Bugzilla ID: 1024418
Bugzilla Summary: Please add Signet Root CA certificate to NSS

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

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	http://www.signet.pl/ (Signet CC website) http://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 ITC services or as a standalone product.
Impact to Mozilla Users	Signet CC provides SSL certificates; with plans to also provide S/MIME certificates in the near future. Orange Polska is the leading Internet access service provider in Poland. Our customers, mostly using Firefox (or other products based on NSS), 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.
Inclusion in other major browsers	http://social.technet.microsoft.com/wiki/contents/articles/20897.windows-and-windows-phone-8-ssl-root-certificate-program-november-2013.aspx
CA Primary Point of Contact (POC)	Email Alias: kontakt@signet.pl Primary POC: Jerzy Rudowski (Signet CC Security Officer, Member of Policy Approval Committee) Email: jerzy.rudowski@orange.com Phone Number: +48 501 393 871 Alternative POC: Janusz Grabowski (Signet CC Security Business-Coordinator) Email: janusz.grabowski@orange.com Phone Number: +48 510 067 426

Technical information about each 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 root currently has one internally-operated subordinate CA that signs SSL server or client certificates. S/MIME certificates may be introduced in the future.
Root Cert URL	http://www.signet.pl/repository/signetrootca/rootca_der.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	3
Certificate Signature Algorithm	SHA-256
Signing key parameters	4096
Test Website URL (SSL)	https://ssl-test.signet.pl
CRL URL	Root CA CRL URL: http://crl.signet.pl/public/rootca.crl 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 for end-entity certs)	To be implemented in 2nd half of 2014 OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	OV
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)	https://wiki.mozilla.org/CA:Communications

CA Hierarchy information for each root certificate

CA Hierarchy	CPS section 1.9.1. Currently this root has one internally-operated subordinate CA, “Signet – Public CA”. Note: Signet CC operates another root certificate and CA hierarchy for internal use only. Signet CC Public Key Infrastructure providing services for external customers is separated from the infrastructure for corporate use.
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

Policy Documentation	Document Repository: http://www.signet.pl/repository/index.html Website is generally in Polish. Key documents are bilingual – Polish/English CPS: http://www.signet.pl/docs/kpc.pdf (bilingual) Root CA CP: http://www.signet.pl/docs/pc_signet_rootca.pdf (bilingual) SSL CP: http://www.signet.pl/docs/pc_csiu_1_7.pdf (in Polish only; English version will be posted soon)
Audits	Audit Type: WebTrust for CAs v. 2.0 Auditor: Ernst & Young Poland, http://www.ey.com/PL/pl/home WebTrust Seal: https://cert.webtrust.org/SealFile?seal=1665&file=pdf (2014-01-16)
Baseline Requirements (SSL)	URL to BR audit statement: Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results. https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Time_Frames_for_included_CAs_to_comply_with_the_new_policy “Any Certificate Authority being considered for root inclusion after February 15, 2013 must comply with Version 2.1 or later of Mozilla's CA Certificate Policy. This includes having a Baseline Requirements audit performed if the websites trust bit is to be enabled. Note that the CA's first Baseline Requirements audit may be a Point in Time audit.” SSL CP section 2.2.3: Centrum Certyfikacji Signet oświadcza, że wszelkie procedury zarządzania cyklem życia certyfikatów SSL wydawanych zgodnie z Polityką są zgodne z aktualną wersją wymagań zawartych w wytycznych organizacji CA/BROWSER FORUM opublikowanymi w dokumencie „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” („Wymagania”), dostępnym w witrynie http://www.cabforum.org. W przypadku wystąpienia rozbieżności pomiędzy zapisami Polityki a wspomnianych wyżej Wymagań, obowiązujące są zapisy Wymagań.
Organization Verification Procedures	CPS section 3 and SSL CP section 3. Please translate section 3 of the SSL CP into English.

SSL Verification Procedures	CPS section 3.1.10: If required by the nature of the server/device data to be included in the certificate, such data is subject to authentication. The authentication may be based on: - a relevant certificate submitted by the future holder - verification in publicly available databases published in the Internet by an authorized entity. The required verification process is presented in detail in the relevant Certificate Policy. SSL CP section 3.1: Please translate (into English) section 3.1 of "Certificates for Servers and Devices" CP (http://www.signet.pl/docs/pc_csiu_1_7.pdf) for rules of verifying domain names/IP addresses referenced in SSL certificates.
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	CPS section 5.2.2. 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.
Network Security	CPS section 6.7. Signet CC meets the requirements defined in CA/Browser Forum's document "Network and Certificate System Security Requirements".

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

Publicly Available CP and CPS	See above
CA Hierarchy	See above
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	Signet CC has no special rules of handling IDNs. Although use of IDNs is not excluded, we do not expect to issue such certificates.
Revocation of Compromised Certificates	SSL CP section 4.6
Verifying Domain Name Ownership	See above
Verifying Email Address Control	N/A
Verifying Identity of Code Signing Certificate Subscriber	N/A

DNS names go in SAN	All DNS names (and/or IP addresses) are placed into SAN extension. SSL CP section 7.1.1.
	Subject: (please correct this translation)
	C = # two-letter country code of the Applicant, according to ISO 3166-1
	L = # the name of the village
	O = # name of the organization included in the application (if the administrator of the domain name or IP address of a natural person, it may contain the name and surname)
	OU = # the name of the organizational unit included in the application (optional field)
	CN = # server address specified in the application; one of the IPaddress or dNSName contained in the

	subjectAltName extension subjectAltName: # Alternative name of the certificate holder The extension must contain at least one field ipaddress or dNSName iPAddress: # IP address of the device (optional field, may occur repeatedly) dNSName: # Domain name of the device (optional field, may occur repeatedly) rvd822Name: # E-mail address of the certificate holder
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.
OCSP	See above

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 roots	End entity certificates are never issued from root. Section 2 of 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 section 3.1 of SSL CP.
Issuing SSL Certificates for Internal Domains	Not allowed. Section 3.1 of SSL CP.
OCSP Responses signed by a certificate under a different root	See above
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 Users	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.