Bugzilla ID: 532377
Bugzilla Summary: Add CERTUM's new Root CA to Mozilla's trusted root list

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	Certum
Website URL	http://www.certum.eu/
Organizational type	Public corporation
Primary 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.
CA Contact Information	CA Email Alias: info@certum.pl CA Phone Number: +48 91 4801 201 Title / Department: CERTUM PKI Services System Administrator - Wojciech Ślusarczyk - wslusarczyk@certum.pl, +48 91 4801 282 Security Inspector - Michał Proszkiewicz - mproszkiewicz@certum.pl, +48 91 4257 441 Product Manager - Tomasz Litarowicz, +48 91 4801 240 Head of the CA - pmatusiewicz@unizeto.pl

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	Certum Trusted Network CA
Cert summary / comments	Certum currently has a root named "Certum CA" included in NSS. Eventually, the certificates under the old "Certum CA" root will be moved to this new root. Currently this new root has two sub-CAs: Class 1 and EV. Comment #4: New root was created due to requirements of WebTrust for EV audit (old root do not have SKI and Key usage extensions). We are going to move all (at first SSL certificates) certificates under the new root, at the moment we have only Class1 an EV intermediate certificate generated.
The root CA certificate URL	http://repository.certum.pl/CTNCA.crt
SHA-1 fingerprint.	07:E0:32:E0:20:B7:2C:3F:19:2F:06:28:A2:59:3A:19:A7:0F:06:9E
Valid from	2008-10-22
Valid to	2029-12-31

Cert Version	3
Modulus length / key length	2048
Test Website	https://juice.certum.pl/
CRL URL	ARL: http://crl.certum.pl/ctnca.crl Class 1 CRL: http://crl.certum.pl/c1.crl (Next Update: 1 month) EV SSL CRL: http://crl.certum.pl/evca.crl (Next Update: 9 days) All Certum CRLs: http://www.certum.eu/certum/cert,certificates_crl_lists.xml
OCSP Responder URL	Comment #4: At the moment we do not support OCSP for new root but due to CA/Browser Forum Guidelines version 1.2 in section 11.1.1 there is: "CAs MUST support an OCSP capability for Subscriber Certificates that are issued after Dec 31, 2010". We are still making some changes and preparation but OCSP will be available as it is required by CA/Browser Forum Guidelines.
CRL/OCSP Issuing Frequency	NextUpdate for the EV SSL CRL is 9 days. EV CP section 26. EV SSL Certificate Status Checking CERTUM maintains an online 24x7 Repository mechanism whereby Internet browsers can automatically check online the current status of all certificates. (1) For EV SSL Certificates: (A) CRLs are updated and reissued at least every seven days, and the nextUpdate field value SHALL NOT be more ten days; or (B) OCSP Since January 2011 Certum Extended Validation CA will provide revocation information via an Online Certificate Status Protocol (OCSP) service and update that service at least every four days. OCSP responses from this service will have a maximum expiration time of ten days.
CA Hierarchy	CA Hierarchy Diagram shown in Figure 1.1 of CPS of CERTUM's Non-Qualified Certification Services There are three separate roots: 1) "National Root" for the Qualified Certification Services (not part of this request) 2) "Certum CA" for the non-Qualified Certification Services (this root is currently in NSS) 3) "Certum Trusted Network CA" for non-Qualified Certification Services (this new root) This "Certum Trusted Network CA" root currently has two sub-CAs: 1) Certum Class 1 CA (for 3 month test certs) 2) Certum Extended Validation CA The hierarchy of this root is referred to as the ctnDomena domain within the CPS. Eventually the certificates under the "Certum CA" root will be transitioned to the new root. The "Certum CA" root has the following sub-CAs: • Certum Level I CA. These certificates are intended mainly for the application or device test performance prior to purchasing final certificate. • Certum Level II CA. These certificates are intended mainly for securing electronic correspondence, encrypting binary objects and protecting data transmission.

	• Certum Level III CA. 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. • Certum Level IV CA. These certificates are intended mainly for the certification authorities, non-repudiation authorities and global network-based electronic transaction systems. • Certum Partners CA. Signs certificates for external CAs**.** Entities, whom such certificates are issued to, are subjected to thorough verification, carried out by Unizeto Technologies S.A. operators. Certificates issued by Certum Partners authority are valid for 5 years and require hardware protection of private keys.
Sub-CAs operated by 3rd parties	Comment #4: We do plan to use this root for subordinate CAs that are operated by external third parties, special intermediate certificate will be created and proper changes to CPS will be done when needed.
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing Comment #4: we do plan to move Email and Code Sign certificate under new root
SSL Validation Type DV, OV, and/or EV	DV, OV, EV Comment #4: Class 1 certificates are mainly Domain Validated certificates, it means that we check if subscriber has access to domain (domain, and email verification), additionally we use publicly available tools like Netcraft. If we have doubts we sometimes require additional documents.
EV policy OID(s)	1.2.616.1.113527.2.5.1.1
CP/CPS	Certum Cert and Document Repository: http://www.certum.pl/repository CP of CERTUM's Non-Qualified Certification Services (English): [general] http://www.certum.eu/upload_module/downloads/certum/dokumenty/polityka_certyfikacji/Certum_CP_v3_1.pdf CPS of CERTUM's Non-Qualified Certification Services (English): [details] http://www.certum.eu/upload_module/downloads/certum/dokumenty/kodeks_postepowania_certyfikacyjnego/Certum_CPS_v3_1.pdf EV CPS -- Appendix 3: Guidelines for the issuance and management of Extended Validation SSL certificate http://www.certum.eu/upload_module/downloads/certum/dokumenty/kodeks_postepowania_certyfikacyjnego/Certum_CPS_v3_1_EV.pdf
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young Auditor Website: http://www.ey.com/pl Audit Report and Management's Assertions: https://cert.webtrust.org/SealFile?seal=1072&file=pdf (2010.04.14)

	Audit Type: WebTrust EV Point In Time Readiness Auditor: Ernst & Young Auditor Website: http://www.ey.com/pl Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=980 (2009.10.20)
Organization Identity Verification	CPS Table 1.4: 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.
Domain Name Ownership / Control for SSL Certs	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. 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 e-mail 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,
Domain Name Ownership / Control	EV CP 14. and 15. Verification of Applicant's Legal Existence and Identity

for EV SSL Certs	16. Verification of Applicant's Physical Existence 17. Verification of Applicant's Operational Existence 18. Verification of Applicant's Domain Name
Email Address Ownership / Control	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*).
Identity of Code Signing Subscriber	CPS section 1.4.1: Code Signing certs are issued under the Certum Level III CA (Organization verified) CPS section 3.2.2: The registration authority is required to request suitable documents from the subscriber, which without any doubts confirm the identity of the legal entity on whose behalf the application is submitted and the private entity that represent it (or submits the application). CPS section 3.2.2: Registration authority may collect the data required for identification by its own, e.g. through publicly available databases. Authentication of legal entity's identity has two purposes. The first purpose is to prove that at the time of application examination the legal entity stated in the application existed; the second purpose is to prove that a private entity applying for a certificate or receiving it is authorized by this legal entity to represent it. Submitted documents (or collected data) should prove: * identity of the subscriber or certificate administrator (in the case of certificates issued for legal entities or devices), * existence of the legal entity or institution, * the right of the subscriber or the certificate administrator to act on behalf of the institution or legal entity. * registration authority operator may – in doubtful cases – verify the registration of the domain in publicly available

	WHOIS services. There are two basic ways of legal entity's identity authentication. The first one requires the legal entity's authorized representative's personal attendance in a registration authority, or a registration authority representative's presence in person in the legal entity's seat (specified in the application). In the second case, the identity can be authenticated on-line by means of messages exchanged directly with a certification authority or its agent. A registration authority is committed to verify the correctness and truthfulness of all data provided in an application. CPS section 4.2.2.1: the operator verifies data listed in the application, e.g. subscriber's personal data (see the procedure described in Chapter 3.2.2, 3.2.3 or 3.2.5) and checks the proof of private key possession if it exists (see Chapter 3.2.1),

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ CPS table 6.6 on page 82. Maximum usage periods of subscriber certs.
	  ▪ Level I: 3 months (DV)
	  ▪ Level II: 1 year (not SSL)
	  ▪ Level III: 2 years (OV)
	  ▪ Level IV: 2 years
	  ▪ EV SSL: 27 months
	• Wildcard DV SSL certificates
	  ○ Wildcard certs aren't allowd for level I. Level III and above SSL certs are OV.
	• Delegation of Domain / Email validation to third parties
	  ○ Comment #4: We do not delegate any validation process to third parties
	• Issuing end entity certificates directly from roots
	  ○ No. Root only signs sub-CAs.
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ Not applicable
	• Distributing generated private keys in PKCS#12 files
	  ○ As it is stated in CPS in section 6.1.1: "Generally, every subscriber generates his/her/its key pair by himself/herself/itself. The generation may also be delegated to a certification authority (applicable only for keys generated on cryptographic cards)."
	• Certificates referencing hostnames or private IP addresses
	  ○ Comment #4: At the moment we do not intend to issue such certificates
	• Issuing SSL Certificates for Internal Domains
	  ○ Comment #4: for SSL certs for internal domains "We validate organization, and person responsible for certification process"

	• OCSP Responses signed by a certificate under a different root
	  ○ Not applicable
	• CRL with critical CIDP Extension
	  ○ CRLs download into Firefox browser without error.
	• Generic names for CAs
	  ○ Root name is not generic