General information about the CA's associated organization

CA Company Name	Ceska posta s.p.
Website URL	http://www.postsignum.cz
Organizational type	The PostSignum certification authority is a governmental certification authority (national government) operated by Ceska posta s.p. (Czech Post). PostSignum is an accredited provider of certification services in the Czech Republic (accreditation by the Ministry of the Interior of the Czech Republic). Qualified certification authorities from the PostSignum PKI hierarchy operate under Czech government regulations and must fulfil mandatory audit requirements stipulated in EU and Czech law.
Primark Market / Customer Base	The certification services of PostSignum are designated for the following groups of customers: • Organizations; and • Individuals (Natural persons). PostSignum does specialize in any particular market segment. PostSignum operates in the Czech Republic market. Certificates issued by PostSignum CAs are recognized in Czech republic and in other EU countries.
Impact to Mozilla Users	Mozilla users will typically encounter the root certificate of PostSignum when sending/receiving S/MIME emails and also while web browsing (HTTPS servers doing SSL)
CA Contact Information	CA Email Alias: manager.postsignum@cpost.cz CA Phone Number: +420 267 196 348 Title / Department: Manager CA

Technical information about each root certificate

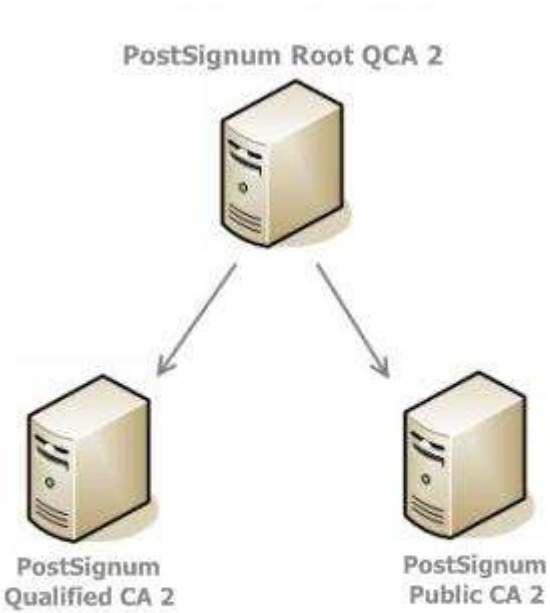
Certificate Name	PostSignum Root QCA 2
Certificate Issuer Field	CN = PostSignum Root QCA 2 O = Česká pošta, s.p. [IČ 47114983] C = CZ
Certificate Summary	A self-signed certificate of root certification authority PostSignum Root QCA 2. The root certification authority PostSignum Root QCA 2 issues system certificates for its subordinate certification authorities: • PostSignum Qualified CA 2

	• PostSignum Public CA 2
Root Cert URL	http://www.postsignum.cz/crt/psrootqca2.crt
SHA1 Fingerprint	a0 f8 db 3f 0b f4 17 69 3b 28 2e b7 4a 6a d8 6d f9 d4 48 a3
Valid From	2010-01-19
Valid To	2025-01-19
Certificate Version	x.509 v3
Certificate Signature Algorithm	sha256RSA
Signing key parameters	2048 bits
Test Website URL (SSL) Example Certificate (non-SSL)	Test website URL: https://www.postsignum.cz/index.php?lang=en Example of certificates: **PostSignum Qualified CA 2 (qualified certificates):** Certificate of an individual: http://www2.postsignum.cz/icz_szng_pcu/vss?VSS_SERV=ZCU003001&VSS_FORM=DATA&VSS_DAT1=1146095&content=DER&qualified=QCA System certificate: http://www2.postsignum.cz/icz_szng_pcu/vss?VSS_SERV=ZCU003001&VSS_FORM=DATA&VSS_DAT1=1036211&content=DER&qualified=QCA **PostSignum Public CA 2 (non-qualified certificates):** Certificate of an individual: http://www2.postsignum.cz/icz_szng_pcu/vss?VSS_SERV=ZCU003001&VSS_FORM=DATA&VSS_DAT1=534030&content=DER&qualified=VCA Server certificate: http://www2.postsignum.cz/icz_szng_pcu/vss?VSS_SERV=ZCU003001&VSS_FORM=DATA&VSS_DAT1=516719&content=DER&qualified=VCA
CRL URL	Certificate revocation lists might be obtained from the following URLs: **PostSignum Root QCA 2** http://www.postsignum.cz/crl/psrootqca2.crl http://www2.postsignum.cz/crl/psrootqca2.crl http://postsignum.ttc.cz/crl/psrootqca2.crl

	PostSignum Qualified CA 2: http://www.postsignum.cz/crl/psqualifiedca2.crl http://www2.postsignum.cz/crl/psqualifiedca2.crl http://postsignum.ttc.cz/crl/psqualifiedca2.crl **PostSignum Public CA 2:** http://www.postsignum.cz/crl/pspublicca2.crl http://www2.postsignum.cz/crl/pspublicca2.crl http://postsignum.ttc.cz/crl/pspublicca2.crl The period for updating CRL for end-entity certificates is set to 12 hours (NextUpdate field in CRL). The requirement for updating CRLs for end-entity certificates is stated in the Certification Policies and CPS in the section 2.3.
OCSP URL	The verification of the validity of the end user or CA certificates via the OSCP protocol is not currently available.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	OV
EV Policy OID(s)	Not applicable. EV certificates are not issued.

CA Hierarchy information for each root certificate

CA Hierarchy	**PostSignum Root QCA 2** is a root certification authority that issues qualified system certificates to subordinate certification authorities: • **PostSignum Qualified CA 2** issuing qualified certificates to the end users; and • **PostSignum Public CA 2** issuing commercial (non-qualified) certificates to the end users.

	 Both intermediate CAs (PostSignum Qualified CA 2 and PostSignum Public CA 2) are operated internally. Certificates of intermediate CAs: http://www.postsignum.cz/crt/psqualifiedca2.crt (PostSignum Qualified CA 2) http://www.postsignum.cz/crt/pspublicca2.crt (PostSignum Public CA 2)
Externally Operated SubCAs	Not applicable. The root certification authority PostSignum Root QCA 2 does not sign any subordinate CAs operated by third parties. Both subordinate CAs (PostSignum Qualified CA 2 and PostSignum Public CA 2) are operated by the same subject as the root CA (Ceska Posta s.p.).
Cross-Signing	Not applicable. PostSignum Root QCA 2 has not issued any cross-signing certificates.

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: CP: Czech CPS: Czech • Relying Party Agreement: Czech **Certification policies** PostSignum Root QCA 2: • http://www.postsignum.cz/files/politiky/QCA_cp_QCARoot_v_2_0.pdf (PostSignum certification authorities) PostSignum Qualified CA 2: • http://www.postsignum.cz/files/politiky/QCA_osobni_crt_v2-0.pdf (personal certificates) • http://www.postsignum.cz/files/politiky/QCA_systemove_crt_v2-0.pdf (systems certificates) PostSignum Public CA 2: • http://www.postsignum.cz/files/politiky/VCA_osobni_crt_v2-0.pdf (personal certificates) • http://www.postsignum.cz/files/politiky/VCA_serverove_crt_v2-0.pdf (server certificates) **Certification Practice Statement** • A Certification Practice Statement (CPS) exists, but it is not publicly available to subscribers. **Relying Party Agreement** • http://www.postsignum.cz/files/smlouvy/PO_PFO_smlouva.doc (organization) • http://www.postsignum.cz/files/smlouvy/FO_smlouva.doc (natural person)
Audits	Audit Type: Audit of full PostSignum PKI infrastructure (ETSI TS 101 456, ETSI TS 102 042) Auditor: Deloitte Advisory s.r.o. Auditor Website: http://www.deloitte.com/view/en_CZ/cz/index.htm

	URL to Audit Report and Management's Assertions: Audit equivalency statement will be provided directly by the auditor (contact Mr. Vlastimil Cerveny, CIA, CISA; vcerveny@deloitteCE.com) Date of completion of last audit: February 26, 2010 (Microsoft Root Certification Program). PostSignum will be re-audited on or before March 2012.
SSL Verification Procedures	PostSignum requests to enable the Websites (SSL/TLS) trust bit. Note: SSL/TLS certificates are only issued by the public certification authority PostSignum Public CA 2 that issues server certificates. The qualified certification authority PostSignum Qualified CA 2 does not issue this type of certificates. The procedures for verifying that the domain name referenced in a server certificate (SSL/TLS) is owned/controlled by the subscriber is stated in the Certification Policy - Section 4.1.2.4 . Note that the CP is currently available only in Czech. http://www.postsignum.cz/files/politiky/VCA_serverove_crt_v2-0.pdf This procedure is also stated in CPS (Note: CPS is not currently available to the public). PostSignum Public CA 2 uses OV type verification when issuing server certificates. The procedure for verifying identity, existence, and authority of the organization to request the certificate is described in the Certification Policy – Section 4.2.1. Note that the CP is currently available only in Czech language. http://www.postsignum.cz/files/politiky/VCA_serverove_crt_v2-0.pdf This procedure is also stated in CPS (Note: CPS is not currently available to the public).
Email Address Verification Procedures	PostSignum requests to enable the Email (S/MIME) trust bit. The current practice of PostSignum is that the email address of the subscriber is not verified. This is in accordance with the Czech legislative requirements and with PostSignum's certification policies and CPS. http://www.postsignum.cz/files/politiky/QCA_osobni_crt_v2-0.pdf http://www.postsignum.cz/files/politiky/VCA_osobni_crt_v2-0.pdf The subscriber's identity is verified against valid legal documents (valid ID card, passport, etc.), which are specified in the certification policies. The procedure for verifying the identity and authority of the certificate subscriber is described n the Certification Policy – Section 4.2.1 Note that the CP is currently available only in Czech language. http://www.postsignum.cz/files/politiky/QCA_osobni_crt_v2-0.pdf (PostSignum Qualified CA 2)

	http://www.postsignum.cz/files/politiky/VCA_osobni_crt_v2-0.pdf (PostSignum Public CA 2) This procedure is also stated in CPS (CPS is not currently available to the public).
Code Signing Subscriber Verification Procedures	Not applicable. PostSignum does not request to enable the Code Signing Trust Bit.

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

Publicly Available CP and CPS	Certification policies (CP) are publicly available on PostSignum's official web site. A Certification Practice Statement (CPS) exists, but it is not publicly available to subscribers. All documents are currently not available in English. **PostSignum Root QCA 2** http://www.postsignum.cz/files/politiky/QCA_cp_QCARoot_v_2_0.pdf (PostSignum certification authorities) **PostSignum Qualified CA 2** http://www.postsignum.cz/files/politiky/QCA_osobni_crt_v2-0.pdf (personal certificates) http://www.postsignum.cz/files/politiky/QCA_systemove_crt_v2-0.pdf (systems certificates) **PostSignum Public CA 2** http://www.postsignum.cz/files/politiky/VCA_osobni_crt_v2-0.pdf (personal certificates) http://www.postsignum.cz/files/politiky/VCA_serverove_crt_v2-0.pdf (server certificates)
CA Hierarchy	PostSignum PKI hierarchy consists of a single root CA with subordinate certification authorities. PostSignum wishes to supply a certificate of the single top-level root CA for Mozilla's root list (certificates of the subordinate authorities will not be submitted for Mozilla's root list).
Audit Criteria	PostSignum PKI hierarchy has been audited by an independent auditor. The most recent audit report is from February 2010. This audit was conducted by Deloitte and covered the full PKI hierarchy PostSignum (root and subordinate CAs). This audit was conducted against the following standards: • ETSI TS 101 456 (qualified CAs – PostSignum Root QCA 2, PostSignum Qualified CA 2) • ETSI TS 102 042 (public CA - PostSignum Public CA 2) The audit equivalency statement is available upon request from the auditor. Auditor's contact: Mr. Vlastimil Cerveny, CIA, CISA; Manager; Deloitte Advisory; vcerveny@deloitteCE.com

Document Handling of IDNs in CP/CPS	Currently it is not against the PostSignum's certificate policy to use IDNs in issued certificates. PostSignum will address this issue in the next version of the Certification Policy for server certificates.
Revocation of Compromised Certificates	Revocation of compromised certificates or certificates for which verification of subscriber information is known to be invalid is incorporated into PostSignum's common practices (this issue is addressed in CP and CPS). Manager CA has the authority to revoke such certificates.
Verifying Domain Name Ownership	During the registration process the subscriber must present the verification of the legal identity together with an affidavit of ownership of the domain name. This procedure is described in the certification policy for server certificates.
Verifying Email Address Control	The current practice of PostSignum is that the email address of the subscriber is not verified. This is in accordance with the Czech legislative requirements and with PostSignum's certification policies. The subscriber's identity is verified against valid legal documents (valid ID card, passport, etc.), which are specified in the particular certification policy.
Verifying Identity of Code Signing Certificate Subscriber	Not applicable. PostSignum certification authorities do not issue code signing certificates.
DNS names go in SAN	Server certificates that are issued by PostSignum Public CA 2 contain primary DNS name in the Subject Common Name field of certificate.
Domain owned by a Natural Person	If the domain is owned by a natural person, the server certificate issued by PostSignum Public CA 2 will have the following fields: • CN = DNS • OU= identifier of a natural person (internal identification code) Note: Field "O" is not used in server certificates for natural persons.
OCSP	Not applicable. The verification of the validity of the end user or CA certificates via the OSCP protocol is not currently available in PostSignum.

Response to Mozilla's list of potentially problematic practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	No long-lived DV certificates exist, PostSignum only issues OV server certificates (SSL/TLS). The expiration period of the server certificates that are issued by PostSignum Public CA 2 is 1 year.
Wildcard DV SSL certificates	Currently it is not against the certification policy to use wildcards in server certificates (SSL/TLS) that are issued by PostSignum Public CA 2. PostSignum will address this issue in the next version of the Certification Policy for server certificates. Note that the server certificates that are issued by PostSignum Public CA 2 are OV type as

	the legal identity of the subscriber is always verified prior to issuing the certificate.
Email Address Prefixes for DV Certs	Not applicable. PostSignum Public CA 2 does not issue domain validating (DV) server certificates (SSL/TLS) that would use an email address to verify the domain ownership. The ownership of the domain name is verified by verifying the legal identity together with an affidavit of ownership of the domain name. This procedure is described in the certification policy for server certificates.
Delegation of Domain / Email Validation to Third Parties	PostSignum does not delegate the validation of the subscriber's identity or domain/email ownership to third parties. Validation is performed by Registration Authorities that are operated by Ceska Posta s.p. Practices of Registration Authorities are audited together with the issuing of certification authorities.
Issuing End Entity Certificates Directly from Roots	The root certification authority PostSignum Root QCA 2 only issues certificates to its subordinate certification authorities (PostSignum Qualified CA 2 and PostSignum Public CA 2). The root authority is in off-line mode. The end entity certificates are issued only by these subordinate (or issuing) certification authorities.
Allowing External Entities to Operate Subordinate CAs	Not applicable. Both subordinate CAs (PostSignum Qualified CA 2 and PostSignum Public CA 2) are operated by the same subject as the root CA (Ceska Posta s.p.).
Distributing Generated Private Keys in PKCS#12 Files	Not applicable. PostSignum CAs do not generate the key pairs for their subscribers. PostSignum CAs do not have any control over subscriber's private keys. The subscribers generate their own key pairs.
Certificates Referencing Hostnames or Private IP Addresses	Currently it is not against the certification policy to issue server certificates that contain public DNS or private IP addresses. PostSignum will address this issue in the next version of the certification policy.
Issuing SSL Certificates for Internal Domains	PostSignum Public CA 2 currently does not apply any restriction against using non-existent .int domain names in issuing certificates. This issue will be addressed in the next version of the certification policy for server certificates. A list of domain names of issued server certificates will be internally reviewed in order to verify that there are no certificates with .int domain names.
OCSP Responses Signed by a Certificate under a Different Root	Not applicable. The verification of the validity of the end user or CA certificates via the OSCP protocol is not currently available in PostSignum.
CRL with Critical CIDP Extension	Not applicable. "CRL Issuing Distribution Point" (CIDP) extensions in the CRLs of PostSignum CAs are not flagged as critical.
Generic Names for CAs	Generic names for CAs are not used. All certification authorities within PostSignum PKI hierarchy have meaningful names: • PostSignum Root QCA 2, • PostSignum Qualified CA 2,

	• PostSignum Public CA 2. Additionally, the issuer and subject information in the PostSignum Root QCA 2 certificate also provides a clear indication about who owns or operates the certificate. • CN = PostSignum Root QCA 2 • O = Česká pošta, s.p. [IČ 47114983] • C = CZ
Lack of Communication With End Users	Subscribers and relying parties can contact PostSignum CA via: • Phone: 840 111 244, or • E-mail: info@cpost.cz Also, PostSignum is willing to answer any questions from the Mozilla community regarding the process of admission into the Mozilla root program. The contact person is Manager CA: (manager.postsignum@cpost.cz)