Print this page

Mozilla - CA Program

Case Information

Case Number	00000049	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Unizeto Certum	**Request Status**	Ready for Public Discussion

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

CA Email Alias 1	info@certum.pl		
CA Email Alias 2			
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	* DNS names go in SAN -- CPS Table 7.1: commonName (in the case of server certificates: contain a single IP address or a domain name that is one of the values contained in the certificate's subjectAltName extension) * CPS section 3.1.1: In the case of SSL certificates CERTUM employs an automated process that prevent the release of	**Verified?**	Verified

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	Ready for Public Discussion	**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=8614648	**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.	**Verified?**	Verified
Revocation Tested	http://certificate.revocationcheck.com/valid-certum-ctncav2.certificates.certum.pl No errors	**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, { 0xB6, 0x76, 0xF2, 0xED, 0xDA, 0xE8, 0x77, 0x5C, 0xD3, 0x6C, 0xB0, 0xF6, 0x3C, 0xD1, 0xD4, 0x60, 0x39, 0x61, 0xF4, 0x9E, 0x62, 0x65, 0xBA, 0x01, 0x3A, 0x2F, 0x03, 0x07, 0xB6, 0xD0, 0xB8, 0x04 }, "MIGAMQswCQYDVQQGEwJQTDEiMCAGA1UEChMZVW5pemV0byBUZWNobm9sb2dpZXMg" "Uy5BLjEnMCUGA1UECxMeQ2VydHVtIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MSQw" "IgYDVQQDExtDZXJ0dW0gVHJ1c3RlZCBOZXR3b3JrIENBIDI=", "IdbQSk8lD8kyN/yqXhKN6Q==", Success!	**Verified?**	Verified

Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	D3:DD:48:3E:2B:BF:4C:05:E8:AF:10:F5:FA:76:26:CF:D3:DC:30:92	**Verified?**	Verified
SHA-256 Fingerprint	B6:76:F2:ED:DA:E8:77:5C:D3:6C:B0:F6:3C:D1:D4:60:39:61:F4:9E:62:65:BA:01:3A:2F:03:07:B6:D0:B8:04	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	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. DV certificates are issued for two separate groups. As a free test certificates for shorter period of validity and the standard certificates with a full usage. Certificates of the first group are issued by intermediate authorities Certum Level I CA, Certum Class 1 CA and Certum Class 1 CA SHA2. The second group of standard certificates are issued by Certum Level II CA and Certum Domain Validation CA SHA2 authorities.	**Verified?**	Verified
Externally Operated SubCAs	None. CPS section 1.3.1.2: 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). However, certificates issued to other CAs are subject to the exclusive control of CERTUM. Also, issuing of end user certificates by these authorities is exclusively under control of the CERTUM.	**Verified?**	Verified
Cross Signing	Certum Trusted Network CA 2 will be crossed with Certum CA. Similarly as the previous Root CA (Certum Trusted Network CA).	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	External RAs (Registration Points) are not allowed to validate certificates' DN. This means that only the Primary Registration Point have exclusive right and technical capabilities to verify subscriber's right to use the domain name and the email address.	**Verified?**	Verified

	* 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 provided 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/cert_doc/pc_nuc/CCP-DK02-ZK01_Certification_Policy_of_CERTUM_Certification_Services_v3_4_1.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.certum.eu/upload_module/wysiwyg/certum/eu/documents/CCP-DK02-ZK02_Certification_Practice_Statement_v3_9.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/servlet/pl.id.sys.servlets.FileDownloadServlet?filename=/upload_module/wysiwyg/certum/cert_doc/cps/CCP-DK02-ZK02_CSP_v3_9.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=1901&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/26/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1903&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/26/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1902&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified

EV Audit Statement Date	6/26/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.4	**Verified?**	Verified
SSL Verification Procedures	CP section 2.1: Test certificates are intended mainly for the application or device test performance prior to purchasing final certificate. DV certificates are issued for all types of applications: securing electronic correspondence, encrypting binary objects and protecting data transmission. CERTUM verifies all data provided by subscriber in the certification process. The verification covers: a domain name, an email address, contact details and the name of private person or representative of the legal entity. Detailed information on identity verification requirements are described in [the CPS] 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 2.4: CERTUM verifies all data provided by the requesters during the certification process. Detailed information on identity verification requirements are described in Certification Practice Statement of CERTUM's Certification Services and on the website http://www.certum.eu. https://www.certum.eu/certum/cert,offer_en_standard_code_signing.xml	**Verified?**	Verified
Multi-Factor Authentication	CPS section 4.3.1: The issuance procedure is the following: - any certification request is recorded and verified at the Primary Registration Point, - only persons performing trusted roles have access to operational accounts of the Primary Registration Point. Using the accounts is protected by multi-level authentication and enables the processing of certificate application including the ability to submit an appropriately formatted certificate request to the issuing CA,	**Verified?**	Verified
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