Bugzilla ID: 999378
Bugzilla Summary: Add CERTUM's SHA2 root certificate

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	Unizeto Certum
Website URL	http://www.certum.pl/
Organizational type	Public corporation
Primark Market / Customer Base	CERTUM - Broader Certification Center is an organizational unit of Unizeto Technologies SA, providing certification services related to electronic signatures. It is the oldest public certification authority in Poland and the commercial certification authority, operating on a global scale - serving customers in over 50 countries worldwide.
Inclusion in other major browsers	Yes. http://social.technet.microsoft.com/wiki/contents/articles/14219.windows-and-windows-phone-8-ssl-root-certificate-program-april-2012-u-z.aspx
CA Primary Point of Contact (POC)	POC direct email: Michał Proszkiewicz - mproszkiewicz@certum.pl CA Email Alias: info@certum.pl CA Phone Number: +48 91 4801 201 Title / Department: CERTUM PKI Services

Technical information about each root certificate

Certificate Name	Certum Trusted Network CA 2
Certificate Issuer Field	CN = Certum Trusted Network CA 2 OU = Certum Certification Authority O = Unizeto Technologies S.A. C = PL
Certificate Summary	This is the next generation of the "Certum Trusted Network CA" root cert that was included via bug #532377.
Mozilla Applied Constraints	Mozilla has the ability to apply Domain Name Constraints at the root level, such that Mozilla products would only recognize SSL certificates in the CA's hierarchy with domains in the listed constraints. Constraints may be at the country level such as *.us; and can include a list such as (*.gov.us, *.gov, *.mil). Please consider the types of SSL certificates that need to be issued within this CA hierarchy, and if applicable provide a list of names to constrain the CA hierarchy to.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=8410206
SHA1 Fingerprint	3E:5D:35:8F:28:3A:0F:64:7C:1C:92:7F:FB:AA:D4:85:2D:99:72:56
Valid From	2011-10-06
Valid To	2046-10-06

Certificate Version	3
Certificate Signature Algorithm	SHA-512
Signing key parameters	4096 Bits
Test Website URL (SSL)	https://valid-certum-ctncav2.certificates.certum.pl/ https://revoked-certum-ctncav2.certificates.certum.pl/ https://expired-certum-ctncav2.certificates.certum.pl/
CRL URL	http://crl.certum.pl/evca2.crl http://crl.certum.pl/ctnca2.crl
OCSP URL	http://evca2.ocsp.certum.pl http://subca.ocsp-certum.com OCSP maximum expiration time?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV, and EV
EV Policy OID(s)	1.2.616.1.113527.2.5.1.1 Please perform the EV test as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version And attach screenshot of successful EV treatment to the bug.
Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ... - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)."

CA Hierarchy information for each root certificate

CA Hierarchy	List, description, and/or diagram of all intermediate CAs signed by this root. Identify which subCAs are internally-operated and which are externally operated. CPS section 1.3.1.1: Certum Trusted Network CA renders certification services to: · itself (issues and renews self-certificates), · Certum Extended Validation CA, Certum Code Signing CA, **Certum Class 1 CA authorities and other certification authorities** which will be registered in certification domain ctnDomena, · entities delivering services of on-line certificate status verification (OCSP) and other entities rendering services of non-repudiation (e.g. time-stamping service). CPS section 1.3.1.2: Only two authorities can issue certificates to other certification authorities: Certum Level I CA (test certification authorities) and Certum Global Services CA (commercial certification authorities).
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.

Cross-Signing	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate. If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	Document Repository (English): http://www.certum.pl/repository CP: http://certum.pl/servlet/pl.id.sys.servlets.FileDownloadServlet?filename=/upload_module/downloads/certum/dokumenty/polityka_certyfikacji/Certum_CP_v3_3.pdf CPS: http://certum.pl/servlet/pl.id.sys.servlets.FileDownloadServlet?filename=/upload_module/downloads/certum/dokumenty/kodeks_postepowania_certyfikacyjnego/Certum_CPS_v3_4.pdf EV CPS: **Get error "No permission to view"** http://certum.pl/servlet/pl.id.sys.servlets.FileDownloadServlet?filename=/upload_module/downloads/certum/dokumenty/kodeks_postepowania_certyfikacyjnego/Certum_CPS_v3_4_EV.pdf
Audits	Auditor: Ernst & Young, http://www.ey.com/pl Audit Type: Baseline Requirements Audit Report: https://cert.webtrust.org/SealFile?seal=1526&file=pdf (2013.07.10) Audit Type: WebTrust CA Audit Report: https://cert.webtrust.org/SealFile?seal=1523&file=pdf (2013.07.10) Audit Type: WebTrust EV Audit Report: https://cert.webtrust.org/SealFile?seal=1524&file=pdf (2013.07.10)
Baseline Requirements (SSL)	The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.
SSL Verification Procedures	Verification procedures for "Certum Class 1 CA" are the same as for "Certum Level I CA". Domain ownership is verified, not identity. For "Certum Level III CA" SSL certs are both DV and OV.

	CPS section 3.2.2: A registration authority is committed to verify the correctness and truthfulness of all data provided in an application. In the case of EV SSL certificates additional procedure set out in Appendix 3 shall be applied. CPS section 3.2.2: In the case of certificates issued for devices, authentication may be accomplished by verifying access to the domain placed in the certificate request. CERTUM may verify the subscriber's right to use the domain name and email address by using one of the following methods: · domain verification – when a verification element indicated by CERTUM is placed on destination server · email address verification – when the Subscriber is required to be able to answer an email sent by CERTUM to his/her/its address. CPS section 3.2.2: registration authority operator may – in doubtful cases – verify the registration of the domain in publicly available WHOIS services. CPS section 4.2.2.3: Certificate issuance denial can occur: … the subscriber cannot prove his/her rights to proposed DN, EV CP 14. and 15. Verification of Applicant's Legal Existence and Identity 16. Verification of Applicant's Physical Existence 17. Verification of Applicant's Operational Existence 18. Verification of Applicant's Domain Name
Organization Verification Procedures	CPS Table 1.5: Certum Level I CA and Certum Class 1 CA – DV only. Identity of subscriber not verified. Only domain name ownership via email exchange. Can only be used for testing with a private SSL server. Certum Level II CA – Signs certs used for S/MIME, not for SSL or code signing. Certum Level III CA – Signs certs for use with enterprise SSL servers. Also signs certs for code signing and S/MIME. Certum Level IV CA -- for the certification authorities, non-repudiation authorities and global network-based electronic transaction systems. Certum Extended Validation CA – Signs EV SSL certs Organizational verification is performed for Levels III, IV, and EV. Section 3.2 of the CPS describes the procedures for authenticating the identity of the certificate subscriber and verifying the existence and identity of the organization.
Email Address Verification Procedures	CPS section 3.2.2: In the case of email certificates, registration authority verifies an email address. The aim of this action is to receive by the subscriber an authentication data sent to the address which has previous placed in the certification request. CPS section 3.2.2: CERTUM may verify the subscriber's right to use the domain name and email address by using one of the following methods: * domain verification – when a verification element indicated by CERTUM is placed on destination server

	* email address verification – when the Subscriber is required to be able to answer an e-mail sent by CERTUM to his/her/its address. CP of CERTUM's Non-Qualified Certification Services Section 2.1, Level I Certificates: In most cases email address, address data and name and surname of the private entity or the representative of the legal entity are subjected to verification. Section 2.2, Level II Certificates: Operators of Certum Level II CA verify the information provided by the requesters during the certification process. Detailed information on identity verification requirements are described in dedicated document (Identity verification instruction). Section 2.3, Level III Certificates: These certificates are intended mainly for securing electronic correspondence, securing binary objects against forgery and protecting data transmission on the basis of SSL and TLS protocol. Operators of Certum Level III CA verify the information provided by the requesters during the certification process. Detailed information on identity verification requirements are described in dedicated document (Identity verification instruction).
Code Signing Subscriber Verification Procedures	Where does the CPS say which levels of authentication apply to code signing certs?
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

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	???
Revocation of Compromised Certificates	???
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	See above
DNS names go in SAN	???
Domain owned by a Natural Person	???
OCSP	See above

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

Long-lived DV certificates	???
Wildcard DV SSL certificates	???

Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification. (BR #11.1.1)
Delegation of Domain / Email validation to third parties	??? - external subCAs - Registration Authorities (CPS section 1.3.2)
Issuing end entity certificates directly from roots	No. See above.
Allowing external entities to operate subordinate CAs	Yes?
Distributing generated private keys in PKCS#12 files	???
Certificates referencing hostnames or private IP addresses	???
Issuing SSL Certificates for Internal Domains	???
OCSP Responses signed by a certificate under a different root	No. See above.
CRL with critical CIDP Extension	
Generic names for CAs	No. See above.
Lack of Communication With End Users	???
Backdating the notBefore date	???