Bugzilla ID: 944783
Bugzilla Summary: Add LuxTrust Global Root CA Certificate

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 CA's associated organization

CA Company Name	LuxTrust S.A.
Website URL	https://www.luxtrust.lu
Organizational type	Government -- LuxTrust S.A. was established in November 2005 and is a state controlled entity, owned of two third by the Luxembourg government and one third by the major retail banks in Luxembourg. LuxTrust S.A. provides Public Key Infrastructure (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).
Primark Market / Customer Base	The CA issues certificates for multiple purposes; end-entity certificates are issued to: - Natural persons, in compliance with EU directive 1999/93/EC - Organisations applicative certificates (incl. SSL and code signing). The Goal of LuxTrust PKI is to provide to each end-user, in Luxembourg but also outside its national borders, one single shared platform to secure both Government and Private e-applications. Security services supported and provided by the LuxTrust PKI will primarily cover the following services for all applications: Strong Authentication, Electronic Signatures, Encryption facilities, Trusted Time Stamping. In practice LuxTrust provides certificates stored on dedicated devices for authentication and signature purposes, as well as SSL certificates for website security and Trusted timestamping. See https://www.luxtrust.lu/en/product_page/61, https://www.luxtrust.lu/en/product_page/205, https://www.luxtrust.lu/en/simple/226
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). LuxTrust aims to provide its subscribers with applicative certificates for general purposes such as HTTP over SSL, code signing, or communications within banking systems. For instance, LuxTrust certificates are used by corporations for provided audit and financial reports to the CSSF.
Inclusion in other major browsers	The LuxTrust Global Root CA is included in Microsoft's browser since October 2011. In inclusion process with Apple.
CA Primary Point of Contact (POC)	Primary Points of Contact (POC): M. Yves Nullens <yves.nullens@luxtrust.lu>, M. Thomas Kopp <thomas.kopp@luxtrust.lu> Email Alias: ca@luxtrust.lu CA Phone Number: +352 26 68 15-1 Title / Department: Security and audit department

Technical information about each root certificate

Certificate Name	LuxTrust Global Root
Certificate Issuer Field	CN = LuxTrust Global Root O = LuxTrust s.a. C = LU
Certificate Summary	LuxTrust Global Root is a self-signed root created for cross signing additional LuxTrust CAs. LuxTrust may cross sign additional CAs only when they are contained within the LuxTrust infrastructure and premises. This root CA will only issue intermediate CAs that will have issuance of aforementioned services as a purpose.
Root Cert URL	https://www.luxtrust.lu/downloads/root/LTGRCA_der.cer
SHA1 Fingerprint	C9:3C:34:EA:90:D9:13:0C:0F:03:00:4B:98:BD:8B:35:70:91:56:11
Valid From	2011-03-17
Valid To	2021-03-17
Certificate Version	3
Cert Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	2048
Test Website URL	https://www.trustme.lu/
CRL URL	CRLs are published at regular intervals on http://crl.luxtrust.lu - Global Root CA CRL: http://crl.luxtrust.lu/LTGRCA.crl (nextUpdate: 3 months) - Global Qualified CA CRL : http://crl.luxtrust.lu/LTGQCA.crl (nextUpdate: 4.5 hours) - SSL CA CRL : http://crl.luxtrust.lu/LTSSLCA.crl (nextUpdate 4.5 hours) SSL CPS section 4.9.7: A CRL is issued each 4 hours, at an agreed time.
OCSP URL	http://ocsp.luxtrust.lu
Requested Trust Bits	Websites (SSL/TLS) Code Signing
SSL Validation Type	OV. LuxTrust plans to implement EV SSL Validation and to be certified by Q1 2014.
EV Policy OID(s)	1.3.171.1.1.10.5.2 https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version EV Test (http://cert-checker.allizom.org/) failed: end-entity cert issued directly by the root.
Non-sequential serial numbers and entropy in cert	Entropy is implemented for LuxTrust SSLCA, Entropy is not implemented for LuxTrust Global Root CA, nor for LuxTrust Global Qualified CA.

CA Hierarchy information for each root certificate

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

Externally Operated SubCAs	LuxTrust does not issue CAs that are externally operated.
Cross-Signing	LuxTrust Global Root CA does not cross sign any CA.
Technical Constraints on Third-party Issuers	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. There is no third party having such rights.

Verification Policies and Practices

Policy Documentation	Documents are all available in English Document Repository: https://repository.luxtrust.lu LuxTrust SSL CA CPS covers both SSL and Code Signing certificates, which are issued under the LuxTrust SSL CA.
Audits	Audit Type: ETSI TS 102 042 V2.4.1, NCP, OVCP, EVCP Auditor: LSTI Auditor Website: http://www.lsti-certification.fr/ Audit Statement: http://www.lsti-certification.fr/images/fichiers/11085.pdf (July 23, 2014)
Baseline Requirements	The LSTI audit statement does not indicate PTC-BR. Comment #21: We recently created a new wiki page: https://wiki.mozilla.org/CA:BaselineRequirements Please review it with your auditor, and update this bug when that has happened. Comment #22: Thank you for this update. We have launched the review and we will come back with an answer shortly. **ALSO**: SSL CPS says: "For the particular case of EV Certificates, this document conforms to the current version of the following CA/Browser Forum documents published at http://www.cabforum.org: - Guidelines for the Issuance and Management of Extended Validation Certificates ("EV Guidelines [10]") - Guidelines Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") What about non-EV SSL certificates? They also have to comply with the BRs.
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.
Organization Verification Procedures	SSL CPS sections 3.2.2, 3.2.3, and 4.1.2
Email Address Verification Procedures	The Email (S/MIME) trust bit is not requested.
Code Signing Subscriber Verification Procedures	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.
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.
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.
Response to Mozilla's CA Communications	Response to May 2014 CA Communication: https://bugzilla.mozilla.org/show_bug.cgi?id=944783#c15

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See above.
CA Hierarchy	See above.
Audit Criteria	See above.
Document Handling of IDNs in CP/CPS	Not applicable.
Revocation of Compromised Certificates	SSL CPS section 4.9.1.
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	Not applicable, not requesting the email trust bit.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	Confirmed
Domain owned by a Natural Person	Not applicable
OCSP	See above.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	All LuxTrust SSL Certificates under LuxTrust SSL CA are issued for a period of 36 months (3y) maximum.
Wildcard DV SSL certificates	Wildcard DV SSL certificates are not allowed.
Email Address Prefixes for DV Certs	See above.
Delegation of Domain / Email validation to third parties	There is no third party having such rights. 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.
Issuing end entity certificates directly from roots	No. See above.
Allowing external entities to operate subordinate CAs	No. See above.
Distributing generated private keys in PKCS#12 files	No. SSL CPS section 3.2.1 requires PKCS #10.
Certificates referencing hostnames or private IP addresses	LuxTrust does not issue certificates for private IP addresses. CPS section 3.2.2: LuxTrust does not issue certificates for private IP addresses or internal domains.
Issuing SSL Certificates for Internal Domains	LuxTrust does not issue certificates for internal domains. CPS section 3.2.2: LuxTrust does not issue certificates for private IP addresses or internal domains.
OCSP Responses signed by a certificate under a different root	no
CRL with critical CIDP Extension	
Generic names for CAs	No. See above.
Lack of Communication With End Users	
Backdating the notBefore date	