Print this page

Mozilla - CA Program

Case Information

Case Number	00000049	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Unizeto Certum	**Request Status**	Need Information from CA

Additional Case Information

Subject	Include Certum's SHA2 root cert	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=999378

General information about CA's associated organization

Company Website	http://www.certum.eu/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Poland	**Verified?**	Verified
Primary Market / Customer Base	Certum is an organizational unit of Unizeto Technologies SA, providing certification services related to electronic signatures. It is the oldest public, commercial certification authority in Poland; operating on a global scale - serving customers in over 50 countries worldwide.	**Verified?**	Verified
Impact to Mozilla Users	Certum already has a root cert included in NSS. This is the next generation root.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_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 CLARIFICATION: * DNS names go in SAN -- In CPS Table 7.1 it says "commonName (in the case of server certificates)" but it does not say anything about the Subject Alternative Name Extension being required. Please see https://wiki.mozilla.org /CA:Recommended_Practices#DNS_names_go_in_SAN == * CPS section 3.1.1: In the case of SSL certificates CERTUM	**Verified?**	Need Clarification From CA

employs an automated process that prevent the release of certificate with a wildcard character (*) which occurs in the first label position to the left of the top level domain.

* CPS section 3.1.1: For requests for internationalized domain names (IDNs) in certificates, CERTUM performs domain name owner verification to detect cases of homographic spoofing of IDNs. CERTUM employs a manual process to find the risk of a particular domain. A search failure result is flagged for manual review and the Registration Authority manually rejects the certificate request.

* Revocation of Compromised Certificates -- CPS section 4.9.1

* Domain owned by a Natural Person -- For Natural Person we issue only DV certificates.

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_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	* Delegation of Domain / Email validation to third parties -- CPS section 1.3.2: "Moreover, Registration Points do not have the rights to verify the subscriber's right to use the Distinguished Name." "The Primary Registration Authority is located at the seat of CERTUM. Contact addresses with the PRA are listed in chapter 1.5.2" CPS Table 7.1: Subject (Distinguished Name) -- Distinguished names comply with the X.501 requirements. Values of all attributes of these fields are optional, except for the following fields: emailAddress (in the case of individual's certificates), organizationName (in the case of non-Repudiation and CA certificates), commonName (in the case of server certificates), unstructured {Address or Name} (in the case of VPN certificates) which are mandatory. * CERTUM issue and issued certificates valid for maximum 36 months. * CERTUM issue DV Wildcard certificates. We do make additional verification for popular domains. * CERTUM uses only those email addresses when performing email verification: admin@domain, administrator@domain, webmaster@domain, hostmaster@domain, postmaster@domain * Allowing external entities to operate subordinate CAs -- No. All intermediates are operated by CERTUM. * CERTUM don't issue certificates for internal names and reserved IP addresses. * CERTUM don't issue certificates for internal domains. * Our proprietary CA software doesn't allow to backdate end-user certificates.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Certum Trusted Network CA 2	**Root Case No**	R00000064
Request Status	Need Information from CA	**Case Number**	00000049

Additional Root Case Information

Subject	Include Certum Trusted Network CA 2

Technical Information about Root Certificate

O From Issuer Field	Unizeto Technologies S.A.	**Verified?**	Verified
OU From Issuer Field	Certum Certification Authority	**Verified?**	Verified
Certificate Summary	This is the next generation of the “Certum Trusted Network CA” root cert that was included via bug #532377.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8410206	**Verified?**	Verified
Valid From	2011 Oct 06	**Verified?**	Verified
Valid To	2046 Oct 06	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-512	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://valid-certum-ctncav2.certificates.certum.pl/	**Verified?**	Verified
CRL URL(s)	http://crl.certum.pl/evca2.crl http://crl.certum.pl/ctnca2.crl	**Verified?**	Verified
OCSP URL(s)	http://evca2.ocsp.certum.pl http://subca.ocsp-certum.com OCSP response is valid for 7 days. When answer is “unknown” there is no nextUpdate field in the response. (RFC 6960 4.2.2.1. "If nextUpdate is not set, the responder is indicating that newer revocation information is available all the time.")	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.2.616.1.113527.2.5.1.1	**Verified?**	Verified
EV Tested	// CN=Certum Trusted Network CA 2,OU=Certum Certification Authority,O=Unizeto Technologies S.A.,C=PL "1.2.616.1.113527.2.5.1.1", "Certum EV OID", SEC_OID_UNKNOWN, { 0x9F, 0x8B, 0x05, 0x13, 0x7F, 0x20, 0xAC, 0xDE, 0x9B, 0x99, 0x64, 0x10, 0xF4, 0xD0, 0xBF, 0x79, 0x71, 0xA1, 0x00, 0x6D, 0xC9, 0x9E, 0x09, 0x4C, 0x34, 0x6D, 0x27, 0x9B, 0x93, 0xCF, 0xF7, 0xAE }, "MIGAMQswCQYDVQQGEwJQTDEiMCAGA1UEChMZVW5pemV0byBUZWNobm9sb2dpZXMg" "Uy5BLjEnMCUGA1UECxMeQ2VydHVtIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MSQw" "IgYDVQQDExtDZXJ0dW0gVHJ1c3RlZCBOZXR3b3JrIENBIDI=", "ALhZFHE/V9+PMcAzPdLWGXojF7Tr", Success!	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified

Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	3E:5D:35:8F:28:3A:0F:64:7C:1C:92:7F:FB:AA:D4:85:2D:99:72:56	**Verified?**	Verified
SHA-256 Fingerprint	9F:8B:05:13:7F:20:AC:DE:9B:99:64:10:F4:D0:BF:79:71:A1:00:6D:C9:9E:09:4C:34:6D:27:9B:93:CF:F7:AE	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	NEED CLARIFICATION: Are test SSL certs allowed? What about domain control validation? Where is this documented? CP section 2.1, Level 1: "In *most* cases domain name, email address, address data and name and surname of the private entity or the representative of the legal entity are subjected to verification." This is very concerning. Domain name control must be validated for *all* SSL certs chaining up to a root in Mozilla's program. Email address verification must also be performed for S/MIME certs... CPS section 1.3.1: authorities subordinate to Certum Trusted Network CA: - Certum Class 1 CA, -- TEST CERTS - Certum Class 1 CA SHA2, -- TEST CERTS - Certum Code Signing CA, - Certum Code Signing CA SHA2, - Certum Domain Validation CA SHA2, - Certum Organization Validation CA SHA2, - Certum Extended Validation CA, - Certum Extended Validation CA SHA2, - Certum Global Services CA SHA2.	**Verified?**	Need Clarification From CA
Externally Operated SubCAs	NEED CLARIFICATION: It looks like externally-operated subordinate CAs are allowed. Is that correct? CPS section 1.3.1: Only two authorities can issue certificates to other certification authorities: Certum Level I CA (test certification authority) and Certum Global Services CA (commercial certification authority). If external subCAs are allowed, then need the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist	**Verified?**	Need Clarification From CA
Cross Signing	NEED CLARIFICATION: Has this root been involved in cross-signing? If yes, with which roots?	**Verified?**	Need Clarification From CA
Technical Constraint on 3rd party Issuer	NEED CLARIFICATION: It looks like external RAs are not allowed to do the validation of the email address or domain names to be included in the certificates. Is that correct?	**Verified?**	Need Clarification From CA

	* Delegation of Domain / Email validation to third parties -- CPS section 1.3.2: "Moreover, Registration Points do not have the rights to verify the subscriber's right to use the Distinguished Name." "The Primary Registration Authority is located at the seat of CERTUM. Contact addresses with the PRA are listed in chapter 1.5.2" CPS Table 7.1: Subject (Distinguished Name) -- Distinguished names comply with the X.501 requirements. Values of all attributes of these fields are optional, except for the following fields: emailAddress (in the case of individual's certificates), organizationName (in the case of non-Repudiation and CA certificates), commonName (in the case of server certificates), unstructured {Address or Name} (in the case of VPN certificates) which are mandatory.

Verification Policies and Practices

Policy Documentation	http://www.certum.eu/ then click on Repository at the bottom of the page. Documents are in Russian and English.	**Verified?**	Verified
CA Document Repository	http://www.certum.eu/certum/179898.xml	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.certum.eu/upload_module/wysiwyg /Certum_CP_v3_3.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://certum.pl/servlet /pl.id.sys.servlets.FileDownloadServlet?filename= /upload_module/downloads/dokuments /Certum_CPS_v3_7_en.pdf	**Verified?**	Verified
Other Relevant Documents	http://www.certum.eu/certum /cert,aboutus_about_webtrust.xml Qualified certs: http://www.certum.eu/upload_module/wysiwyg /CCK-DK02-ZK01_CPv3_8.pdf http://www.certum.eu/upload_module/wysiwyg /CCK-DK02-ZK02_CPSv3_8.pdf	**Verified?**	Verified
Auditor Name	Ernst & Young	**Verified?**	Verified
Auditor Website	http://www.ey.com/pl	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1697&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	7/9/2014	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1699&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	7/9/2014	**Verified?**	Verified

EV Audit	https://cert.webtrust.org/SealFile?seal=1698&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	7/9/2014	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.4	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.6: For all SSL certificates, authentication of the Applicant's ownership or control of all requested Domain Name(s) is done using one of the following methods: - by uploading file with the specified name to the root directory of the domain; - by uploading specific metadata to the main page on the domain; - by uploading specific metadata to the DNS text record of the domain; - by direct confirmation with the contact listed by the Domain Name Registrar in the WHOIS record or provided to CERTUM by the Domain Name Registrar directly; - by successfully replying to a challenge response email sent to one or more of the following email addresses: owebmaster@domain.com, postmaster@domain, admin@domain.com, administrator@domain.com, hostmaster@domain.com. CERTUM only uses the WHOIS records linked to on the IANA root database and the ICANN approved registrars.	**Verified?**	Verified
EV SSL Verification Procedures	CPS section 3.2.2: The 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 shall be applied according to Guidelines for the Issuance and Management of Extended Validation Certificates requirements.	**Verified?**	Verified
Organization Verification Procedures	CPS section 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2: In the case of email certificates, the 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.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	CP section 2.6: "Certificates issued by Certum Code Signing CA provide a high level of confidence the identity of the subscriber, but the usage of the certificates is limited to code signing only. Detailed information on identity verification requirements are described in at http://www.certum.pl." NEED CLARIFICATION: Where is this "Detailed information on identity verification requirements are described in at http://www.certum.pl."? Where is it documented that the identity and authority of the Code Signing cert subscriber must be validated?	**Verified?**	Need Clarification From CA

Multi-Factor Authentication	NEED CLARIFICATION: Where is it documented that multi-factor authentication is required for all accounts capable of directly causing certificate issuance, as per Baseline Requirements section 16.5?	**Verified?**	Need Clarification From CA
Network Security	CPS section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.certum.eu/certum/cert,expertise_root_certificates.xml	**Verified?**	Verified