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 An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. pmatusiewicz@unizeto.pl (Head of the CA) wslusarczyk@certum.pl (System Administrator) mproszkiewicz@certum.pl (Security Inspector) CA Phone Number: +48 91 4801 201 Company main phone number A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA. Title / Department: CERTUM PKI Services If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for? Wojciech Ślusarczyk (System Administrator) +48 91 48 01 282 Michał Proszkiewicz (Security Inspector) +48 91 42 57 441 Tomasz Litarowicz (Product Manager) +48 91 48 01 240

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	What is the relation of this "Certum Trusted Network CA" root to the "Certum CA" root that is currently in Mozilla/NSS? Will all or part of the hierarchy of the "Certum CA" root be moved to the "Certum Trusted Network CA" root? 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 firs 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	2049
Test Website	For testing purposes, please provide a URL to a website whose SSL cert chains up to this root. Note that this can be a test site. If possible, please provide a website whose SSL cert is enabled for EV under this root.
CRL URL	ARL: http://crl.certum.pl/ctnca.crl All Certum CRLs: http://www.certum.eu/certum/cert,certificates_crl_lists.xml (CRL for the EV certs not here) CRL should be present by now
OCSP Responder URL	http://ocsp.certum.pl Problem with OCSP of current root: https://www.certum.pl/certum/main.xml SSL Cert chains up to old root currently included in Mozilla/NSS: CN = Certum CA AIA extension of the SSL cert has OCSP: URI: http://ocsp.certum.pl Enforce OCSP in Firefox: Tools->Options…->Advanced->Encryption->Validation Select the box for “When an OCSP server connection failes, treat the certificate as invalid” Clear history/cache… Then this website gives error: An error occurred during a connection to www.certum.pl. The signer of the OCSP response is not authorized to give status for this certificate. (Error code: sec_error_ocsp_unauthorized_response) **This means that your end-users who use the Firefox browser are currently on not protected from revoked certificates. This must be fixed ASAP.** We currently do not support OCSP for new root (new certificates for the time being will have CRL distribution point included – http://crl.certum.pl/c1.crl for class1 and http://crl.certum.pl/evca.crl for EV SSL). For Certum CA, our OCSP is working in trusted responder mode which is not supported by Firefox, this was submitted as bug: https://bugzilla.mozilla.org/show_bug.cgi?id=378673
CRL/OCSP Issuing Frequent	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; CRL’s for EV SSL are published et least every 7 days at http://crl.certum.pl/evca.crl (first publication was made last week) or (B) OCSP Since January 2010 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. 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.

CA Hierarchy	CA Hierarchy Diagram shown in Figure 1.1 of CPS of CERTUM's 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 only 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.
Sub-CAs operated by 3rd parties	Does or will this root have any subordinate CAs that are operated by external third parties? CPS: "Only two authorities can issue certificates to other certification authorities: **Certum Level I CA** (test certification authorities) and **Certum Partners** (commercial certification authorities)" So, as long as a Certum Partners sub-CA isn't created under this root, then it looks like this root will not have sub-CAs that are operated by external third parties. 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	List any other root CAs that have issued cross-signing certificates for this root CA
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) – The Email trust bit does not appear to be applicable to this root. Code Signing – The Code Signing trust bit does not appear to be applicable to this root. As we do plan to move Email and Code Sign certificate under new root it would be most expected to enable all 3 trust bits
SSL Validation Type DV, OV, and/or EV	? Not clear if the Class 1 certs are even DV. Do you perform verification of ownership of domain name for all SSL certs issued under this root? Do you perform identity/organization verification for all SSL certificates under this root? Class 1 certificate 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. Identity verification procedures are non-public available for authorized personnel and auditors.
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_0.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_0.pdf EV CP --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_0_AppendixEV.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/ViewSeal?id=965 (2009.04.14) Audit Type: WebTrust EV Auditor: Ernst & Young Auditor Website: http://www.ey.com/pl Audit Report and Management's Assertions: In Progress Additionally we do have point in time WebTrust for EV audit available at: https://cert.webtrust.org/ViewSeal?id=980 It is a audit report that according to our auditors should be enough to start enabling our root as EV in browser
Organization Identity Verification	From CPS Table 1.4: Certum Class 1 CA (certs are valid for up to 3 months) – Validation is same as Certum Level I CA: The lowest credibility level of the identity of a certificate entity. Level I certificates should be applied to test the compatibility of CERTUM services with the services of other deliverers of PKI services, and to test certificate functionality in cooperation with applications being tested. These certificates can also be used for other purposes, as long as assurance of the credibility of a message being sent or received is not important. Attention. Relying party has no guarantee that a user of certificate is actually person that was mentioned in the certificate Can Certium Class 1 certs be issued for SSL? If so, what verification is done in regards to the ownership/control of the domain name? Which section of the CPS is this documented in? Yes, verification process is similar to Certum Level I CA SSL certificates. It is documented in identity verification procedures which are non-public documents. 3.2.2. Authentication of Legal Entity's Identity 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). 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. Detailed requirements on the identification documents and it verification are specified in separate document – *Identity verification instruction*.

	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. 3.2.3. Authentication of Private Entity’s Identity Authentication of private entity’s identity has two purposes. The authentication must prove that (1) data provided in an application concern an existing private entity and (2) the requester is indeed the private entity stated in the application. Procedures and requirements for private entity identity authentication are the same as for legal entities. The only difference is that the existence of the legal entity and the right to act on its behalf verification is amended by verification of the right to use distinguished names other that name and surname. 3.2.5. Government Entities and Organizations validation In the case where a person's name placed on the certificate contains the name of the organization (O), then this should be interpreted as the person's affiliation or authorization of that person to act on behalf of the organization. This means that CERTUM: -verified that the organization was existing at the time of issued the certificate, the verification was based on independent sources of information or based on an extract from the National Court Register; -verified that the individual whose data are included in the certificate was an employee organization or its subcontractor at the time of issuance of the certificate of organization and has the right to act on behalf of the organization; the scope of authorization and the period of validity may be regulated by separate legislation or the relying party in the course of verification a digital signature or decryption the received document and is outside the scope of liability of CERTUM; individual’s identity and authorization may be checked by CERTUM on the basis of available records or database, contact by phone or e-mail to the organization. 4.2.2.1. Application Processing in Registration Authority Every application submitted to a request confirmation box or submitted to a registration authority in a paper version, is processed in the following way: -a registration authority operator obtains subscriber’s application (a paper version or an electronic version from the request confirmation box), -a registration authority operator checks whether the subscriber has made a charge for processing an application for a certificate, provided that such payment is provided in the price list of CERTUM, in the absence of such a charge, the request is rejected. -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), -positive verification, the operator confirms (signs) the request; if the original application contains wrong data, it is rejected, -the confirmed application is submitted to a request box of a certification authority, -a registration authority may also verify other data that are not listed in an application and required by CERTUM to run a business. 4.2.2.3. Certificate Issuance Denial CERTUM can refuse certificate issuance to any requester without taking any obligations or responsibility that might follow the requester’s damages or loss resulting from this denial. The certification authority should immediately refund the requester the certificate fee (if the requester paid it), unless the requester stated false data in his/her/its application. Certificate issuance denial can occur: -the subscriber cannot prove his/her rights to proposed **DN**, -if there is suspicion or certainty that the subscriber falsified the data or stated false data, -subscriber in especially inconvenient manner engaged resources and processing means of CERTUM by submitting number of request clearly in excess of his/her/its needs, -subscriber did not make a payment for issuing a certificate, provided that such payment is provided in the price list of CERTUM, -other reasons not specified above.

Domain Name Ownership / Control	Not clear for Class 1 certs. Same as for Certum Level I CA From EV CP 18. Verification of Applicant's Domain Name To verify Applicant's registration, or exclusive control, of the domain name(s) to be listed in the EV SSL Certificate, CERTUM verifies that each such domain name satisfies the following requirements: (1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA); (2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization. For Government Entity Applicants, CERTUM relies on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name. (3) Applicant is the registered holder of the domain name, or has been granted the exclusive right to use the domain name by the registered holder of the domain name; (4) Applicant is aware of its registration or exclusive control of the domain name; (A) Acceptable methods by which CERTUM verifies that Applicant is the registered holder of the domain name include the following: (1) Performing a WHOIS inquiry on the Internet for the domain name supplied by Applicant, and obtaining a response indicating that Applicant or a Parent/Subsidiary Company is the entity registered to the domain name; or (2) Communicating with the contact listed on the WHOIS record to confirm that Applicant is the registered holder of the domain name and having the contact update the WHOIS records to reflect the proper domain name registration. Confirmation that the registered owner of the domain name is a Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant is sufficient to establish that Applicant is the registered owner of the domain name; (3) In cases where domain registration information is private, and the domain registrar offers services to forward communication to the registered domain holder, CERTUM contacts Applicant through the domain registrar by e-mail or paper mail. (B) In cases where Applicant is not the registered holder of the domain name, CERTUM verifies Applicant's exclusive right to use the domain name(s). In addition, CERTUM verifies Applicant's exclusive right to use the domain name using one of the following methods: (1) Relying on a Verified Legal Opinion to the effect that Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or (2) Relying on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract. In cases where the registered domain holder cannot be contacted, CERTUM will: -Relies on a Verified Legal Opinion to the effect that Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, and -Relies on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract, coupled with a practical demonstration by Applicant establishing that it controls the domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing Applicant's FQDN; CERTUM may verifies the Applicant is aware that it has exclusive control of the domain name obtaining a confirmation from the Contract Signer or Certificate Approver verifying that Applicant is aware that it has exclusive control of the domain name.

Email Address Ownership / Control	The Email trust bit does not appear to be applicable to this root section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: ▪ for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; It will apply in the future. We do check if entity submitting the request have access to email account.
Identity of Code Signing Subscriber	The Code Signing trust bit does not appear to be applicable to this root. section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: ▪ for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; We check organization identity, and if entity submitting request have the rights to do so.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information and relevant CPS section numbers. ▪ Long-lived DV certificates o See CPS Tab.6.6 Maximal usage periods of the subscriber's certificates for information about validity period o EV CP section 8: The validity period for an EV SSL Certificate is twenty seven (27) months. o EV CP section 8: The age of validated data used to support issuance of an EV SSL Certificate cannot exceed… Domain name – thirteen (13) months; ▪ Wildcard DV SSL certificates o Not applicable at the moment ▪ Delegation of Domain / Email validation to third parties o Looks like this applies o We do not delegate any validation process to third parties ▪ Issuing end entity certificates directly from roots o We do not attend to issue end entity certificates directly form root ▪ Allowing external entities to operate unconstrained subordinate CAs o Not applicable ▪ Distributing generated private keys in PKCS#12 files o 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 o At the moment we do not intend to issue such certificates ▪ Issuing SSL Certificates for Internal Domains o We validate organization, and person responsible for certification process ▪ OCSP Responses signed by a certificate under a different root o Not applicable ▪ CRL with critical CIDP Extension o Not applicable ▪ Generic names for CAs o Root name is not generic