Print this page

Mozilla - CA Program

Case Information

Case Number	00000034	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Orange Polska S.A.	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Include Orange Polska's root cert	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1024418

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	http://www.signet.pl/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)	Signet CC 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.)	**Verified?**	Verified
Geographic Focus	Poland	**Verified?**	Not Verified
Primary Market / Customer Base	“Signet CC” is a brand name of certification services provided by Orange S.A.	**Verified?**	Verified
Impact to Mozilla Users	Orange Polska is the leading Internet access service provider in Poland	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	NEED: CP/CPS sections meeting https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#OCSP 1. Publicly Available CP and CPS: CPS section 1.6 2. Audit Criteria: Audits provided 3. Revocation of Compromised Certificates: Servers and Devices CP section 4.5 4. Verifying Domain Name Ownership: Servers and Devices CP section 3.1 5. Verifying Email Address Control: Not requesting email trust bit	**Verified?**	Need Response From CA

6. DNS names go in SAN: Servers and Devices CP section 7.1.1
7. OCSP: ??? It is not clear to me if Signet meets this requirement, and where to find this in their CP/CPS.
8. Network Security Controls: CPS section 6.7

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	NEED: CP/CPS sections meeting https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices#Delegation_of_Domain_.2F_Email_Validation_to_Third_Parties 1. Long-lived Certificates: Servers and Devices CP section 7.1.1 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: Servers and Devices CP section 3.1 3. Issuing End Entity Certificates Directly From Roots: CPS section 1.8.1 4. Distributing Generated Private Keys in PKCS#12 Files: Servers and Devices CP section 3.1 5. Certificates Referencing Local Names or Private IP Addresses: Servers and Devices CP section 3.1 6. Issuing SSL Certificates for .int Domains: Servers and Devices CP section 3.1 7. OCSP Responses Signed by a Certificate Under a Different Root: no 8. Issuance of SHA-1 Certificates: Servers and Devices CP section 7.1.1 9. Delegation of Domain / Email Validation to Third Parties: Unclear	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Signet Root CA	**Root Case No**	R00000042
Request Status	Information Verification In Process	**Case Number**	00000034

Certificate Data

Certificate Issuer Common Name	Signet Root CA
O From Issuer Field	Telekomunikacja Polska S.A.
OU From Issuer Field	Signet Certification Authority
Valid From	2013 May 06
Valid To	2038 May 06
Certificate Serial Number	01
Subject	CN=Signet Root CA, OU=Signet Certification Authority, O=Telekomunikacja Polska S.A., C=PL
Signature Hash Algorithm	sha256WithRSAEncryption

Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	B2:BD:90:31:AA:6D:0E:14:F4:C5:7F:D5:48:25:8F:37:B1:FB:39:E4
SHA-256 Fingerprint	72:86:CE:24:9F:E9:E3:2B:D4:75:22:57:C1:7C:D8:F6:99:1A:9C:1E:6F:1A:3C:C7:33:04:ED:02:3E:6A:E4:EB
Certificate ID	09:79:EA:A3:A8:06:99:09:6C:41:2D:58:0F:DF:73:EB:A0:98:EF:9A:32:CD:00:DD:69:15:87:EC:AE:3D:3A:DF
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This 'Signet Root CA' is operated by Signet Certification Center, which is managed by Orange Polska. This root currently has one internally-operated subCA, Signet - Public CA'.	**Verified?**	Verified
Root Certificate Download URL	http://www.signet.pl/repository/signetrootca/rootca_der.crt	**Verified?**	Verified
CRL URL(s)	http://crl.signet.pl/public/rootca.crl http://www.signet.pl/crl/publicca.crl Servers and Devices CP section 7.2: nextUpdate set to no more than 24 hours after thisUpdate	**Verified?**	Verified
OCSP URL(s)	http://ocsp.signet.pl	**Verified?**	Verified
Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://ssl-test.signet.pl/	**Verified?**	Verified
Test Website - Expired	https://ssl-test.signet.pl:8443/		
Test Website - Revoked	https://ssl-test.signet.pl:9443/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/ssl-test.signet.pl NEED CA to Fix errors: http://ocsp.signet.pl (GET) Unexpected HTTP response: 404 Not Found Error making OCSP request: Post http://ocsp.signet.pl: dial tcp: lookup ocsp.signet.pl on 169.254.169.250:53: no such host	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	https://crt.sh/?caid=5677&opt=cablint,zlint,x509lint&minNotBefore=2013-06-13 NEED CA to fix errors: subCA cert missing required OCSP info in authorityInformationAccess extension.	**Verified?**	Need Response From CA

Test Website Lint Test	See above	**Verified?**	Verified
EV Tested		**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	This root currently has one internally-operated subCA, Signet - Public CA'.	**Verified?**	Verified
Externally Operated SubCAs	Externally-operated subCAs are allowed per CPS section 1.8.1. NEED: It is not clear in the CPS if external subCAs are capable of issuing SSL/TLS certs, and if they are what rules they must follow (e.g. BRs, audits, etc.)	**Verified?**	Need Response From CA
Cross Signing	Currently none. See above.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Externally-operated RAs are allowed, see CPS section 1.8.1.4. NEED: CP/CPS need to clearly state the requirements for RAs, especially if they are able to verify the domain names to be included in SSL certs.	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	Documents are in Polish, with some translated into English.	**Verified?**	Verified
CA Document Repository	http://www.signet.pl/repository/	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.signet.pl/docs/pc_csiu_1_8.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.signet.pl/docs/kpc.pdf	**Verified?**	Verified
Other Relevant Documents	Servers and Devices CP: http://www.signet.pl/docs/pc_csiu_1_8.pdf Trusted Functions CP: http://www.signet.pl/docs/pc_zfccs_1_3.pdf RootCA CP: http://www.signet.pl/docs/pc_signet_rootca_1_1.pdf	**Verified?**	Verified
Auditor (New)	Ernst & Young, LLP	**Verified?**	Verified
Auditor Location (New)	Poland	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2236&file=pdf NEED: Make sure your 2018 Audit Statements meet Mozilla's requirements: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy#public-audit-information	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	2/10/2017	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2238&file=pdf NEED: Make sure your 2018 audit statements include: Distinguished Name and SHA256	**Verified?**	Need Response From CA

	fingerprint of each root and intermediate certificate that was in scope;		
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	2/10/2017	**Verified?**	Verified
EV SSL Audit		**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	Servers and Devices CP section 2.2.3.	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8908489	**Verified?**	Verified
SSL Verification Procedures	Servers and Devices CP section 3.1 NEED: It's not clear exactly what the CA does to verify domain ownership/control. CP needs to be clear enough that it is easy to determine which of the BR-allowed domain validation methods are used.	**Verified?**	Need Response From CA
EV SSL Verification Procedures	Not EV	**Verified?**	Not Applicable
Organization Verification Procedures	Servers and Devices CP sections 2.2.3 and 3.1.	**Verified?**	Verified
Email Address Verification Procedures	Not requesting email trust bit.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro		**Verified?**	Not Applicable
Multi-Factor Authentication	NEED: Where in your CP/CPS does it specify multi-factor authentication as per section 6.5.1 of the BRs?	**Verified?**	Need Response From CA
Network Security	CPS section 6.7	**Verified?**	Verified