Print this page

Mozilla - CA Program

Case Information

Case Number	00000079	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Dhimyotis / Certigna	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Include renewed Certigna Root	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1265683

General information about CA's associated organization

CA Email Alias 1	security@dhimyotis.com		
CA Email Alias 2			
Company Website	http://www.certigna.fr/	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	France, Europe	**Verified?**	Verified
Primary Market / Customer Base	Dhimyotis is the name of the company and Certigna is the brand for their certificates.	**Verified?**	Verified
Impact to Mozilla Users	DHIMYOTIS is one of the biggest French CAs which issues qualified certificates for general public, public administrations and privates companies. The CA focus its activities in France and worldwide. DHIMYOTIS has already sold certificates to more than 10,000 customers worldwide. .	**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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices 1) Publicly Available CP and CPS: Yes	**Verified?**	Verified

Recommended Practices	2) CA Hierarchy: Yes 3) Audit Criteria: Yes 4) Document Handling of IDNs in CP/CPS: Yes, but our CAs don't allow the use of IDNs in certificates. 5) Revocation of Compromised Certificates: Yes 6) Verifying Domain Name Ownership: Yes 7) Verifying Email Address Control: Yes 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates. 9) DNS names go in SAN: Yes 10) Domain owned by a Natural Person: Yes 11) OCSP: Yes 12) Network Security Controls: Yes

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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices 1) Long-lived DV certificates: No, CAs don't issue Long-lived DV certificates 2) Wildcard DV SSL certificates: Wildcard OV SSL certs are issued. 3) Email Address Prefixes for DV Certs: No, CAs don't issue DV certificates 4) Delegation of Domain / Email validation to third parties: No 5) Issuing end entity certificates directly from roots: No 6) Allowing external entities to operate subordinate CAs: No 7) Distributing generated private keys in PKCS#12 files: Only for Identity CA, Authentication and signature key pair are generated and stored in P12 file which is downloaded by the authentified subject through a secured HTTPS channel. 8) Certificates referencing hostnames or private IP addresses: No. The FQDN of SSL certificates are controled and have to be publicaly recognized, but for our SSL Client certificates, it's allowed to use a CN with the syntax <Identity of entity>-<Name of the service>. 9) Issuing SSL Certificates for Internal Domains: No 10) OCSP Responses signed by a certificate under a different root: No 11) SHA-1 Certificates: No 12) Generic names for CAs: No 13) Lack of Communication With End Users: No 14) Backdating the notBefore date: No	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Certigna Root CA	**Root Case No**	R00000114
Request Status	Ready for Public Discussion	**Case Number**	00000079

Certificate Data

Certificate Issuer Common Name	Certigna Root CA
O From Issuer Field	Dhimyotis

OU From Issuer Field	0002 48146308100036
Valid From	2013 Oct 01
Valid To	2033 Oct 01
Certificate Serial Number	00cae91b89f155030da3e6416dc4e3a6e1
Subject	CN=Certigna Root CA, OU=0002 48146308100036, O=Dhimyotis, C=FR
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	2D:0D:52:14:FF:9E:AD:99:24:01:74:20:47:6E:6C:85:27:27:F5:43
SHA-256 Fingerprint	D4:8D:3D:23:EE:DB:50:A4:59:E5:51:97:60:1C:27:77:4B:9D:7B:18:C9:4D:5A:05:95:11:A1:02:50:B9:31:68
Certificate Fingerprint	4D:9E:D8:52:A7:5A:C7:B9:28:23:B4:74:5C:46:28:7F:F5:2A:E2:E9:F1:5F:14:5F:F5:B7:F9:35:2C:2F:B2:3A
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This SHA-256 root certificate will eventually replace the SHA-1 Certigna root certificate that was included via Bugzilla Bug #393166.	**Verified?**	Verified
Root Certificate Download URL	http://autorite.dhimyotis.com/certignarootca.der	**Verified?**	Verified
CRL URL(s)	http://crl.certigna.fr/certignarootca.crl https://www.certigna.fr/autorites/index.xhtml CP/CPS section 4.9.6 next update: 6 days but they are published every 24 hours or after a certificate's revocation. Frequency of updating CRL is described in chapters 2.3 and 4.9.6 of the CP/CPS	**Verified?**	Verified
OCSP URL(s)	URI for SSL certificate: http://servicesca.ocsp.certigna.fr/ Frequency of updating OCSP is described in chapter 4.9.6 of the CP/CPS. The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation : 1 hour	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Apple; Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	N/A	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://valid.servicesca.dhimyotis.com	**Verified?**	Verified
Test Website - Expired	https://expired.servicesca.dhimyotis.com		
Test Website - Revoked	https://revoked.servicesca.dhimyotis.com		

Example Cert	
Test Notes	

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	This error appears to be a bug in the revocation check website, so we already notified the revocation check site owner error: OCSP signing certificate does not contain the OCSP No Check extension	**Verified?**	Verified
CA/Browser Forum Lint Test	This error appears to be a problem in the way we are using the test -- the error is intended for subscriber certs, not root certs Run x509lint: ERROR: Subject with organizationName but without stateOrProvince or localityName	**Verified?**	Verified
Test Website Lint Test	http://cert-checker.allizom.org/ run certlint no errors	**Verified?**	Verified
EV Tested	Not requesting EV treatment	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	Certificate hierarchy diagram : :https://www.certigna.fr/autorites/index.xhtml	**Verified?**	Verified
Externally Operated SubCAs	No any external operated SubCAs	**Verified?**	Verified
Cross Signing	The intermediate CA certificates signed by our new root certificate «Certigna Root CA» are also signed by the root certificate «Certigna» already included in Mozilla program.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No third-parties can directly cause the issuance of certificates. Several External Delegued Registration Authorities are working with DHIMYOTIS but all registrations are validated by the RA of DHIMYOTIS.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are provided in French Root CP: http://politique.certigna.fr/PCcertignarootca.pdf Services CP: http://politique.certigna.fr/PCcertignaservicesca.pdf	**Verified?**	Verified
CA Document Repository	https://www.certigna.fr/autorites/index.xhtml	**Verified?**	Verified
CP Doc Language	French		
CP	http://politique.certigna.fr/PCcertignaservicesca.pdf	**Verified?**	Verified
CP Doc Language	French		
CPS	http://politique.certigna.fr/PCcertignarootca.pdf	**Verified?**	Verified
Other Relevant Documents	Identity CP : http://politique.certigna.fr/PCcertignaidentityca.pdf Identity Plus CP: http://politique.certigna.fr/PCcertignaidentityplusca.pdf Entity CP: http://politique.certigna.fr/PCcertignaentityca.pdf Entity Code signing CP:	**Verified?**	Verified

	http://politique.certigna.fr/PCcertignaentitycsca.pdf Wild CP: http://politique.certigna.fr/PCcertignawildca.pdf FR03 CP: http://politique.certigna.fr/PCfr03.pdf		
Auditor Name	LSTI	**Verified?**	Verified
Auditor Website	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	**Verified?**	Verified
Auditor Qualifications	http://www.acab-c.com/accredited-bodies/	**Verified?**	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8836773	**Verified?**	Verified
Standard Audit Type	ETSI EN 319 411	**Verified?**	Verified
Standard Audit Statement Date	2/3/2017	**Verified?**	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8836773	**Verified?**	Verified
BR Audit Type	ETSI EN 319 411	**Verified?**	Verified
BR Audit Statement Date	2/3/2017	**Verified?**	Verified
EV Audit	Not EV	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	Services CP and Wild CP section 1.1.1.	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8861810	**Verified?**	Verified
SSL Verification Procedures	in the all CP section 3.2, it mentions that "During the certificate request, the email address of the Certificate Manager is verified through sending multiple emails that allow the Certificate Manager to access to his Certigna Customer account ...". Also, in the "service CA" and "wild CA" section 4.2.1, "Validation by RA of the FQDN of the server attached to the certificate, through the use of "WHO IS" websites and of the AFNIC website if applicable".	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment.	**Verified?**	Not Applicable
Organization Verification Procedures	Translation of Service CA and Wild CA Certification Policy, section 3.2.3 : « The RC must demonstrate that he has the right to use the domain included in the FQDN (ownership rights over the domain or right to use the part of the entity right holder). The registration of the futur RC requires the verification of the legal person's identity, RC's identity, and the relationship between the RC and the legal person. The certificate requestfile, send to RA, shall include : - The certificate request (template available on certigna website : http://www.certigna.fr), dated within 3 months, completed and co-signed by a legal representative and the RC, with especially : o The acceptance of the terms and conditions ; o The identity of the server to be used the certificate (FQDN) ; o Identification personal data of the RC ; o Identification information of the legal person ; o Contact information of a legal representative of the entity (name, entity, address, phone number, email) ; o Contact information of the future RC (name, entity, address, phone number, email) ; - A mandate signed and dated less than 3 months, by a legal representative of the entity, designating the future RC as eligible to be RC for the service to which the	**Verified?**	Verified

	certificate should be issued. This mandate must be signed for acceptance by the future RC.		
Email Address Verification Procedures	added in All CP, section 3.2	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	Administrators and operators intervening within the CA system are identified with certificates on token from Certigna Identity Plus CA. Relevant events involved in the management and operation of the IGC are recorded in handwritten form or electronically (by seizure or by automatic generation) and, for purposes of audit. The means for event logs management were checked during the certification audit and are described in the Certification Policies at the section 5.4.	**Verified?**	Verified
Network Security	Services CP section 6.7 DHIMYOTIS confirms the following : - Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements. - Check for mis-issuance of certificates, especially for high-profile domains. - Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. - Ensure Intrusion Detection System and other monitoring software is up-to-date. - Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion. Means are especially described in section 6.7 of Ccertification policies : « Interconnection to public networks is protected by security gateways configured to accept only the necessary protocols to the desired operation by AC. The network features include two firewalls (clustered on) with integrated intrusion detection system (IPS with alerting). The CA guarantees that the components of the local network are kept in a physically secure environment and their configurations are periodically audited for compliance with the requirements specified by the AC. »	**Verified?**	Verified