**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:<br>- Natural persons, in compliance with EU directive 1999/93/EC<br>- Organisations applicative certificates (incl. SSL and code signing).<br>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.<br>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.<br>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.<br>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).<br>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><br>Email Alias: ca@luxtrust.lu<br>CA Phone Number: +352 26 68 15-1<br>Title / Department: Security and audit department |

**Technical information about each root certificate**

| | |
|---|---|
| Certificate Name | LuxTrust Global Root |
| Certificate Issuer Field | CN = LuxTrust Global Root<br>O = LuxTrust s.a.<br>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<br>- Global Root CA CRL: http://crl.luxtrust.lu/LTGRCA.crl (nextUpdate: 3 months)<br>- Global Qualified CA CRL : http://crl.luxtrust.lu/LTGQCA.crl (nextUpdate: 4.5 hours)<br>- SSL CA CRL : http://crl.luxtrust.lu/LTSSLCA.crl (nextUpdate 4.5 hours)<br>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)<br>Code Signing |
| SSL Validation Type | OV. LuxTrust plans to implement EV SSL Validation and to be certified by Q1 2014. |
| EV Policy OID(s) | Not requesting EV treatment at this time. |
| Non-sequential serial numbers and entropy in cert | Entropy is implemented for LuxTrust SSLCA,<br>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.<br>LuxTrust Global Root CA signs internally-operated intermediate certificates which sign end-entity certificates. The current subCAs are:<br>- LuxTrust Global Qualified CA<br>- LuxTrust SSL CA<br>- 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.<br>In addition, for compliance with ETSI 101 456, all RAs are subject to regular audits.<br>There is no third party having such rights. |

**Verification Policies and Practices**

| | |
|---|---|
| Policy Documentation | Documents are all available in English<br>Document Repository: https://repository.luxtrust.lu<br>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<br>Auditor: Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services (ILNAS).<br>Auditor Website: http://www.ilnas.public.lu/fr/confiance-numerique/pki/en/digital-trust/index.html<br>Audit Statement: http://www.ilnas.public.lu/fr/confiance-numerique/pki/psc-accredites/luxtrust/index.html<br>The last ETSI audit is dated November 16, 2012.<br>The Luxembourg law regarding CSP, which required a yearly audit, is currently under revision and will be updated according to the EU Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market.<br>Therefore, the next ETSI audit is planned for March 2014.<br>We can proceed with the process, but approval will be dependent on a current audit – annual audits are required. |
| Baseline Requirements | The verification of compliance with the CA/Browser Forum Baseline will be included in the ETSI audit planned in March 2014.<br>We can proceed with the process, but approval will be dependent on the BR audit. |
| 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.<br>LuxTrust validates that the Subscriber has the right to control the domain names using the following verification procedures:<br>[1] Communicating with the technical contact information provided by the Subscriber in the order form.<br>[2] Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;<br>[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.<br>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.<br>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.<br>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.<br>The PKI infrastructure is monitored 24/7, logs are centralized.<br>Software tools used for monitoring and centralizing are up-to-date with the latest stable version.<br>Networks and systems would be disconnected directly if intrusions are detected. |

**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.<br>Regarding applicative certificates (SSL and code-signing), only LuxTrust and the Chamber of Commerce of Luxembourg are entitled to authenticate and authorize certificate creation.<br>In addition, for compliance with ETSI 101 456, all RAs are subject to regular audits. |
| Issuing end entity certificates directly from | No. See above. |

| | |
|---|---|
| roots | |
| 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.<br>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.<br>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 | |
| CRL with critical CIDP Extension | |
| Generic names for CAs | No. See above. |
| Lack of Communication With End Users | |
| Backdating the notBefore date | |