> <td>Signet is not fully compliant with CAB Requirements at the moment</td> </tr> <tr> <td>#3: Test with mozilla::pkix</td> <td>A</td> <td></td> <td>Tested with Nightly v. 32.0a1</td> </tr> <tr> <td>#4: Behavior changes in mozilla::pkix</td> <td>B</td> <td></td> <td>Issue #2: (informative) Signet does include basicConstraints extension (non-critical) in end-user certificates, but its value FALSE (default) is not explicitly encoded. We will remove in the next PC version. Issues #4 & #6: OCSP responder is not implemented yet. We observe these issues during OCSP deployment later this year.</td> </tr> <tr> <td>#5: Disclosed subCA Certs</td> <td>A</td> <td>http://www.signet.pl/repository/index.html</td> <td></td> </tr> </tbody> </table>			Action #	Response	Relevant URL	Comment	#1: Current Audit	N/A	https://cert.webtrust.org/SealFile?seal=1665&file=pdf	Signet root is not included yet	#2: BR Audit	E		Signet is not fully compliant with CAB Requirements at the moment	#3: Test with mozilla::pkix	A		Tested with Nightly v. 32.0a1	#4: Behavior changes in mozilla::pkix	B		Issue #2: (informative) Signet does include basicConstraints extension (non-critical) in end-user certificates, but its value FALSE (default) is not explicitly encoded. We will remove in the next PC version. Issues #4 & #6: OCSP responder is not implemented yet. We observe these issues during OCSP deployment later this year.	#5: Disclosed subCA Certs	A	http://www.signet.pl/repository/index.html	
Action #	Response	Relevant URL	Comment																								
#1: Current Audit	N/A	https://cert.webtrust.org/SealFile?seal=1665&file=pdf	Signet root is not included yet																								
#2: BR Audit	E		Signet is not fully compliant with CAB Requirements at the moment																								
#3: Test with mozilla::pkix	A		Tested with Nightly v. 32.0a1																								
#4: Behavior changes in mozilla::pkix	B		Issue #2: (informative) Signet does include basicConstraints extension (non-critical) in end-user certificates, but its value FALSE (default) is not explicitly encoded. We will remove in the next PC version. Issues #4 & #6: OCSP responder is not implemented yet. We observe these issues during OCSP deployment later this year.																								
#5: Disclosed subCA Certs	A	http://www.signet.pl/repository/index.html																									

CA Hierarchy information for each root certificate

CA Hierarchy	<div style="text-align: center;">  <pre> graph TD PRCA[Public Root CA] --> POCA[Public Operational CA] CRCA[Corporate Root CA] --> COCA[Corporate Operational CA] </pre> </div> <p>The above diagram presents the hierarchy of Signet CC authorities. Signet CC Public Key Infrastructure providing services for external customers is separated from the infrastructure for corporate use. All PKIs of Signet CC is internally operated.</p> <p>The Root CA certificate of public infrastructure (“Signet Root CA”) is the subject of this application. Currently Signet CC operates one operational CA signed by this root (“Signet – Public CA”).</p>
Externally Operated SubCAs	Signet CC does not have any externally operated SubCAs.
Cross-Signing	Signet Root CA does not cross-sign with any other root certificates.
Technical Constraints on Third-party Issuers	Signet CC does not have any third party issuers



Verification Policies and Practices

<p>Policy Documentation</p>	<p>Document Repository: http://www.signet.pl/repository/index.html Language(s) that the documents are in: Website is generally in Polish. Key documents mentioned below are bilingual – Polish/English CPS: http://www.signet.pl/docs/kpc.pdf Certificate Policies: “Signet Root CA Certificate Policy: Certificates of the Signet Root CA and Signet – Public CA Certification Authorities” http://www.signet.pl/docs/pc_signet_rootca.pdf “Certificate Policy – Certificates for Servers and Devices” http://www.signet.pl/docs/pc_csiu_1_7.pdf “Certificate Policy – Trusted Functions in Signet CC” http://www.signet.pl/docs/pc_zfccs_1_2.pdf (personal certificates for Signet CC internal use) Relying Party Agreement: None. Obligations of relying party are listed in relevant Certificate Policies.</p>
<p>Audits</p>	<p>Audit Type: WebTrust for CAs v. 2.0 Auditor: Ernst & Young in Poland Auditor Website: http://www.ey.com/PL/pl/home</p> <p>Ernst & Young - WebTrust Accreditation Audit carried out in June 2011 Ernst & Young – WebTrust Periodic Audit carried out in December 2011 Ernst & Young – WebTrust Periodic Audit carried out in December 2012 WebTrust Seal: https://cert.webtrust.org/SealFile?seal=1465&file=pdf (2012-12-18) Ernst & Young – WebTrust Periodic Audit carried out in December 2013 WebTrust Seal: https://cert.webtrust.org/SealFile?seal=1665&file=pdf (2014-01-16)</p>
<p>Baseline Requirements (SSL)</p>	<p>The CA/Browser Forum Baseline Requirements” compliance statement can be found in “Certificates for Servers and Devices” CP (http://www.signet.pl/docs/pc_csiu_1_7.pdf).</p> <p>Please refer to Sec. 2.2.3: “Signet Certification Center declares that all procedures for lifecycle management of SSL certificates issued in accordance with the Policy are compatible with the current version of the requirements contained in the guidelines of CA/BROWSER FORUM published in the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" ("Requirements") available at http://www.cabforum.org. In the event of discrepancies between the provisions of the Policy and the above-mentioned Requirements, the provisions of the Requirements shall prevail.”</p> <p>When all requirements of CAB Forum will be fulfilled (OCSP, non-sequential long serial number), relevant audit will be conducted.</p>



SSL Verification Procedures	Signet CC apply OV verification (see below). Please refer to Sec. 3.1.10 of CPS (http://www.signet.pl/docs/kpc.pdf) and 3.1 of “Certificates for Servers and Devices” CP (http://www.signet.pl/docs/pc_csiu_1_7.pdf) (both bilingual – English/Polish) for rules of verifying domain names/IP addresses referenced in SSL certificates.
Organization Verification Procedures	Process of subscriber identity verification is described in Sec. 3 of CPS (http://www.signet.pl/docs/kpc.pdf) and Sec. 3 of “Certificates for Servers and Devices” CP (http://www.signet.pl/docs/pc_csiu_1_7.pdf) (both bilingual – English/Polish)
Email Address Verification Procedures	Not applicable, Signet CC is not requesting the Email trust bit.
Code Signing Subscriber Verification Procedures	Not applicable, Signet CC is not requesting the code signing trust bit.
Multi-factor Authentication	Multi-factor authentication including username, password and digital client certificates on PIN-protected electronic card or token are required to access Signet CC systems enabling certificate lifecycle management. Please refer to Sec 5.2 “Checking the organizational protections” of CPS (http://www.signet.pl/docs/kpc.pdf).
Network Security	Signet CC meets the requirements defined in CA/Browser Forum’s document “Network and Certificate System Security Requirements”. General statement about controlling network security can be found in Sec. 6.7 of CPS (http://www.signet.pl/docs/kpc.pdf)

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes, see above section.
CA Hierarchy	See Sec. “CA hierarchy Information” above.
Audit Criteria	See above section.
Document Handling of IDNs in CP/CPS	Actually, Signet CC has no special rules of handling IDNs. Although use of IDNs is not excluded, we do not expect to issue such certificates. If it really a problem, we disallow using of IDNs in the next version of CP.
Revocation of Compromised Certificates	Yes. Please refer to Sec. 4.6 of “Certificates for Servers and Devices” CP (http://www.signet.pl/docs/pc_csiu_1_7.pdf)
Verifying Domain Name Ownership	Please see above.

Verifying Email Address Control	Not applicable
Verifying Identity of Code Signing Certificate Subscriber	Not applicable
DNS names go in SAN	<p>Yes. All DNS names (and/or IP addresses) are placed into SAN extension. Please refer to SSL certificate profile in Sec. 7.1.1 of “Certificates for Servers and Devices” CP (http://www.signet.pl/docs/pc_csiu_1_7.pdf):</p> <p>“subject: C = # two-letter country code of the Applicant in accordance with ISO 3166-1 L = # the name of 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 = # the server address specified in the request; one of IPAddress or dNSName values contained in the subjectAltName extension” subjectAltName: # alternative name of the certificate holder’; The extension must contain at least one IPAddress or dNSName field.</p> <p> 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”</p>
Domain owned by a Natural Person	Signet CC does issue SSL certificates for domains owned by natural person. In such case, the name of this person is placed in the “O” attribute of “subject” field. Please see SSL certificate profile, as above.
OCSP	Not implemented yet.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	Signet CC does not issue DV certificates. Validity period of SSL certificates is 365 days.
Wildcard DV SSL certificates	Not applicable. Signet CC does not issue DV certificates.
Email Address Prefixes for DV Certs	Not applicable. Signet CC does not issue DV certificates.



Delegation of Domain / Email validation to third parties	Currently, Signet CC does not delegate any task connected with subscriber verification and/or certificate lifecycle management to external parties.
Issuing end entity certificates directly from root	Signet Root CA issue certificates exclusively for subordinate operational CAs (currently, only for Signet – Public CA). End entity certificates are never issued from root. Please refer to Sec. 2 of “Signet Root CA Certificate Policy” (http://www.signet.pl/docs/pc_signet_rootca.pdf)
Allowing external entities to operate subordinate CAs	Currently, Signet CC does not allow external entities to operate subordinate CAs.
Distributing generated private keys in PKCS#12 files	Not applicable. Signet CC does not generate key pairs for SSL certificate subscribers.
Certificates referencing hostnames or private IP addresses	Referencing of hostnames or private IP addresses in SSL certificates issued according to “Certificates for Servers and Devices” CP (http://www.signet.pl/docs/pc_csiu_1_7.pdf) is not allowed. Please, see Sec. 3.1 of the CP.
Issuing SSL Certificates for Internal Domains	Not allowed. Same as above.
OCSP Responses signed by a certificate under a different root	OCSP is not implemented yet.
CRL with critical CIDP Extension	Signet CC does not use partitioned CRLs (no CIDP extension). CRLs do not include any critical extension.
Generic names for CAs	CAs names used in Signet CC PKI are not generic.
Lack of Communication With End User	Signet CC contact information is publicly available.
Backdating the notBefore date	Due to system time synchronization feature and applied PKI software, the “notBefore” field value cannot be backdated.