Bugzilla ID:
Bugzilla Summary:

CAs wishing to have their certificates included in Mozilla products must
1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.

a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the associated organization of the CA

CA Company Name	Certigna Root CA
Website URL	www.dhimyotis.com; www.certigna.fr
Organizational type	Private corporation. Dhimyotis is the name of the company and Certigna is the brand for their certificates.
Primary market / customer base	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 worldwilde.
Impact to Mozilla Users	DHIMYOTIS has already sold certificates to more than 10 000 customers worldwilde. Most of them are using Mozilla and we would like to ensure that the provider confirms that our products are secured and certified.
Inclusion in other major browsers	Inclusion in the browsers of APPLE and MICROSOFT is in progress.
CA Primary Point of Contact (POC)	CA Email Alias : security@dhimyotis.com CA Phone number : +333 20 79 24 09 Chief Information Security Officer Mr Josselin ALLEMANDOU Email : j.allemandou@dhimyotis.com R&D Director : Mr Yannick LEPLARD Email : y.leplard@dhimyotis.com

Technical information about each root certificate

Certificate Name	Certigna Root CA

Certificate Issuer Field	CN = Certigna Root CA
	OU = 0002 48146308100036
	O = Dhimyotis
	C = FR

Certificate Summary	The Certigna root has 7 internally operated subordinated CAs : – Identity CA : encipherment, authentication and/or digitally-signed email – Identity Plus CA : authentication and/or digitally-signed email – Entity CA : seal (EKU : emailProtection or timeStamping) – Entity Code signing CA : seal (EKU : codeSigning) – Services CA : SSL (EKU : authServer and/or authClient) – Wild CA : SSL (EKU : authServer and authClient) – FR03 : Seal
Root Certificate URL	URL 1 : http://autorite.certigna.fr/certignarootca.der URL 2 : http://autorite.dhimyotis.com/certignarootca.der
SHA1 Fingerprint	2D 0D 52 14 FF 9E AD 99 24 01 74 20 47 6E 6C 85 27 27 F5 43
SHA2 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
Valid From	2013-10-01
Valid To	2033-10-01
Certificate Version	Version 3
Certificate Signature Algorithm	sha256RSA
Signing key parameters	RSA 4096 bits
Test website URL (SSL)	https://test.dhimyotis.com
CRL URL	Root CA : – http://crl.certigna.fr/certignarootca.crl – nextUpdate : 1 year Subordinated CAs : – https://www.certigna.fr/autorites/index.xhtml – nextUpdate : 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.

OCSP URL	URI for SSL certificates : 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
Requested rust Bits	Websites Email Code Signing
SSL Validation Type	OVCP/PTC-BR QCP-w EVCP/PTC-BR
EV Policy OID(s)	QCP-w + EVCP : 1.2.250.1.177.2.5.1.3.1

CA Hierarchy information for each root certificate

CA Hierarchy	URL of certificate hierarchy diagram : : https://www.certigna.fr/autorites/index.xhtml			
	Certigna Root CA	**Key CertSign (5) + CRL Sign (6)**		
	Identity CA	**Key CertSign (5) + CRL Sign (6)**	**ETSI EN 319 411-1**	
	Chiffrement	Key Encipherment (2)	ETSI EN 319 411-1 LCP	
	ID RGS*	Digital Signature (0) + Non Repudiation (1)	ETSI EN 319 411-1 NCP+	
	Identity Plus CA	**Key CertSign (5) + CRL Sign (6)**	**ETSI EN 319 411-1**	
	ID RGS**	Digital Signature (0) + Non Repudiation (1)	ETSI EN 319 411-2 QCP-n-qscd	
	ID RGS***	Non Repudiation (1)	ETSI EN 319 411-2 QCP-n-qscd	
	Authentification RGS ***	Digital Signature (0)	ETSI EN 319 411-1 NCP+	
	Entity CA	**Key CertSign (5) + CRL Sign (6)**	**ETSI EN 319 411-1**	
	Cachet Serveur RGS *	Digital Signature (0) + Non Repudiation (1)	ETSI EN 319 411-1 LCP	
	Cachet Serveur RGS **	Digital Signature (0) + Non Repudiation (1)	ETSI EN 319 411-2 QCP-l-qscd	
	Entity Code Signing CA	**Key CertSign (5) + CRL Sign (6)**	**ETSI EN 319 411-1**	
	Signature de code RGS*	Digital Signature (0)	ETSI EN 319 411-1 LCP	
	Signature de code RGS**	Digital Signature (0)	ETSI EN 319 411-2 QCP-l-qscd	
	Services CA	**Key CertSign (5) + CRL Sign (6)**	**ETSI EN 319 411-1**	
	SSL Serveur RGS*	Digital Signature (0) + Key Encipherment (2)	ETSI EN 319 411-1 LCP	OVCP/PTC BR
	SSL Client RGS*	Digital Signature (0) + Key Encipherment (2)	ETSI EN 319 411-1 LCP	OVCP/PTC BR
	SSL EV/Qualified	Digital Signature (0) + Key Encipherment (2)	ETSI EN 319 411-2 QCP-w	EVCP/PTC-BR
	Wild CA	**Key CertSign (5) + CRL Sign (6)**	**ETSI EN 319 411-1**	
	SSL	Digital Signature (0) + Key Encipherment (2)	ETSI EN 319 411-1 LCP	OVCP/PTC BR
	SSL Wildcard	Digital Signature (0) + Key Encipherment (2)	ETSI EN 319 411-1 LCP	OVCP/PTC BR
	FR03	**Key CertSign (5) + CRL Sign (6)**	**ETSI EN 319 411-1**	
	Cachet Serveur	Digital Signature (0) + Non Repudiation (1)	ETSI EN 319 411-1 LCP	
Externally Operated SubCAs	We do not have any external operated SubCAs.			
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.			
Technical Constraints on Third-party Issuers	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.			

Verification Policies and Practices

Policy Documentation	Documents are provided in French.
CA Document Repository	https://www.certigna.fr/autorites/index.xhtml
CP Doc Language	French
CP	– Certigna Root CA : http://politique.certigna.fr/PCcertignarootca.pdf – Identity CA : http://politique.certigna.fr/PCcertignaidentityca.pdf – Identity Plus CA : http://politique.certigna.fr/PCcertignaidentityplusca.pdf – Entity CA : http://politique.certigna.fr/PCcertignaentityca.pdf – Entity Code signing CA : http://politique.certigna.fr/PCcertignaentitycsca.pdf – Services CA : http://politique.certigna.fr/PCcertignaservicesca.pdf – Wild CA : http://politique.certigna.fr/PCcertignawildca.pdf – FR03 : http://politique.certigna.fr/PCfr03.pdf
CPS Doc Language	French
CPS	https://www.certigna.fr/autorites/index.xhtml
Other Relevant Documents	https://www.certigna.fr/autorites/index.xhtml
Auditor Name	LSTI
Auditor Website	http://www.lsti-certification.fr
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx
Standard Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe
Standard Audit Type	ETSI EN 319 411-1 / 319 411-2
Standard Audit Statement Date	01-20-2018
BR Audit	Attachment LSTI – Attestation letter 2018.pdf
BR Audit Type	ETSI EN 319 411-1 / 319 411-2 / PTC BR / EV BR
BR Audit Statement Date	01-20-2018
EV Audit	Attachment LSTI – Attestation letter 2018.pdf
EV Audit Type	ETSI EN 319 411-1 / 319 411-2 / PTC BR / EVCG
EV Audit Statement Date	01-20-2018
BR Commitment to Comply	Commitment to comply with CA/Browser Forum Baseline Requirements is formalized in section 1.1.1 of the Certification Policies. Compliance with CA/Browser Forum Baseline Requirements is controlled during the certification audit achieved by LSTI.

	Translation of Certification Policies, section 1.1.1 : *« This CP seeks compliance with PC type […] of General Security Referential (RGS) developed by the National Security Agency Information Systems (ANSSI) and requirements of the CA / Browser Forum. »*

SSL Verification Procedures	Translation of Service CA and Wild CA Certification Policy, section 3.2.3 : To note : RC is an authorized representative of the legal person in charge of certificate management. *« 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 request folder, send to RA, shall include :* – *The certificate request (form 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 :* ○ *The acceptance of the terms and conditions ;* ○ *The identity of the server to be used the certificate (FQDN) ;* ○ *Identification personal data of the RC ;* ○ *Identification information of the legal person ;* ○ *Contact information of a legal representative of the entity (name, entity, address, phone number, email) ;* ○ *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 certificate should be issued. This mandate must be signed for acceptance by the future RC. »* WHOIS and AFNIC website are used by RA for checking ownership/control of the domain name for SSL certificate applications.

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 :* ○ *The acceptance of the terms and conditions ;* ○ *The identity of the server to be used the certificate (FQDN) ;* ○ *Identification personal data of the RC ;* ○ *Identification information of the legal person ;* ○ *Contact information of a legal representative of the entity (name, entity, address, phone number, email) ;* ○ *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 certificate should be issued. This mandate must be signed for acceptance by the future RC.* − *A photocopy of a valid identity official document of the futur RC or a professional card issued by an administrative authority with a passeport photograph or a reference to the administrative file of the agent.* − *A photocopy of a valid identity official document of the legal representative or a professional card issued by an administrative authority with a passeport photograph or a reference to the administrative file of the agent.* − *Identification informations of the legal person :* ○ *For a company :* ▪ *A document attesting to the quality of legal representative (eg : a copy of the articles of the company, valid, including the signature of its representatives) ;* ▪ *Any document, valid at the time of registration, with SIREN number of the company or, failing that, another document with the unique identification of the company to be included in the certificate.* − *For administration* ○ *A document, valid at the time of registration, or with delegation or sub-delegation of the authority in charge of administrative structure.* »

Email Address Verification Procedures	Subject's email is controlled during the registration phase, through the exchange of several emails in particular to create the customer account and manage his certificate. If the subject provide a wring email he can not obtain his certificate. Furthermore the email used for registration is always the one inserted in the subject certificate. Translation of Identity CA and Identity Plus CA Certification Policy, section 4.1.2 : *The request file is established either directly by the future subject from the elements provided by the entity or by the entity and signed by the future subject. The file is transmitted directly to the RA if the entity has not implemented a process with MC (representative person).* *The file is delivered to him otherwise. When registrating the future subject, he must provide an email address that allows RA to contact for any questions regarding registration. The MC must also provide an email address when registering, so that RA can make contact with him on all matters relating to registration of subjects. The certificate application must contain the elements described in section 3.2.3.*

Code Signing Subscriber Verification Procedures	Translation of Entity code signing CA Certification Policy, section 3.2.3 : *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 :* ○ *The acceptance of the terms and conditions ;* ○ *The identity of the application service to be used the certificate ;* ○ *Identification personal data of the RC ;* ○ *Identification information of the legal person ;* ○ *Contact information of a legal representative of the entity (name, entity, address, phone number, email) ;* ○ *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 certificate should be issued. This mandate must be signed for acceptance by the future RC.* − *A photocopy of a valid identity official document of the futur RC or a professional card issued by an administrative authority with a passeport photograph or a reference to the administrative file of the agent.*

	− A photocopy of a valid identity official document of the legal representative or a professional card issued by an administrative authority with a passeport photograph or a reference to the administrative file of the agent. − Identification informations of the legal person : ○ For a company : ▪ A document attesting to the quality of legal representative (eg : a copy of the articles of the company, valid, including the signature of its representatives) ; ▪ Any document, valid at the time of registration, with SIREN number of the company or, failing that, another document with the unique identification of the company to be included in the certificate. − For administration ○ A document, valid at the time of registration, or with delegation or sub-delegation of the authority in charge of administrative structure. » ** level Authentication of RC by RA is performed during a physical face-to-face or in dematerialized form provided that the application be signed by the RC with a process for at least comply with electronic signature ** level requirements and the signature is verified and valid at the time of registration. * level Authentication of future RC by RA is achieved by sending the file either by mail or in paperless form (scanned file and then e-mailed).

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.
Network Security	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. »*