Mozilla - CA Program

Case Number	00000033	Case Record Type	CA Owne	r/Root Inclusion Request
CA Owner/Certificate Name	DocuSign (OpenTrust/Keynectis)	Request Status		Public Discussion
dditional Case Info	ormation			
Subject	CertPlus root renewal request	Case Reason	New Own	er/Root inclusion requested
ugzilla Informatior	1			
Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1025095			
eneral information	about CA's associated organization			
CA Email Alias 1	rcprogram@docusign.com			
CA Email Alias 2				
Company Website	https://www.opentrustdtm.com/	Verified?	Verified	
Organizational Type	Private Corporation	Verified?	Verified	
Organizational Type (Others)		Verified?	Not Appli	cable
Geographic Focus	EMEA	Verified?	Verified	
Primary Market / Customer Base	The company is known as Keynectis, with the Certplus and OpenTrust brands. Issues certs to public or private corporations, associations.	Verified?	Verified	
npact to Mozilla Users	Renew already registered root certificate (Certplus Class 2 expiring in 2019) with five different CA certificates for the next 24 years based upon different characteristics: - Two brandings: existing one "Certplus" and the new one "OpenTrust" - Different technologies about keys and algorithms: RSA/ECC, SHA 256 / 512 / ECC	Verified?	Verified	
esponse to Mozilla	a's list of Recommended Practices			
Recommended Practices /	nttps://wiki.mozilla.org CA:Recommended_Practices#CA_Recommended_Pr		mmended 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.
		9: IDN	Verified?	Verified

4.9.1.3

* DNS names go in SAN - SSL CP section 7.1.1.2 * Domain owned by a Natural Person - SSL CP section 7.1.1.2, Comment #9: domain owned by natural person is only possible for DV certificate (not authorized for OV, French RGS and EV SSL). SAN shall be filled with at least one entry and one of the entries shall be placed in the CN of the DN of the subject.

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.
A's Response to Problematic Practices	* DV and OV Certificates include a wildcard asterisk character. Before issuing a Wildcard certificate, RA verifies that rules given in section "11.1.3 Wildcard Domain Validation" from CAB Forum requirements for SSL/TLS certificate are respected.	Verified?	Verified
	* Distributing generated private keys in PKCS#12 files - Comment #9: CAs may be authorized by OpenTrust to issue such key pair and associated certificate. OpenTrust's has a CA who provides Pkcs#12 key pair and the process is audited each year by external entity (LSTI) according RGS and ETSI rules (102 042) and uses a HSM certified EAL4+ or FIPS 140-2 level 3. But for SSL/TLS certificate, OpenTrust doesn't generate the key for Subscriber.		
	* Both external CAs and External RAs are allowed. RCA's CP describes how Root CA, ICA and all CA (OpenTrust's CA and Customer's CA) are audited. Please refer to section 1.4, 4.1, 4.2 and 8 of the RCA's CP. Comment #9: In addition to that and as already explained in this section and in the RCA's CP, OpenTrust's PMA audits and approves all procedures from external entities signed by RCA. This control covers all PKI component of the PKI whom CA is signed by OpenTrust's RCA or ICA (refer to section 8 of RCA's CP). Additionally to that, when external entity is only RA for OpenTrust's CA, a contract shall be established between OpenTrust and external entity and the contract reference the		
	procedure approved by PMA and that have to be used by RA. A contract is also required when a CA wants to get signed by OpenTrust.		
	RCA CP section 8.1: According level of trust chosen for each type of Subscriber Certificate, audit of the CA (means all PKI component used by CA and RA and sample of Local Registration authority according the need of audit) shall be conducted with the following rules: - CA issue Subscriber Certificate for External Subscriber:		
	o For DV SSL certificate: level of Trust shall be [ETSI 102 042] for DVCP plus relevant "CA:Information checklist" as described in [Mozilla]. Customer shall be successfully audited against this standard by external qualified auditor according schema 1, 2 or 3. o For OV SSL certificate: level of Trust shall be [ETSI 102 042] for		
	OVCP plus relevant "CA:Information checklist" as described in [Mozilla]. Customer shall be successfully audited against this standard by external qualified auditor according schema 1, 2 or 3. o For EV SSL certificate: level of Trust shall be at minimum [ETSI 102.0421 for EV CD plus relevant" of the formation checklist" on		
	102 042] for EVCP plus relevant "CA:Information checklist" as described in [Mozilla]. Customer may choose also [ETSI 102 042] for EVCP+. Customer shall be successfully audited		

against this standard by external qualified auditor according schema 1, 2 or 3. o For other type of Subscriber certificate: any level of trust among [ETSI 102 042] and [ETSI 101 456] plus relevant "CA:Information checklist" as described in [Mozilla]. One level of trust for each type of Subscriber Certificate. Customer shall be successfully audited against all required standards for each type of Subscriber Certificate by auditor approved by PMA according schema 1, 2, 3 or 4.

Root Case Record # 1

Root Case Information

Root Certificate Name	Certplus Root CA G1	Root Case No	R0000037
Request Status	Ready for Public Discussion	Case Number	0000033

Additional Root Case Information

Subject Include Certplus Root CA G1

Ready for Public Discussion

Technical Information about Root Certificate

O From Issuer Field	Certplus	Verified?	Verified
OU From Issuer Field		Verified?	Verified
Certificate Summary	This root certificate will replace the already included "Certplus Class 2", with our old brand name, and different crypto parameters (SHA512, RSA4096); certificates to be produced are TLS, Email, Code Signing.	Verified?	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8446784	Verified?	Verified
Valid From	2014 May 26	Verified?	Verified
Valid To	2038 Jan 15	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://certplusrootcag1-test.opentrust.com Must use a new profile to test, see https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c18	Verified?	Verified
CRL URL(s)	http://get-crl.certificat.com/public/certplusrootcag1.crl	Verified?	Verified
OCSP URL(s)	http://get-ocsp.certificat.com/certplusrootcag1 SSL CP section 4.10.1: maximum expiration time of ten days	Verified?	Verified
Revocation Tested	http://certificate.revocationcheck.com/certplusrootcag1-test.opentrust.com No errors	Verified?	Verified
Trust Bits	Code; Email; Websites	Verified?	Verified

0000033

SSL Validation Type	,,	EV			Verified?	Verifie	d
EV Policy OID(s)		4.1.22234.3.5.3.1			Verified?	Verifie	d
EV Tested	"1.3.6.1 "Certplu SEC_OI { 0x15, (0x22, 0x 0xB0, 0 "MD4xC "dHBsd	ertplus Root CA G1,O=Certplus,C=FR 4.1.22234.3.5.3.1", s EV OID a", ID_UNKNOWN, 0x2A, 0x40, 0x2B, 0xFC, 0xDF, 0x2C, 0xD5, 0x48, x75, 0xB3, 0x9C, 0x7F, 0xCA, 0x3E, 0xC0, 0x97, 0x xF0, 0xEA, 0x76, 0xE5, 0x61, 0xA6, 0xC7, 0x43, 0x xzAJBgNVBAYTAkZSMREwDwYDVQQKDAhDZXJ XMgUm9vdCBDQSBHMQ==", +QtPIRWhS2DN7cs3EYR", s!	x80, 0x78, x3E },	1UEAwwTQ2Vy	Verified?	Verifie	d
Root Stores Included In	Microso	ft			Verified?	Verifie	d
Mozilla Applied Constraints	None				Verified?	Verifie	d
Digital Fing	gerprint lı	nformation					
SHA-1 Fingerprint	22:FD:D0	B7:FD:A2:4E:0D:AC:49:2C:A0:AC:A6:7B:6A:1F:E	:F7:66		Ve	rified?	Verifie
SHA-256 Fingerprint	15:2A:40:	2B:FC:DF:2C:D5:48:05:4D:22:75:B3:9C:7F:CA:3E:	C0:97:80:78:B0:F0	:EA:76:E5:61:A6	:C7:43:3E Ve	rified?	Verifie
CA Hierarc	:hy Inforn Hierarchy	Certplus Root CA G1 issued: - EV CA: KEYNECTIS Extended Validation CA	Verified?	Verified			
Externally	Operated SubCAs	Currently none, but the CP does allow for external CAs. RCA CP section 1.1: The present CP represents the common requirements that RCAs, ICAs and CAs have to enforce to be signed by a RCA or an ICA and designates standards to be implemented by a CA in order to issue Subscriber (or Subject) Certificates. OpenTrust manages its RCA certificates lifecycle as detailed in [ETSI 102 042] and [ETSI 101 456]. CAs signed by a RCA or an ICA shall be audited against ETSI standards (102 042 and/or 101 456) or WebTrust (http://www.webtrust.org /item64428.aspx) or according to rules defined by [Adobe] for all types of Subscriber certificates it issues and in the certification path of the RCA. In case the CA issues SSL and / or email certificates, as an alternative to the above audits, this CA may be technically constrained in the CA certificate and audited by Opentrust.	Verified?	Verified			
Cros	ss Signing	One existing EV SSL CA that has been cross certified with this new root CA (for EV SSL issuance). This CA is the one used to issue EV SSL certificates under the Certplus Class 2 already included within major browsers and OS.	Verified?	Verified			

Technical Constr on 3rd party Is:			
/erification Pol	icies and Practices		
Policy Documentation	In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement) In § K.SSL / Club SSL / ISP SSL EV SSL CPS = Politique de Certification SSL Extended Validation (Version anglaise)	Verified?	Verified
	Some documents are also available in English: https://www.opentrustdtm.com/security-policies/?lang=en		
CA Document Repository	https://www.opentrustdtm.com/security-policies/?lang=en	Verified?	Verified
CP Doc Language	English		
CP	https://www.opentrustdtm.com//wp-content/uploads/2015/03/OpenTrust_DMS_RCA- Program_OpenTrust_CP-v-1.2s2.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.opentrustdtm.com//wp-content/uploads/2015/03 /OpenTrust_DMS_EV_SSL_CA_Certification_Practice_Statement_2014_12_18s.pdf	Verified?	Verified
Other Relevant Documents	SSL CP (French): <u>https://www.opentrustdtm.com/wp-content/uploads/2015/11</u> /OpenTrust_DMS_PC-Certificats-OpenTrust-SSL-RGS-et-ETSI-V15.pdf EV CPS (English): <u>https://www.opentrustdtm.com//wp-content/uploads/2015/03</u> /OpenTrust_DMS_EV_SSL_CA_Certification_Practice_Statement_2014_12_18s.pdf	Verified?	Verified
	RCA CP (English): <u>https://www.opentrustdtm.com//wp-content/uploads/2015/03</u> /OpenTrust_DMS_RCA-Program_OpenTrust_CP-v-1.2s2.pdf		
Auditor Name	LSTI	Verified?	Verified
Auditor Website	http://lsti-certification.fr/	Verified?	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	Verified?	Verified
Standard Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	Verified?	Verified
Standard Addit			

Standard Audit Statement Date	4/9/2015	Verified?	Verified
BR Audit	https://bug1025095.bugzilla.mozilla.org/attachment.cgi?id=8590352	Verified?	Verified
BR Audit Type	ETSI TS 102 042	Verified?	Verified
BR Audit Statement Date	4/9/2015	Verified?	Verified
EV Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	Verified?	Verified
EV Audit Type	ETSI TS 102 042	Verified?	Verified
EV Audit Statement Date	4/9/2015	Verified?	Verified
BR Commitment to Comply	SSL CP and RCA CP sections 1.1 and 1.2	Verified?	Verified
SSL Verification Procedures	https://bugzilla.mozilla.org/show bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3 4.1.2.1 Certificate non RGS: DV (Domain Validated Certificate) and 4.1.2.2 Certificate non RGS: OV (Organization Validated Certificate) The following information must be included in the SSL certificate request: The information required by RA to contact the TC and the domain owner (phone, email, etc.). At a minimum, an electronic mail address as entered in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the email address contained in the WHOIS or be of the form "admin", "administrator", "webmaster", "hostmaster "or" postmaster "@ <domain name<br="">requested by TB>. The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC.</domain>	Verified?	Verified
EV SSL Verification Procedures	EV CPS section 3.2.2: Authentication of an entity identity is based on the verification of information provided by the entity, in compliance with information verification requirements issued from "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" (refer to [EV SSL, section 11 to 14]). Applicant's existence and identity and Applicant's legal existence (business presence at a physical address), and Applicant's operational existence (business activity), and Verification of Applicant's Domain Name. Further details also provided in the EV CPS. section 3.2.2.4: Checks on domain names are such that the KEYNECTIS EV CA confirms such domain name satisfies the following requirements: 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); Domain registration information in the WHOIS is public and shows the name, physical address, and administrative contact information for the organization. For Government Entity Applicants, the CA relies on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name. 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; Applicant is aware of its registration or exclusive control of the domain name. In case an EV Certificate request is made for a domain name containing mixed character KEYNECTIS EV CA visually compares the domain name with mixed character sets with known high risk domains. If a similarity is found the the EV Certificate Request is flagged as High Risk. The CA performs appropriate additional authentication and verification to be certain that Applicant and the target in question	Verified?	Verified

Verificatio Procedure	n has t	://bugzilla.n translations		P sections 4.1 to				Verified?		fied
Email Addres Verificatio Procedure	n (OTF s conta signa	(OTP code), and OpenTrust signature Portal, transmitted to the email address							Veri	fied
Code Signin Subscribe	er			0 0	ne requirements.			Verified?	Veri	fied
Verification Pr	See			P sections 4.1 t						
Multi-Facto Authenticatio	n all P This	KI compone mean that a	nts." all accounts c	apable of directl	nentication for ad y issue certificate n) to connect to t	e shall use a	a strong	Verified?	Veri	fied
letwork Securit	y RCA	CP section	6.7					Verified?	Veri	fied
ink to Publi	cly Disc	losed and	d Audited s	subordinate	CA Certificate	es				
Publicly Discl Audited s		https://ww	w.opentrustdt	m.com/pc/		Verified?	Verified			
oot Case In	formati	on								
Root Certificate	e Name	Certplus R	oot CA G2		Roc	ot Case No	R00000038			
Root Certificato		•	oot CA G2 Public Discus	sion		ot Case No se Number	R00000038			
	Status	Ready for	Public Discus	sion						
Request	Status	Ready for	Public Discus							
Request	Status OOt Cas	Ready for e Informa	Public Discus tion	A G2						
Request	Status OOt Cas	Ready for e Informa	Public Discus tion	A G2				Verifie	ed?	Verified
Request additional Ro echnical Inf O From Issuer Field OU From	Status oot Cas Subject	Ready for e Informa	Public Discus tion	A G2				Verifie		Verified Verified
Request additional Ro echnical Inf O From Issuer Field OU From	Status oot Cas Subject Certplus This root name, ar	Ready for e Informa Include Ce n about F	Public Discus tion ertplus Root C Root Certifi vill replace th crypto paramo	A G2 Cate		se Number	00000033	Verifie Verifie	ed?	
Request Additional Re Sechnical Inf O From Issuer Field OU From Issuer Field Certificate	Status Subject Cormatio Certplus This root name, ar Email, C	Ready for e Informa Include Ce n about F	Public Discus tion ertplus Root C Root Certifi vill replace th crypto paramo	A G2 Cate	Cas ed "Certplus Cla ECC); certificate	se Number	00000033	Verifie Verifie	ed? ed?	Verified
Request Additional Ro Cechnical Inf O From Issuer Field OU From Issuer Field Certificate Summary Root Certificate Download	Status Subject Cormatio Certplus This root name, ar Email, C	Ready for e Informa Include Ce n about F certificate v ad different ode Signing igzilla.mozil	Public Discus tion ertplus Root C Root Certifi vill replace th crypto paramo	A G2 Cate e already includ eters (SHA384,	Cas ed "Certplus Cla ECC); certificate	se Number	00000033	Verifie Verifie	ed? ed? ed?	Verified Verified
Request additional Ro echnical Inf O From Issuer Field OU From Issuer Field Certificate Summary Root Certificate Download URL	Status Subject Cormatio Certplus This root name, ar Email, C https://bu	Ready for e Informa Include Ce n about F certificate v ad different ode Signing gzilla.mozil	Public Discus tion ertplus Root C Root Certifi vill replace th crypto paramo	A G2 Cate e already includ eters (SHA384,	Cas ed "Certplus Cla ECC); certificate	se Number	00000033	Verifie Verifie Verifie	ed? ed? ed?	Verified Verified Verified
Request additional Ro echnical Inf O From Issuer Field OU From Issuer Field Certificate Summary Certificate Download URL Valid From	Status Subject Certplus This root name, ar Email, C https://bu	Ready for e Informa Include Ce n about F certificate v ad different ode Signing gzilla.mozil	Public Discus tion ertplus Root C Root Certifi vill replace th crypto paramo	A G2 Cate e already includ eters (SHA384,	Cas ed "Certplus Cla ECC); certificate	se Number	00000033	Verifie Verifie Verifie Verifie	ed? ed? ed? ed?	Verified Verified Verified

Signing Key Parameters	ECC P-3	384	Verified?	Verified
Test Website URL (SSL) or Example Cert		ertplusrootcag2-test.opentrust.com Must use a new profile to test, see ugzilla.mozilla.org/show_bug.cgi?id=1025095#c18	Verified?	Verified
CRL URL(s)	http://ge	t-crl.certificat.com/public/certplusrootcag2.crl	Verified?	Verified
OCSP URL(s)		t-ocsp.certificat.com/certplusrootcag2 section 4.10.1: maximum expiration time of ten days	Verified?	Verified
Revocation Tested	<u>http://ce</u> No error	rtificate.revocationcheck.com/certplusrootcag2-test.opentrust.com s	Verified?	Verified
Trust Bits	Code; E	mail; Websites	Verified?	Verified
SSL Validation Type	DV; OV;	EV	Verified?	Verified
EV Policy OID(s)	1.3.6.1.4	4.1.22234.3.5.3.2	Verified?	Verified
EV Tested	"1.3.6.1. "Certplu: SEC_OI { 0x6C, (0xFB, 0) 0xCE, 0: "MD4xC "dHBsd>	ertplus Root CA G2,O=Certplus,C=FR 4.1.22234.3.5.3.2", s EV OID b", D_UNKNOWN, 0xC0, 0x50, 0x41, 0xE6, 0x44, 0x5E, 0x74, 0x69, 0x6C, 0x4C, xC9, 0xF8, 0x0F, 0x54, 0x3B, 0x7E, 0xAB, 0xBB, 0x44, 0xB4, x6F, 0x78, 0x7C, 0x6A, 0x99, 0x71, 0xC4, 0x2F, 0x17 }, zAJBgNVBAYTAkZSMREwDwYDVQQKDAhDZXJ0cGx1czEcMBoGA1UEAwwTQ2Vy" KMgUm9vdCBDQSBHMg==", c6uo+jF5//pAq/Pc7xV",	Verified?	Verified
Root Stores Included In	Microsof	t	Verified?	Verified
Mozilla Applied Constraints	None		Verified?	Verified
Digital Fing	gerprint Ir	nformation		
SHA-1 Fingerprint	4F:65:8E:	1F:E9:06:D8:28:02:E9:54:47:41:C9:54:25:5D:69:CC:1A	Ve	rified? Verifi
SHA-256 Fingerprint	6C:C0:50:	41:E6:44:5E:74:69:6C:4C:FB:C9:F8:0F:54:3B:7E:AB:BB:44:B4:CE:6F:78:7C:6A:99:71:C	4:2F:17 Ve	rified? Verifi
Fingerprint			4:2F:17 Ve	rmea / Verm
Fingerprint			4:2F:17 Vei	ified? Verifi

	WebTrust (<u>http://www.webtrust.org</u> / <u>item64428.aspx</u>) or according to rules defined by [Adobe] for all types of Subscriber certificates it issues and in the certification path of the RCA. In case the CA issues SSL and / or email certificates, as an alternative to the above audits, this CA may be technically constrained in the CA certificate and audited by Opentrust.		
Cross Sigr	ning One existing EV SSL CA that has been cross certified with this new root CA (for EV SSL issuance). This CA is the one used to issue EV SSL certificates under the Certplus Class 2 already included within major browsers and OS. Verified? Verified? Verified?		
Technical Constr on 3rd party Iss	 must be authorized by the PMA prior to issuance. The issuance process will include documenting the following information to be contained in the CA certificate request: For SSL/TLS Certificate and email certificate under [Mozilla] program, choice for the CA certificate between "audit" against ETSI standards, or [CAB Forum] for SSL/TLS, (refer to section 8 below) or "technical constraint" (refer to section 10.3 below). If Subscribers are only internal: Customer may choose to have only "technical constraint". 		
erification Poli	 If some Subscribers are external: Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). icies and Practices 		
erification Policy Policy Documentation	Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). 	Verified?	Verified
Policy	Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). iccies and Practices In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement) In § K.SSL / Club SSL / ISP SSL	Verified?	Verified
Policy	Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). iccies and Practices In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement) In § K.SSL / Club SSL / ISP SSL EV SSL CPS =	Verified?	Verified
Policy	Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). icies and Practices In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement) In § K.SSL / Club SSL / ISP SSL EV SSL CPS = Politique de Certification SSL Extended Validation (Version anglaise) Some documents are also available in English:	Verified? Verified?	Verified
Policy Documentation	Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). icies and Practices In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement) In § K.SSL / Club SSL / ISP SSL EV SSL CPS = Politique de Certification SSL Extended Validation (Version anglaise) Some documents are also available in English: https://www.opentrustdtm.com/security-policies/?lang=en		
Policy Documentation	Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). icies and Practices In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement) In § K.SSL / Club SSL / ISP SSL EV SSL CPS = Politique de Certification SSL Extended Validation (Version anglaise) Some documents are also available in English: https://www.opentrustdtm.com/security-policies/?lang=en https://www.opentrustdtm.com/security-policies/?lang=en	Verified?	
Policy Documentation	Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). icies and Practices In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement) In § K.SSL / Club SSL / ISP SSL EV SSL CPS = Politique de Certification SSL Extended Validation (Version anglaise) Some documents are also available in English: https://www.opentrustdtm.com/security-policies/?lang=en https://www.opentrustdtm.com/security-policies/?lang=en English	Verified?	Verified
Policy Documentation	Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). icies and Practices In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement) In § K.SSL / Club SSL / ISP SSL EV SSL CPS = Politique de Certification SSL Extended Validation (Version anglaise) Some documents are also available in English: https://www.opentrustdtm.com/security-policies/?lang=en https://www.opentrustdtm.com/security-policies/?lang=en English https://www.opentrustdtm.com/wp-content/uploads/2015/03/OpenTrust_DMS_RCA- Program_OpenTrust_CP-v-1.2s2.pdf	Verified? Verified? Verified?	Verified

	/OpenTrust DMS EV SSL CA Certification Practice Statement 2014 12 18s.pdf RCA CP (English): https://www.opentrustdtm.com//wp-content/uploads/2015/03		
	OpenTrust_DMS_RCA-Program_OpenTrust_CP-v-1.2s2.pdf		
Auditor Name	LSTI	Verified?	Verified
Auditor Website	http://lsti-certification.fr/	Verified?	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	Verified?	Verified
Standard Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	Verified?	Verified
Standard Audit Type	ETSI TS 102 042	Verified?	Verified
Standard Audit Statement Date	4/9/2015	Verified?	Verified
BR Audit	https://bug1025095.bugzilla.mozilla.org/attachment.cgi?id=8590352	Verified?	Verified
BR Audit Type	ETSI TS 102 042	Verified?	Verified
BR Audit Statement Date	4/9/2015	Verified?	Verified
EV Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	Verified?	Verified
EV Audit Type	ETSI TS 102 042	Verified?	Verified
EV Audit Statement Date	4/9/2015	Verified?	Verified
BR Commitment to Comply	SSL CP and RCA CP sections 1.1 and 1.2	Verified?	Verified
SSL Verification Procedures	https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3 4.1.2.1 Certificate non RGS: DV (Domain Validated Certificate) and 4.1.2.2 Certificate non RGS: OV (Organization Validated Certificate) The following information must be included in the SSL certificate request: The information required by RA to contact the TC and the domain owner (phone, email, etc.). At a minimum, an electronic mail address as entered in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the email address contained in the WHOIS or be of the form "admin", "administrator", "webmaster", "hostmaster "or" postmaster "@ <domain by="" name="" requested="" tb="">. The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC.</domain>	Verified?	Verified
Verification Procedures	 section 3.2.2: Authentication of an entity identity is based on the verification of information provided by the entity, in compliance with information verification requirements issued from "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" (refer to [EV SSL, section 11 to 14]). Applicant's existence and identity are verified, including; Applicant's legal existence and identity, and Applicant's operational existence (business presence at a physical address), and Applicant's operational existence (business activity), and Verification of Applicant's Domain Name. Further details also provided in the EV CPS. section 3.2.2.4: Checks on domain names are such that the KEYNECTIS EV CA confirms such domain name satisfies the following requirements: 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); Domain registration information in the WHOIS is public and shows the name, physical address, and administrative contact information for the organization. For 		

oject	Include OpenTrust Root CA G1				
atus	Ready for Public Discussion	Case Number	0000033		
ame	OpenTrust Root CA G1	Root Case No	R00000039		
e R	ecord # 3				
	https://www.opentrustdtm.com/pc/	Verified?	Verified		
-		A Certificates		Verified?	Verified
all P This	KI components." mean that all accounts capable of directly	issue certificate shall use a	strong	Verified?	Verified
		requirements.		Verified?	Verified
(OTF conta signa	P code), and OpenTrust signature Portal, tr ained in the certificate request described a ature policy [Form Signing]. This ensures to ature policy [Form Signing].	ransmitted to the email add bove in accordance with th	ress e	Verified?	Verified
				Verified?	Verified
- App is ha holdd - App In ca chan Certi auth	blicant: the registered holder of the domain name; s been granted the exclusive right to use the of the domain name; blicant is aware of its registration or exclus se an EV Certificate request is made for a acter KEYNECTIS EV CA visually compar- acter sets with known high risk domains. If ficate Request is flagged as High Risk. The entication and verification to be certain tha	he domain name by the reg ive control of the domain na domain name containing n es the domain name with m a similarity is found then th e CA performs appropriate	ame. nixed nixed ne EV additional		
	entity Dom - App is 1 ha holde - App In ca chara Certi authe are tl https has t RCA (OTF conta signa Adm Oper See https RCA all PI This authe achara Conta signa Adm Oper See https Cas Cas	entity in the records of the QGIS in Applicant's Domain Name. - Applicant: is the registered holder of the domain name; has been granted the exclusive right to use tholder of the domain name; - Applicant is aware of its registration or exclus In case an EV Certificate request is made for a character KEYNECTIS EV CA visually compar- character sets with known high risk domains. If Certificate Request is flagged as High Risk. Th authentication and verification to be certain that are the same org https://bugzilla.mozilla.org/show_bug.cgi?id=10 has translations of the SSL CP sections 4.1 to RCA CP section 4.1.2: The certificate request if (OTP code), and OpenTrust signature Portal, th contained in the certificate request described a signature policy [Form Signing]. This ensures the Administrator SSL. OpenTrust follow the EV code signing baseline See translations of the SSL CP sections 4.1 to https://bugzilla.mozilla.org/show_bug.cgi?id=10 RCA CP section 6.5.1.2: "Enforce strong auther all PKI components." This mean that all accounts capable of directly authentication (means 2 factors authentication) RCA CP section 6.7 Disclosed and Audited subordinate C ed & https://www.opentrustdtm.com/pc/ cAs function ame OpenTrust Root CA G1 atus Ready for Public Discussion	 Applicant: - is the registered holder of the domain name; or - has been granted the exclusive right to use the domain name by the regishalder of the domain name; Applicant is aware of its registration or exclusive control of the domain name in case an EV Certificate request is made for a domain name with m character KEYNECTIS EV CA visually compares the domain name with m character KEYNECTIS EV CA visually compares the domain name with m character KEYNECTIS EV CA visually compares the domain name with m character KEYNECTIS EV CA visually compares the domain name with m character sets with known high risk domains. If a similarity is found then th Certificate Request is flagged as High Risk. The CA performs appropriate authentication and verification to be certain that Applicant and the target in are the same org https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3. RCA CP section 4.1.2: The certificate request is signed using a temporary (OTP code), and OpenTrust signature Portal, transmitted to the email add contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC Administrator SSL. OpenTrust follow the EV code signing baseline requirements. See translations of the SSL CP sections 4.1 to 4.3 https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 RCA CP section 6.5.1.2: "Enforce strong authentication for administrator and all PKI components." This mean that all accounts capable of directly issue certificate shall use a authentication (means 2 factors authentication) to connect to the PKI system of CAs https://www.opentrustdtm.com/pc/ Ver	entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name Applicant: - 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; - Applicant is aware of its registration or exclusive control of the domain name. In case an EV Certificate request is made for a domain name containing mixed character KEYNECTIS EV CA visually compares the domain name containing mixed character KEYNECTIS EV CA visually compares the domain name containing mixed character KEYNECTIS EV CA visually compares the domain name with mixed character KEYNECTIS EV CA visually compares the domain name with mixed character KEYNECTIS EV CA visually compares the domain name with mixed character sets with known high risk domains. If a similarity is found then the EV Certificate Request is flagged as High Risk. The CA performs appropriate additional authentication and verification to be certain that Applicant and the target in question are the same org https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3. RCA CP section 4.1.2: The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC or the Administrator SSL. OpenTrust follow the EV code signing baseline requirements. See translations of the SSL CP sections 4.1 to 4.3 https://uugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 RCA CP section 6.5.1.2: "Enforce strong authentication for administrator access to all PK components." This mean that all accounts capable of directly issue certificate shall use a strong authentication (means 2 factors authentication) to connect to the PKI system. RCA CP section 6.7 PublicClosed and Audited subordinate CA Certificates ame OpenTrust Root CA	entign in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name: - 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: - Applicant is aware of its registration or exclusive control of the domain name. In case an EV Certificate request is made for a domain name containing mixed character stess with known high risk domains. It a similarity is found then the EV Certificate Request is flagged as High Risk. The CA performs appropriate additional authentication and verification to be certain that Applicant and the target in question are the same org https://bugzilla.mozilla.org/show.bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3. RCA CP section 4.1.2: The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC or the Administrator SSL. QpenTrust follow the EV code signing baseline requirements. Verified? See translations of the SSL CP sections 4.1 to 4.3 https://bugzilla.mozilla.org/show bug.cgi?id=1025095#c24 RCA CP section 6.5.1.2: "Enforce strong authentication for administrator access to all PKI components." This meant that all accounts capable of directly issue certificate shall use a strong authentication (means 2 factors authentication) to connect to the PKI system. RCA CP section 6.7 Verified? Pisclosed and Audited subordinate CA Certificates Applicant Sec. Pisclosed and Audited subordinate CA Certificates Ready for Public Discussion Ready for Public

Certificate This root certificate will replace the already included "Certplus Class 2", with our new Verified? Verified? Summary company name, and different crypto parameters (SHA256, RSA4096); certificates to be produced are TLS, Email, Code Signing. Verified? Verified?	Issuer Field				
		company name, and different crypto parameters (SHA256, RSA4096); certificates to be	Verified?	Verified	

Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8446791	Verified?	Verified	
Valid From	2014 May 26	Verified?	Verified	
Valid To	2038 Jan 15	Verified?	Verified	
Certificate Version	3	Verified?	Verified	
Certificate Signature Algorithm	SHA-256	Verified?	Verified	
Signing Key Parameters	4096	Verified?	Verified	
Test Website URL (SSL) or Example Cert	https://opentrustrootcag1-test.opentrust.com	Verified?	Verified	
CRL URL(s)	http://get-crl.certificat.com/public/opentrustrootcag1.crl	Verified?	Verified	
OCSP URL(s)	http://get-ocsp.certificat.com/opentrustrootcag1 SSL CP section 4.10.1: maximum expiration time of ten days	Verified?	Verified	
Revocation Tested	http://certificate.revocationcheck.com/opentrustrootcag1-test.opentrust.com No errors	Verified?	Verified	
Trust Bits	Code; Email; Websites	Verified?	Verified	
SSL Validation Type	DV; OV; EV	Verified?	Verified	
EV Policy OID(s)	1.3.6.1.4.1.22234.2.14.3.11	Verified?	Verified	
EV Tested	<pre>// CN=OpenTrust Root CA G1,O=OpenTrust,C=FR "1.3.6.1.4.1.22234.2.14.3.11", "OpenTrust EV OID", SEC_OID_UNKNOWN, { 0x56, 0xC7, 0x71, 0x28, 0xD9, 0x8C, 0x18, 0xD9, 0x1B, 0x4C, 0xFD, 0xFF, 0xBC, 0x25, 0xEE, 0x91, 0x03, 0xD4, 0x75, 0x8E, 0xA2, 0xAB, 0xAD, 0x82, 0x6A, 0x90, 0xF3, 0x45, 0x7D, 0x46, 0x0E, 0xB4 }, "MEAxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAIPcGVuVHJ1c3QxHTAbBgNVBAMMFE9w" "ZW5UcnVzdCBSb290IENBIEcx", "ESCzkFU5fX82bWTCp59rY45n", Success!</pre>	Verified?	Verified	
Root Stores Included In	Microsoft	Verified?	Verified	
Mozilla Applied Constraints	None	Verified?	Verified	
Digital Fing	erprint Information			
SHA-1 Fingerprint	79:91:E8:34:F7:E2:EE:DD:08:95:01:52:E9:55:2D:14:E9:58:D5:7E	v	erified?	Verif
SHA-256 Fingerprint	56:C7:71:28:D9:8C:18:D9:1B:4C:FD:FF:BC:25:EE:91:03:D4:75:8E:A2:AB:AD:82:6A:90:F3:45:7D	:46:0E:B4 V	erified?	Verif
CA Hierarc	hy Information			
CA	Hierarchy OpenTrust Root CA G1 issued: Verified? Verified - EV CA: KEYNECTIS Extended Validation CA - AATL CA: OpenTrust CA for AATL G1			

Externally Oper. Sub		Verified?	Verified		
Cross Sig	ning One existing EV SSL CA that has been cross certified with this new root CA (for EV SSL issuance). This CA is the one used to issue EV SSL certificates under the Certplus Class 2 already included within major browsers and OS.	Verified?	Verified		
Technical Constr on 3rd party Is		Verified?	Verified		
/erification Pol	icies and Practices				
Policy Documentation	In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authe seulement)	ntification ser	veur	Verified?	Verified
	In § K.SSL / Club SSL / ISP SSL EV SSL CPS = Politique de Certification SSL Extended Validation (Version a	nglaise)			
	Some documents are also available in English:				
	https://www.opentrustdtm.com/security-policies/?lang=en				

CP Doc Language	English		
СР	https://www.opentrustdtm.com//wp-content/uploads/2015/03/OpenTrust_DMS_RCA- Program_OpenTrust_CP-v-1.2s2.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.opentrustdtm.com//wp-content/uploads/2015/03 /OpenTrust_DMS_EV_SSL_CA_Certification_Practice_Statement_2014_12_18s.pdf	Verified?	Verified
Other Relevant Documents	SSL CP (French): <u>https://www.opentrustdtm.com/wp-content/uploads/2015/11</u> / <u>OpenTrust_DMS_PC-Certificats-OpenTrust-SSL-RGS-et-ETSI-V15.pdf</u> EV CPS (English): <u>https://www.opentrustdtm.com//wp-content/uploads/2015/03</u> / <u>OpenTrust_DMS_EV_SSL_CA_Certification_Practice_Statement_2014_12_18s.pdf</u>	Verified?	Verified
	RCA CP (English): <u>https://www.opentrustdtm.com//wp-content/uploads/2015/03</u> /OpenTrust_DMS_RCA-Program_OpenTrust_CP-v-1.2s2.pdf		
Auditor Name	LSTI	Verified?	Verified
Auditor Website	http://lsti-certification.fr/	Verified?	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	Verified?	Verified
Standard Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	Verified?	Verified
Standard Audit Type	ETSI TS 102 042	Verified?	Verified
Standard Audit Statement Date	4/9/2015	Verified?	Verified
BR Audit	https://bug1025095.bugzilla.mozilla.org/attachment.cgi?id=8590352	Verified?	Verified
BR Audit Type	ETSI TS 102 042	Verified?	Verified
BR Audit Statement Date	4/9/2015	Verified?	Verified
EV Audit	http://www.lsti-certification.fr/images/liste entreprise/Liste%20PSCe.pdf	Verified?	Verified
EV Audit Type	ETSI TS 102 042	Verified?	Verified
EV Audit Statement Date	4/9/2015	Verified?	Verified
BR Commitment to Comply	SSL CP and RCA CP sections 1.1 and 1.2	Verified?	Verified
SSL Verification Procedures	 <u>https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24</u> has translations of the SSL CP sections 4.1 to 4.3 4.1.2.1 Certificate non RGS: DV (Domain Validated Certificate) and 4.1.2.2 Certificate non RGS: OV (Organization Validated Certificate) The following information must be included in the SSL certificate request: The information required by RA to contact the TC and the domain owner (phone, email, etc.). At a minimum, an electronic mail address as entered in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the email address contained in the WHOIS or be of the form "admin", "administrator", "webmaster", "hostmaster "or" postmaster "@ <domain name<br="">requested by TB>.</domain> The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC. 	Verified?	Verified
EV SSL Verification Procedures	EV CPS section 3.2.2: Authentication of an entity identity is based on the verification of information provided by the entity, in compliance with information verification requirements issued from "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" (refer to [EV SSL, section 11 to 14]).	Verified?	Verified

	Applicant's existence and identity are verified, including; - Applicant's legal existence and identity, and - Applicant's physical existence (business presence at a physical address), and - Applicant's operational existence (business activity), and - Verification of Applicant's Domain Name.		
	Further details also provided in the EV CPS.		
	 section 3.2.2.4: Checks on domain names are such that the KEYNECTIS EV CA confirms such domain name satisfies the following requirements: 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); Domain registration information in the WHOIS is public and shows the name, physical address, and administrative contact information for the organization. For Government Entity Applicants, the CA relies on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name. 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; Applicant is aware of its registration or exclusive control of the domain name. In case an EV Certificate request is made for a domain name with mixed character KEYNECTIS EV CA visually compares the domain name with mixed character sets with known high risk domains. If a similarity is found then the EV Certificate Request is flagged as High Risk. The CA performs appropriate additional authentication and verification to be certain that Applicant and the target in question are the same org 		
Organization Verification Procedures	https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3.	Verified?	Verified
Email Address Verification Procedures	RCA CP section 4.1.2: The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC or the Administrator SSL.	Verified?	Verified
Code Signing Subscriber Verification Pro	OpenTrust follow the EV code signing baseline requirements. See translations of the SSL CP sections 4.1 to 4.3 https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24	Verified?	Verified
Multi-Factor Authentication	RCA CP section 6.5.1.2: "Enforce strong authentication for administrator access to all PKI components." This mean that all accounts capable of directly issue certificate shall use a strong authentication (means 2 factors authentication) to connect to the PKI system.	Verified?	Verified
Network Security	RCA CP section 6.7	Verified?	Verified
ink to Publicly	v Disclosed and Audited subordinate CA Certificates		

Publicly Disclosed & https://www.opentrustdtm.com/pc/ Audited subCAs

Verified? Verified

Root Case Record # 4

Root Case Information Root Certificate Name OpenTrust Root CA G2 Root Case No R00000040 Request Status Ready for Public Discussion Case Number 00000033 Additional Root Case Information

Technical Information about Root Certificate

O From Issuer Field	OpenTrust	Verified?	Verified
OU From Issuer Field		Verified?	Verified
Certificate Summary	This root certificate will replace the already included "Certplus Class 2", with our new company name, and different crypto parameters (SHA512, RSA4096); certificates to be produced are TLS, Email, Code Signing.	Verified?	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8446792	Verified?	Verified
Valid From	2014 May 26	Verified?	Verified
Valid To	2038 Jan 15	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://opentrustrootcag2-test.opentrust.com Must use a new profile to test, see https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c18	Verified?	Verified
CRL URL(s)	http://get-crl.certificat.com/public/opentrustrootcag2.crl	Verified?	Verified
OCSP URL(s)	http://get-ocsp.certificat.com/opentrustrootcag2 SSL CP section 4.10.1: maximum expiration time of ten days	Verified?	Verified
Revocation Tested	http://certificate.revocationcheck.com/opentrustrootcag2-test.opentrust.com No errors	Verified?	Verified
Trust Bits	Code; Email; Websites	Verified?	Verified
SSL Validation Type	DV; OV; EV	Verified?	Verified
EV Policy OID(s)	1.3.6.1.4.1.22234.2.14.3.11	Verified?	Verified
EV Tested	<pre>// CN=OpenTrust Root CA G2,O=OpenTrust,C=FR "1.3.6.1.4.1.22234.2.14.3.11", "OpenTrust EV OID", SEC_OID_UNKNOWN, { 0x27, 0x99, 0x58, 0x29, 0xFE, 0x6A, 0x75, 0x15, 0xC1, 0xBF, 0xE8, 0x48, 0xF9, 0xC4, 0x76, 0x1D, 0xB1, 0x6C, 0x22, 0x59, 0x29, 0x25, 0x7B, 0xF4, 0x0D, 0x08, 0x94, 0xF2, 0x9E, 0xA8, 0xBA, 0xF2 }, "MEAxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAIPcGVuVHJ1c3QxHTAbBgNVBAMMFE9w" "ZW5UcnVzdCBSb290IENBIEcy", "ESChaRu/vbm9UpaPI+hlvyYR", Success!</pre>	Verified?	Verified
Root Stores Included In	Microsoft	Verified?	Verified
Mozilla Applied Constraints	None	Verified?	Verified

Digital Fingerprint Information

SHA-1 Fingerprint 79:5F:88:60:C5:AB:7C:3D:92:E6:CB:F4:8D:E1:45:CD:11:EF:60:0B

Verified? Verified

SHA-256 27:99:58:29:FE:6A:75:15:C1:BF:E8:48:F9:C4:76:1D:B1:6C:22:59:29:25:7B:F4:0D:08:94:F2:9E:A8:BA:F2 Verified? Verified Fingerprint

CA Hierarchy Information

CA Hierarchy	OpenTrust Root CA G2 issued: - EV CA: KEYNECTIS Extended Validation CA - AATL CA: OpenTrust CA for AATL G2	Verified?	Verified
Externally Operated SubCAs	Currently none, but the CP does allow for external CAs. RCA CP section 1.1: The present CP represents the common requirements that RCAs, ICAs and CAs have to enforce to be signed by a RCA or an ICA and designates standards to be implemented by a CA in order to issue Subscriber (or Subject) Certificates. OpenTrust manages its RCA certificates lifecycle as detailed in [ETSI 102 042] and [ETSI 101 456]. CAs signed by a RCA or an ICA shall be audited against ETSI standards (102 042 and/or 101 456) or WebTrust (http://www.webtrust.org /item64428.aspx) or according to rules defined by [Adobe] for all types of Subscriber certificates it issues and in the certification path of the RCA. In case the CA issues SSL and / or email certificates, as an alternative to the above audits, this CA may be technically constrained in the CA certificate and audited by Opentrust.	Verified?	Verified
Cross Signing	One existing EV SSL CA that has been cross certified with this new root CA (for EV SSL issuance). This CA is the one used to issue EV SSL certificates under the Certplus Class 2 already included within major browsers and OS.	Verified?	Verified
Technical Constraint on 3rd party Issuer	RCA CP section 4.1.2.3: CA certificates must be authorized by the PMA prior to issuance. The issuance process will include documenting the following information to be contained in the CA certificate request: For SSL/TLS Certificate and email certificate under [Mozilla] program, choice for the CA certificate between "audit" against ETSI standards, or [CAB Forum] for SSL/TLS, (refer to section 8 below) or "technical constraint" (refer to section 10.3 below). - If Subscribers are only internal: Customer may choose to have only "technical constraint". - If some Subscribers are external: Customer shall choose to have "audit" against ETSI standards (refer to section 8 below).	Verified?	Verified

Policy	In § Certificats OpenTrust SSL RGS et ETSI	Verified?	Verified
Documentation	CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement)		
	In § K.SSL / Club SSL / ISP SSL EV SSL CPS = Politique de Certification SSL Extended Validation (Version anglaise)		
	Some documents are also available in English: https://www.opentrustdtm.com/security-policies/?lang=en		
CA Document Repository	https://www.opentrustdtm.com/security-policies/?lang=en	Verified?	Verified
CP Doc Language	English		
CP	https://www.opentrustdtm.com//wp-content/uploads/2015/03/OpenTrust_DMS_RCA- Program_OpenTrust_CP-v-1.2s2.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.opentrustdtm.com//wp-content/uploads/2015/03 /OpenTrust_DMS_EV_SSL_CA_Certification_Practice_Statement_2014_12_18s.pdf	Verified?	Verified
Other Relevant Documents	SSL CP (French): <u>https://www.opentrustdtm.com/wp-content/uploads/2015/11</u> /OpenTrust_DMS_PC-Certificats-OpenTrust-SSL-RGS-et-ETSI-V15.pdf	Verified?	Verified
	EV CPS (English): <u>https://www.opentrustdtm.com//wp-content/uploads/2015/03</u> /OpenTrust_DMS_EV_SSL_CA_Certification_Practice_Statement_2014_12_18s.pdf		
	RCA CP (English): <u>https://www.opentrustdtm.com//wp-content/uploads/2015/03</u> /OpenTrust_DMS_RCA-Program_OpenTrust_CP-v-1.2s2.pdf		
Auditor Name	LSTI	Verified?	Verified
Auditor Website	http://lsti-certification.fr/	Verified?	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	Verified?	Verified
Standard Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	Verified?	Verified
Standard Audit Type	ETSI TS 102 042	Verified?	Verified
Standard Audit Statement Date	4/9/2015	Verified?	Verified
BR Audit	https://bug1025095.bugzilla.mozilla.org/attachment.cgi?id=8590352	Verified?	Verified
BR Audit Type	ETSI TS 102 042	Verified?	Verified
BR Audit Statement Date	4/9/2015	Verified?	Verified
EV Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	Verified?	Verified
EV Audit Type	ETSI TS 102 042	Verified?	Verified
EV Audit Statement Date	4/9/2015	Verified?	Verified
R Commitment to Comply	SSL CP and RCA CP sections 1.1 and 1.2	Verified?	Verified
SSL Verification Procedures	https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3	Verified?	Verified
	4.1.2.1 Certificate non RGS: DV (Domain Validated Certificate)		

etwork Security	RCA CP section 6.7	Verified?	Verified
Multi-Factor Authentication	RCA CP section 6.5.1.2: "Enforce strong authentication for administrator access to all PKI components." This mean that all accounts capable of directly issue certificate shall use a strong authentication (means 2 factors authentication) to connect to the PKI system.	Verified?	Verified
Code Signing Subscriber Verification Pro	OpenTrust follow the EV code signing baseline requirements. See translations of the SSL CP sections 4.1 to 4.3 https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24	Verified?	Verified
Email Address Verification Procedures	RCA CP section 4.1.2: The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC or the Administrator SSL.	Verified?	Verified
Organization Verification Procedures	https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3.	Verified?	Verified
	certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC. EV CPS section 3.2.2: Authentication of an entity identity is based on the verification requirements issued from "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" (refer to [EV SSL, section 11 to 14]). Applicant's existence and identity, and - Applicant's existence and identity, and - Applicant's operational existence (business presence at a physical address), and - Applicant's operational existence (business activity), and - Verification of Applicant's Domain Name. Further details also provided in the EV CPS. section 3.2.2.4: Checks on domain names are such that the KEYNECTIS EV CA confirms such domain name satisfies the following requirements: - 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); - Domain registration information in the WHOIS is public and shows the name, physical address, and administrative contact information for the organization. For Government Entity Applicants, the CA relies on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name. - 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; if a similarity is found then the EV Certificate request is made for a domain name containing mixed character KEYNECTIS EV CA visually compares the domain name with mixed character KEYNECTIS EV CA visually compares the domain name with mixed character KEYNECTIS EV CA visually compares the domain name with mixed character KEYNECTIS EV CA visually compares the domain name with mixed character KEYNECTIS EV CA visually compares the domain name with mixed character sets with known high risk domains. If a similarit	Verified?	Verified
	email, etc.). At a minimum, an electronic mail address as entered in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the email address contained in the WHOIS or be of the form "admin", "administrator", "webmaster", "hostmaster "or" postmaster "@ <domain by="" name="" requested="" tb="">. The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form</domain>		

Verified? Verified

Root Case I	nformati	on						
Root Certifica	te Name	OpenTrust Ro	ot CA G3	Ro	oot Case No	R00000041		
Reques	st Status	Ready for Put	lic Discussion	Ca	ase Number	0000033		
Additional F	Root Cas	e Informatio	n					
	Subject	Include Open	Trust Root CA G3					
Fechnical In	formatio	on about Roo	ot Certificate					
O From Issuer Field	OpenTr	ust					Verified?	Verified
OU From Issuer Field							Verified?	Verified
Certificate Summary	compan		replace the already incl ferent crypto parameter igning.				Verified?	Verified
Root Certificate Download URL	https://b	ugzilla.mozilla.c	org/attachment.cgi?id=8	446793			Verified?	Verified
Valid From	2014 M	ay 26					Verified?	Verified
Valid To	2038 Ja	n 15					Verified?	Verified
Certificate Version	3						Verified?	Verified
Certificate Signature Algorithm	ECC						Verified?	Verified
Signing Key Parameters	ECC P-	384					Verified?	Verified
Test Website URL (SSL) or Example Cert			3-test.opentrust.com M rg/show_bug.cgi?id=10		ofile to test, se	e	Verified?	Verified
CRL URL(s)	http://ge	t-crl.certificat.co	m/public/opentrustroot	cag3.crl			Verified?	Verified
OCSP URL(s)			.com/opentrustrootcag3 maximum expiration tin				Verified?	Verified
Revocation Tested	http://ce No error		oncheck.com/opentrus	trootcag3-test.ope	entrust.com		Verified?	Verified
Trust Bits	Code; E	mail; Websites					Verified?	Verified
SSL Validation Type	DV; OV	EV					Verified?	Verified
EV Policy OID(s)	1.3.6.1.4	4.1.22234.2.14.	3.11				Verified?	Verified
EV Tested	"1.3.6.1	penTrust Root (.4.1.22234.2.14 rust EV OID",	CA G3,O=OpenTrust,C= .3.11",	=FR			Verified?	Verified

SEC_OID_UNKNOWN, { 0xB7, 0xC3, 0x62, 0x31, 0x70, 0x6E, 0x81, 0x07, 0x8C, 0x36, 0x7C, 0xB8, 0x96, 0x19, 0x8F, 0x1E, 0x32, 0x08, 0xDD, 0x92, 0x69, 0x49, 0xDD, 0x8F, 0x57, 0x09, 0xA4, 0x10, 0xF7, 0x5B, 0x62, 0x92 }, "MEAxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAIPcGVuVHJ1c3QxHTAbBgNVBAMMFE9w" "ZW5UcnVzdCBSb290IENBIEcz", "ESDm+Ez8JLC+BUCs2oMbNGA/", Success! **Root Stores** Microsoft Verified? Verified Included In Mozilla Verified? None Verified Applied Constraints **Digital Fingerprint Information**

 SHA-1 Fingerprint
 6E:26:64:F3:56:BF:34:55:BF:D1:93:3F:7C:01:DE:D8:13:DA:8A:A6
 Verified?
 Verified?

 SHA-256 Fingerprint
 B7:C3:62:31:70:6E:81:07:8C:36:7C:B8:96:19:8F:1E:32:08:DD:92:69:49:DD:8F:57:09:A4:10:F7:5B:62:92
 Verified?
 Verified?

CA Hierarchy Information

CA Hierarchy	OpenTrust Root CA G3 issued: - EV CA: KEYNECTIS Extended Validation CA - AATL CA: OpenTrust CA for AATL G3	Verified?	Verified
Externally Operated SubCAs	Currently none, but the CP does allow for external CAs. RCA CP section 1.1: The present CP represents the common requirements that RCAs, ICAs and CAs have to enforce to be signed by a RCA or an ICA and designates standards to be implemented by a CA in order to issue Subscriber (or Subject) Certificates. OpenTrust manages its RCA certificates lifecycle as detailed in [ETSI 102 042] and [ETSI 101 456]. CAs signed by a RCA or an ICA shall be audited against ETSI standards (102 042 and/or 101 456) or WebTrust (http://www.webtrust.org /item64428.aspx) or according to rules defined by [Adobe] for all types of Subscriber certificates it issues and in the certification path of the RCA. In case the CA issues SSL and / or email certificates, as an alternative to the above audits, this CA may be technically constrained in the CA certificate and audited by Opentrust.	Verified?	Verified
Cross Signing	One existing EV SSL CA that has been cross certified with this new root CA (for EV SSL issuance). This CA is the one used to issue EV SSL certificates under the Certplus Class 2 already included within major browsers and OS.	Verified?	Verified
Technical Constraint on 3rd party Issuer	RCA CP section 4.1.2.3: CA certificates must be authorized by the PMA prior to issuance. The issuance process will include documenting the following information to be contained in the CA certificate request: For SSL/TLS Certificate and email	Verified?	Verified

	certificate under [Mozilla] program, choice for the CA certificate between "audit" against ETSI standards, or [CAB Forum] for SSL/TLS, (refer to section 8 below) or "technical constraint" (refer to section 10.3 below). - If Subscribers are only internal: Customer may choose to have only "technical constraint". - If some Subscribers are external: Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). 		
Verification Poli	icies and Practices		
Policy Documentation	In § Certificats OpenTrust SSL RGS et ETSI CP for French RGS and European ETSI SSL certs = Politique de certification des AC SSL RGS et/ou ETSI (authentification serveur seulement) In § K.SSL / Club SSL / ISP SSL EV SSL CPS = Politique de Certification SSL Extended Validation (Version anglaise)	Verified?	Verified
	Some documents are also available in English: https://www.opentrustdtm.com/security-policies/?lang=en		
CA Document Repository	https://www.opentrustdtm.com/security-policies/?lang=en	Verified?	Verified
CP Doc Language	English		
CP	https://www.opentrustdtm.com//wp-content/uploads/2015/03/OpenTrust_DMS_RCA- Program_OpenTrust_CP-v-1.2s2.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.opentrustdtm.com//wp-content/uploads/2015/03 /OpenTrust_DMS_EV_SSL_CA_Certification_Practice_Statement_2014_12_18s.pdf	Verified?	Verified
Other Relevant Documents	SSL CP (French): https://www.opentrustdtm.com/wp-content/uploads/2015/11/0penTrust_DMS_PC-Certificats-OpenTrust-SSL-RGS-et-ETSI-V15.pdf EV CPS (English): https://www.opentrustdtm.com//wp-content/uploads/2015/03/0penTrust_DMS_EV_SSL_CA_Certification_Practice_Statement_2014_12_18s.pdf RCA CP (English): https://www.opentrustdtm.com//wp-content/uploads/2015/03/0penTrust_DMS_RCA-Program_OpenTrust_CP-v-1.2s2.pdf	Verified?	Verified
Auditor Name	LSTI	Verified?	Verified
Auditor Website	http://lsti-certification.fr/	Verified?	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	Verified?	Verified
Standard Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	Verified?	Verified
Standard Audit Type	ETSI TS 102 042	Verified?	Verified
Standard Audit Statement Date	4/9/2015	Verified?	Verified
BR Audit	https://bug1025095.bugzilla.mozilla.org/attachment.cgi?id=8590352	Verified?	Verified
BR Audit Type	ETSI TS 102 042	Verified?	Verified
BR Audit Statement Date	4/9/2015	Verified?	Verified

EV Audit	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	Verified?	Verified
EV Audit Type	ETSI TS 102 042	Verified?	Verified
EV Audit Statement Date	4/9/2015	Verified?	Verified
BR Commitment to Comply	SSL CP and RCA CP sections 1.1 and 1.2	Verified?	Verified
SSL Verification Procedures	https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3 4.1.2.1 Certificate non RGS: DV (Domain Validated Certificate)	Verified?	Verified
	and 4.1.2.2 Certificate non RGS: OV (Organization Validated Certificate) The following information must be included in the SSL certificate request: The information required by RA to contact the TC and the domain owner (phone, email, etc.). At a minimum, an electronic mail address as entered in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the email address contained in the WHOIS or be of the form "admin", "administrator", "webmaster", "hostmaster "or" postmaster "@ <domain name<br="">requested by TB>.</domain>		
	The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC.		
EV SSL Verification Procedures	EV CPS section 3.2.2: Authentication of an entity identity is based on the verification of information provided by the entity, in compliance with information verification requirements issued from "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" (refer to [EV SSL,	Verified?	Verified
	section 11 to 14]). Applicant's existence and identity are verified, including; - Applicant's legal existence and identity, and - Applicant's physical existence (business presence at a physical address), and - Applicant's operational existence (business activity), and - Verification of Applicant's Domain Name.		
	Further details also provided in the EV CPS.		
	 section 3.2.2.4: Checks on domain names are such that the KEYNECTIS EV CA confirms such domain name satisfies the following requirements: 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); Domain registration information in the WHOIS is public and shows the name, physical address, and administrative contact information for the organization. For Government Entity Applicants, the CA relies on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify 		
	Domain Name. - 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; - Applicant is aware of its registration or exclusive control of the domain name. In case an EV Certificate request is made for a domain name containing mixed		
	character KEYNECTIS EV CA visually compares the domain name with mixed character sets with known high risk domains. If a similarity is found then the EV Certificate Request is flagged as High Risk. The CA performs appropriate additional authentication and verification to be certain that Applicant and the target in question are the same org		
Organization Verification Procedures	https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24 has translations of the SSL CP sections 4.1 to 4.3.	Verified?	Verified
Email Address Verification Procedures	RCA CP section 4.1.2: The certificate request is signed using a temporary password (OTP code), and OpenTrust signature Portal, transmitted to the email address contained in the certificate request described above in accordance with the signature policy [Form Signing]. This ensures the email address of the TC or the Administrator SSL.	Verified?	Verified

Code Signing Subscriber Verification Pro	OpenTrust follow the EV code signing baseline requirements.	Verified?	Verified
	See translations of the SSL CP sections 4.1 to 4.3 https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c24		
Multi-Factor Authentication	RCA CP section 6.5.1.2: "Enforce strong authentication for administrator access to all PKI components." This mean that all accounts capable of directly issue certificate shall use a strong authentication (means 2 factors authentication) to connect to the PKI system.	Verified?	Verified
Network Security	RCA CP section 6.7	Verified?	Verified
Network Security	v Disclosed and Audited subordinate CA Certificates	verified ?	Verified
Link to Publicly			