Print this page

Mozilla - CA Program

Case Information

Case Number	00000028	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	LuxTrust	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	New Owner/Root inclusion requested	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=944783

General information about CA's associated organization

Company Website	https://www.luxtrust.lu	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)	Owned of 2/3 by the Luxembourg government and 1/3 by the major retail banks in Luxembourg.	**Verified?**	Verified
Geographic Focus	Luxembourg LuxTrust S.A. provides PKI services for the whole economic marketplace in Luxembourg, for both private and public organisations. LuxTrust S.A. provides PKI services to the Financial Sector, and therefore is under regulation of the Luxembourg's financial regulator: CSSF (Commission de Surveillance du Secteur Financier).	**Verified?**	Verified
Primary Market / Customer Base	LuxTrust aims to provide its subscribers with certificates for HTTP over SSL, code signing, and communications within banking systems. End-entity certificates are issued to: - Natural persons, in compliance with EU directive 1999/93/EC - Organisations (incl. SSL and code signing).	**Verified?**	Verified
Impact to Mozilla Users	LuxTrust previous Root CA was cross signed by Baltimore CyberTrust Root CA. In order for LuxTrust to provide a National Certification Authority service and in accordance with the Grand Duchy of Luxembourg's strategy, LuxTrust decided to generate and deploy its own trusted Root CA (LuxTrust Global Root CA).	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	Revocation of Compromised Certificates: SSL CPS section 4.9.1.	**Verified?**	Verified

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	* All LuxTrust SSL Certificates under LuxTrust SSL CA are issued for a period of 36 months (3y) maximum. * Wildcard DV SSL certificates are not allowed. * Regarding applicative certificates (SSL and code-signing), only LuxTrust and the Chamber of Commerce of Luxembourg are entitled to authenticate and authorize certificate creation. * In addition, for compliance with ETSI 101 456, all RAs are subject to regular audits. * SSL CPS section 3.2.1 requires PKCS #10. * CPS section 3.2.2: LuxTrust does not issue certificates for private IP addresses or internal domains.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	LuxTrust Global Root	**Root Case No**	R00000032
Request Status	Ready for Public Discussion	**Case Number**	00000028

Additional Root Case Information

Subject	Include LuxTrust Global Root

Technical Information about Root Certificate

O From Issuer Field	LuxTrust s.a.	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This root signs internally-operated subordinate CAs that issue SSL and code signing certificates.	**Verified?**	Verified
Root Certificate Download URL	https://www.luxtrust.lu/downloads/root/LTGRCA_der.cer	**Verified?**	Verified
Valid From	2011 Mar 17	**Verified?**	Verified
Valid To	2021 Mar 17	**Verified?**	Verified

Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://www.trustme.lu/	**Verified?**	Verified
CRL URL(s)	http://crl.luxtrust.lu http://crl.luxtrust.lu/LTSSLCA4.crl http://crl.luxtrust.lu/LTGRCA.crl SSL CPS section 4.9.7: A CRL is issued each 4 hours, at an agreed time.	**Verified?**	Verified
OCSP URL(s)	http://ssl.ocsp.luxtrust.lu http://ltgroot.ocsp.luxtrust.lu	**Verified?**	Verified
Trust Bits	Code; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.171.1.1.10.5.2	**Verified?**	Verified
EV Tested	// CN=LuxTrust Global Root,O=LuxTrust s.a.,C=LU "1.3.171.1.1.10.5.2", "LuxTrust EV OID", SEC_OID_UNKNOWN, { 0xA1, 0xB2, 0xDB, 0xEB, 0x64, 0xE7, 0x06, 0xC6, 0x16, 0x9E, 0x3C, 0x41, 0x18, 0xB2, 0x3B, 0xAA, 0x09, 0x01, 0x8A, 0x84, 0x27, 0x66, 0x6D, 0x8B, 0xF0, 0xE2, 0x88, 0x91, 0xEC, 0x05, 0x19, 0x50 }, "MEQxCzAJBgNVBAYTAkxVMRYwFAYDVQQKEw1MdXhUcnVzdCBzLmEuMR0wGwYDVQQD" "ExRMdXhUcnVzdCBHbG9iYWwgUm9vdA==", "C7g=", Success!	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	C9:3C:34:EA:90:D9:13:0C:0F:03:00:4B:98:BD:8B:35:70:91:56:11	**Verified?**	Verified
SHA-256 Fingerprint	A1:B2:DB:EB:64:E7:06:C6:16:9E:3C:41:18:B2:3B:AA:09:01:8A:84:27:66:6D:8B:F0:E2:88:91:EC:05:19:50	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	See section 1.3.1.1 of the LuxTrust Global Root CA CPS for a diagram of the planned CA hierarchy. LuxTrust Global Root CA signs internally-operated intermediate certificates which sign end-entity certificates. The current subCAs are: - LuxTrust Global Qualified CA - LuxTrust SSL CA - LuxTrust TSA CA	**Verified?**	Verified

	Comment #34: We confirm that the only RAs issuing SSL, EV SSL and code signing certificates are “LuxTrust S.A.” and “Chambre de Commerce“. The SSL CA CPS mentions, respectively in its sections 3.2.2 and 1.3.2, that: - “RAs operating under the LuxTrust SSL CA shall perform a verification of any organizational identities that are submitted by an Applicant or Subscriber.” - “The list of the authorised RAs governed by this CPS is published on LuxTrust’s website https://www.luxtrust.lu.” In addition, LuxTrust’s web site https://www.luxtrust.lu/en/simple/206 mentions that the RAs issuing SSL, EV SSL and code signing certificates are “LuxTrust S.A.” and “Chambre de Commerce.”		
Externally Operated SubCAs	LuxTrust does not issue CAs that are externally operated.	**Verified?**	Verified
Cross Signing	LuxTrust Global Root CA does not cross sign any CA.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Regarding applicative certificates (SSL and code-signing), only LuxTrust and the Chamber of Commerce of Luxembourg are entitled to authenticate and authorize certificate creation. In addition, for compliance with ETSI 101 456, all RAs are subject to regular audits. Comment #34: We confirm that LuxTrust and the RA issuing SSL, EV SSL and code signing certificates under LuxTrust SSL CA are yearly audited against ETSI TS 102 042 with OVCP and PTC-BR. The SSL CA CPS mentions, respectively in its sections 8 and 9.6.1: - "With regards to the provision of LuxTrust Certificates, LuxTrust S.A. through its LuxTrust SSL CA operates: - According to the ETSI technical standard TS 102 042, [3]." - "LuxTrust S.A., through its LuxTrust SSL CA issues Certificates compliant with ETSI TS 102 042 Certificates requirements."	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in French and English.	**Verified?**	Verified
CA Document Repository	https://repository.luxtrust.lu	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.luxtrust.lu/upload/data/repository/LuxTrust%20Global%20Root%20CA%20-%20Certificate%20Profiles%20v1.20.pdf	**Verified?**	Verified
CP Doc Language	English		

CPS	https://www.luxtrust.lu/upload/data/repository /LuxTrust_Global_Root%20CA_Certification_Practice_Statements_v1_08.pdf	**Verified?**	Verified
Other Relevant Documents	* Qualified Certs CPS: https://www.luxtrust.lu/upload/data/repository /LuxTrust_Global_Qualified_CA_Certification_Practice_Statements_v1_06.pdf * SSL CPS: https://www.luxtrust.lu/upload/data/repository /LuxTrust%20SSL%20CA%20CPS%20v1.2.pdf	**Verified?**	Verified
Auditor Name	LSTI	**Verified?**	Verified
Auditor Website	http://www.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/fichiers/11085.pdf	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	7/23/2014	**Verified?**	Verified
BR Audit	http://www.lsti-certification.fr/images/fichiers/11085.pdf With note: https://bugzilla.mozilla.org/show_bug.cgi?id=944783#c31	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	7/23/2014	**Verified?**	Verified
EV Audit	http://www.lsti-certification.fr/images/fichiers/11085.pdf	**Verified?**	Verified
EV Audit Type	ETSI TS 102 042	**Verified?**	Verified
EV Audit Statement Date	7/23/2014	**Verified?**	Verified
BR Commitment to Comply	SSL CPS section 1.1.4	**Verified?**	Verified
SSL Verification Procedures	SSL CPS section 3.2.2: In the particular case of SSL, RAs operating under the LuxTrust SSL CA shall determine whether the domain referenced in the SSL Certificate application is owned and controlled by the subscriber. LuxTrust validates that the Subscriber has the right to control the domain names using the following verification procedures: [1] Communicating with the technical contact information provided by the Subscriber in the order form. [2] Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record’s “registrant”, “technical”, or “administrative” field; [3] Relying upon a Domain Authorization Document which contains the signature of an authorized representative of the domain holder, a date that is on or after the certificate request and a statement confirming the Subscriber’s control over the domain names in the certificate. LuxTrust also relies on a reliable third-party, the Chamber of Commerce of Luxembourg, to confirm the authenticity of the Domain Authorization Document.	**Verified?**	Verified
EV SSL Verification Procedures	SSL CPS section 3.2.2: In the particular case of EV SSL Certificates, RAs operating under the LuxTrust SSL CA shall determine whether the organizational identity, legal existence, physical existence, operational existence, and domain name provided with a LuxTrust EV SSL Certificate Application are consistent with the requirements set forth in the EV Guidelines [10] published by the CA/Browser Forum. The information and sources used for the verification of LuxTrust EV SSL Certificate Applications may vary depending on the jurisdiction of the Applicant or Subscriber. In addition, for EV SSL Certificates, for organisations registered for less than 3 years, a document from a regulated financial institution proving the existence of a current account is also required for the identification of the organisation.	**Verified?**	Verified
Organization Verification Procedures	SSL CPS sections 3.2.2, 3.2.3, and 4.1.2	**Verified?**	Verified

Email Address Verification Procedures	The Email (S/MIME) trust bit is not requested.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	SSL CPS sections 3.2.2, 3.2.3, and 4.1.2.3.2. SSL CPS section 3.2.2: In the particular case of Object signing Certificates, RAs operating under the LuxTrust SSL CA shall verify the subscriber’s identity and authority, and the organization’s identity and existence.	**Verified?**	Verified
Multi-Factor Authentication	LuxTrust Global Root CA CPS section 6.2.1.2. The Registration Authority Operators access the interface of the registration tool to validate the order forms for certificate issuance. The RA authenticates to the registration tool with their LuxTrust certificate, stored on their smart cards and protected by their PIN code.	**Verified?**	Verified
Network Security	LuxTrust Global Root CA CPS section 6. The network security controls are assessed on a regularly basis during the ETSI audits (yearly basis), the EDP CWA 14167-1 full audits (every four years) and other dedicated assessments. The PKI infrastructure is monitored 24/7, logs are centralized. Software tools used for monitoring and centralizing are up-to-date with the latest stable version. Networks and systems would be disconnected directly if intrusions are detected.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.luxtrust.lu/downloads/root/LTSSLCA_der.cer	**Verified?**	Verified