CA Information checklist

Version number: Final

Publication Date: 29/11/2013

Table of content

LuxTrust – CA Information Checklist

Important note: Unless specified otherwise, the acronym CPS refers to "all" CPS issued by LuxTrust, publically available under https://repository.luxtrust.lu

1.1 General information about the associated organization of the CA

CA Company Name	LuxTrust S.A.
Website URL	https://www.luxtrust.lu
Organizational type	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).
Primary market / customer base	Which types of customers does the CA serve? 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). Are there particular vertical market segments in which it operates? Does the CA focus its activities on a particular country or other geographic region? 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

1.1 General information about the associated organization of the CA

	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	**Why does the CA need to have their root certificate directly included in Mozilla's products, rather than being signed by another CA's root certificate that is already included in NSS?** 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). **Describe the types of Mozilla users who are likely to encounter your root certificate as relying parties while web browsing (HTTPS servers doing SSL), sending/receiving email to their own MTA (SMTPS, IMAPS servers doing SSL), sending/receiving S/MIME email (S/MIME email certs), etc.** 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. A complete description can be found in LuxTrust SSL CA CPS.
Inclusion in other major browsers	**Does this CA have root certificates included in any other major browsers? If yes, which? If no, why not?** • The LuxTrust Global Root CA is included in Microsoft's browser. • The CA inclusion process will be undertaken with Apple in December 2013. • No inclusion process has been undertaken with Opera, as Opera uses the root store provided by the operating systems since version 14, and after fall 2013, older versions of Opera will use Network Security Services (NSS) by Mozilla. • No inclusion process has been undertaken with Google, as Google Chrome uses the root certificate store of the underlying operating system. For Linux, Google Chrome uses NSS by Mozilla.
CA Primary Point of Contact (POC)	**POC direct email :** LuxTrust S.A. has two Primary Points of Contact (POC) : M. Yves Nullens / email : yves.nullens@luxtrust.lu

1.1 General information about the associated organization of the CA

	M. Thomas Kopp / email : thomas.kopp@luxtrust.lu **Email Alias: An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization.** A dedicated email for such communication is available: ca@luxtrust.lu **CA Phone Number: A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA.** +352 26 68 15-1 **Title / Department: If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?** Security and audit department

1.2 Technical information about LuxTrust Global Root CA

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
Certificate Signature Algorithm	SHA256WithRsa
Signing key parameters	RSA2048 bits
Test Website URL (SSL)	**Test website for integration purposes:**

Example Certificate (non-SSL)	– https://www.trustme.lu/
CRL URL	**CRL URLs:** – Global Root CA CRL: http://crl.luxtrust.lu/LTGRCA.crl – Global Qualified CA CRL : http://crl.luxtrust.lu/LTGQCA.crl – SSL CA CRL : http://crl.luxtrust.lu/LTSSLCA.crl **nextUpdate value:** - Global Root CA CRL: 3 months - Global Qualified CA CRL 4h30 - SSL CA CRL : 4h30 **CP reference** - Reference in the CP LuxTrust Global Root CA - Certificate Profiles, in the section 3.4 *CRL profiles*

OCSP URL (Required now)	**OCSP URI in the AIA of end-entity certificates.**
	The OCSP responder appears in the AIA of our certificates, please refer to the sample available on http://www.trustme.lu
	The OCSP URI is http://ocsp.luxtrust.lu
	
	Maximum expiration time of OCSP responses
	The maximum expiration time of an OCSP response is 4h30 after the creation of the response.
	
	Testing results
	
	a) Browsing to test website with OCSP enforced in Firefox browser
	
	The OCSP responder is compatible with FireFox and is available on ocsp.luxtrust.lu, port 80. A sample test can be performed using:
	`@echo off`
	`echo.`
	`echo Checking REVOKED certificates`
	`openssl ocsp -issuer LTGQCA.cer -serial 500143 -host ocsp.luxtrust.lu:80 -CAfile LTGRCA_CHAIN.pem`
	`openssl ocsp -issuer LTGQCA.cer -serial 500343 -host ocsp.luxtrust.lu:80 -CAfile LTGRCA_CHAIN.pem`
	`echo.`
	`echo Checking GOOD certificates`
	`openssl ocsp -issuer LTGQCA.cer -serial 500333 -host ocsp.luxtrust.lu:80 -CAfile LTGRCA_CHAIN.pem`
	`openssl ocsp -issuer LTGQCA.cer -serial 500334 -host ocsp.luxtrust.lu:80 -CAfile LTGRCA_CHAIN.pem`
	`echo.`
	`echo Checking UNKNOWN certificates`
	`openssl ocsp -issuer VeriSignClass3ExtendedValidationSSLCA.crt -cert www.paypal.com.pem -host ocsp.luxtrust.lu:80 -no_cert_verify`

	b) If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Not applicable
Requested Trust Bits	State which of the three trust bits you are requesting to be enabled for this root. One or more of: Trust bits requested by LuxTrust are: • Websites (SSL/TLS) • Code Signing
SSL Validation Type	Indicate the levels of SSL validation that are used for certificates within this root's hierarchy. One or more of: LuxTrust currently complies with OV SSL Validation. LuxTrust plans to implement EV SSL Validation and to be certified by Q1 2014.
EV Policy OID(s)	Not applicable
Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html 9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: … - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)." Entropy is implemented for LuxTrust SSLCA, but neither for LuxTrust Global Root CA, nor for LuxTrust Global Qualified CA.

1.3 CA Hierarchy information for each root certificate

CA Hierarchy	List, description, and/or diagram of all intermediate CAs signed by this root. The subordinate CAs signed by LuxTrust Global Root CA are: • LuxTrust Global Qualified CA • LuxTrust SSL CA • LuxTrust TSA CA In the document LuxTrust Global Root CA - Certificate Profiles, chapter 2, section 2.1 *Two-level CA hierarchy*, the diagram presents a target of all SubCAs which are foreseen. Identify which of the subordinate CAs are internally-operated and which are externally operated All these SubCAs are internally operated.

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	**For each external third party (CAs and RAs) that issues certificates or can directly cause the issuance of certificates within the hierarchy of the root certificate(s) that you wish to include in Mozilla products, either:** • **Implement technical controls to restrict issuance to a specific set of domain names which you have confirmed that the third party has registered or has been authorized to act for (e.g. RFC5280 x509 dNSName name constraints, marked critical)** Regarding applicative certificates (SSL and code-signing), only LuxTrust and the Chamber of Commerce of Luxembourg are entitled to authenticate and authorise certificate creation. In addition, for compliance with ETSI 101 456, all RAs are subject to regular audits. • **Provide the name and url of the unconstrained third party along with links to their corresponding Certificate Policy and/or Certification Practice Statement and provide attestation of their conformance to the stated verification requirements and other operational criteria by a competent independent party or parties with access to details of the subordinate CA's internal operations.** There is no third party having such rights.

1.4 Verification Policies and Practices

Policy Documentation	**The publicly accessible URLs to the document repository and the published document(s) describing how certificates are issued within the hierarchy rooted at this root, as well as other practices associated with the root CA and other CAs in the hierarchy, including in particular the Certification Practice Statement(s) (CPS) and related documents.**
	CP/CPS and all related documentation such as relying party agreements are publically available on:
	https://repository.luxtrust.lu
	
	Language(s) that the documents are in:
	• CP: English
	• CPS: English
	• Relying Party Agreements:
	  ○ General terms and conditions: English, French and German
	  ○ Dispute Resolution Procedure: English

Audits	**Audit type:** The audit types that are regularly performed at LuxTrust can be summarized as follows: - Yearly audits against ETSI TS 101 456 and ETSI TS 102 042 standards for accreditation purposes. LuxTrust was accredited against ETSI TS 101 456 and ETSI TS

102 042 from October, 13th, 2011 to October, 13th 2013. Since October, 13th 2013, they are in a supervised mode until the next ETSI certification audit planned in March 2014.

- Audits against CWA 14167-1 standard for accreditation purposes (every four years), as a pre-requisite to the ETSI audits. This year, a full audit against this standard was performed.
- Mandatory yearly internal audits as required by the Luxembourg's financial regulator for support PFS (Professionals of Financial Sector) (art. 29-1 and 29-2 of the Luxembourg's financial law)
- Data privacy audits according to the Data Privacy National Committee (on an ad-hoc basis)

The audit should not be more than a year old. If it is, then provide an estimate of when the updated audit report will be available. While ETSI Certificates may be valid for 3 years, it is our expectation that there is an annual renewal/review process for the ETSI Certificate to remain valid.

- The last ETSI audit is dated November, 16th, 2012.

  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. Therefore, the next ETSI audit is planned for March 2014.
- A full EDP audit based on CWA 14167-1 was performed this year and finished in November, 2013.

- **Renewed root certificates also need to be included in audits. If the root certificate was created after the most recent audit, then provide an estimate of when the new audit report (that includes the operations of the new root) will be available.**

  The audits relates to the processes and the operations of the PKI infrastructure as a whole. At LuxTrust, all CAs are subject to the same level of security, regardless of the type of CA.

Auditor:

- ETSI audits are performed by the Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services (ILNAS).
- CWA audits are performed by Deloitte.
- As a regulated PFS, the internal audit is under the CSSF supervision, given that it is a mandatory role defined by this National Regulatory Entity.

Auditor Website:

http://www.ilnas.public.lu/

http://www.cssf.lu/en/

URL to Audit Report and Management's Assertions :

Accreditation information from ILNAS can be found under: http://www.ilnas.public.lu/fr/confiance-numerique/pki/en/digital-trust/index.html

The LuxTrust Accreditation Certificate can be found under: http://www.ilnas.public.lu/fr/confiance-numerique/pki/psc-accredites/luxtrust/certificat.pdf

The technical annexes for the certification can be found under: http://www.ilnas.public.lu/fr/confiance-numerique/pki/psc-accredites/luxtrust/annexe-technique-v-

	04.pdf ILNAS reference for accredited certification authorities in Luxembourg: http://www.ilnas.public.lu/fr/confiance-numerique/pki/psc-accredites/index.html LuxTrust page on ILNAS web server: http://www.ilnas.public.lu/fr/confiance-numerique/pki/psc-accredites/luxtrust/index.html
Baseline Requirements (SSL)	**The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3. Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy and the audit statement shall indicate the results.** The verification of compliance with the CA/Browser Forum Baseline will be included in the ETSI audit planned in March 2014.
SSL Verification Procedures	• **URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber.** The LT SSL CA CPS mentions in the section 3.2 *Initial Identity Validation* that in the case of SSL Certificates, 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. • **If a challenge-response mechanism via email is used to confirm the ownership/control of the domain name, then provide the list of email addresses that are used for verification.** Due to internal verifications that are performed, as well as to the documentation that is required, we do not authenticate the request based on a challenge -response mechanism. • **Confirm that you have automatic blocks in place for high-profile domain names (including those targeted in the DigiNotar and Comodo attacks in 2011).** ○ **Specify the procedure for additional verification of a certificate request that is blocked.** LuxTrust has no automatic certificate generation. Every domain is analysed using dedicated processes to guarantee ownership of the domain before issuing a certificate. All certificates issued are currently manually validated against ALEXA top 100. An automatic post-processing will be implemented in Q1 2014 and will verify that all issued certificates correspond to requests validated by a LuxTrust RA. • **If OV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the identity, existence, and authority of the organization to request the certificate.** ○ **There should be a description of the types of resources that are used to confirm the authenticity of the information provided by the certificate subscriber, what**

	data is retrieved from public resources, and how that data is used for verification of the entity referenced in the certificate. OV is applied; The LT SSL CA CPS mentions in the section 3.2 *Initial Identity Validation* the documents required and the verification procedures for a Certificate application. • **If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate.** ○ **The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.** Not applicable.
Email Address Verification Procedures	The Email (S/MIME) trust bit is not requested.
Code Signing Subscriber Verification Procedures	**If you are requesting to enable the Code Signing trust bit...** • **URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the certificate subscriber's identity and authority, and the organization's identity and existence.** • **Recommended Practices for Verifying Identity of Code Signing Certificate Subscriber** The LT SSL CA CPS mentions in the section 3.2 *Initial Identity Validation* that in the 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	**Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance.** 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	**Confirm that you have done the following, and will do the following on a regular basis:** • **Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements.** 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. • **Check for mis-issuance of certificates, especially high-profile domains.** LuxTrust has no automatic certificate generation. Every domain is analysed using dedicated processes to guarantee ownership of the domain before issuing a certificate. All certificates issued are manually validated against ALEXA top 100. An automatic post-processing will be implemented in Q1 2014 and will verify that all issued certificates correspond to requests validated by a LuxTrust RA. • **Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.** Confirmed: The PKI infrastructure is monitored 24/7, logs are centralized. • **Ensure Intrusion Detection System and other monitoring software is up-to-date.** Confirmed: Software tools used for monitoring and centralizing are up-to-date with the latest stable version. • **Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion.** Confirmed: Networks and systems would be disconnected directly if intrusions are detected.
Additional Notes	Since October 2011, Microsoft distributes the LuxTrust Global Root CA Official page: https://social.technet.microsoft.com/wiki/contents/articles/5225.aspx Certificate: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/C93C34EA90D9130C0F03004B98BD8B3570915611.crt

1.5 CA recommended practices

Publicly Available CP and CPS	CP/CPS and all related documentation such as terms and conditions and relying party agreements are publically available in PDF file format in English language on: https://repository.luxtrust.lu
CA Hierarchy	Confirmed as described above
Audit criteria	Confirmed as described above

Document Handling of IDN in CP/CPS	Not applicable
Revocation of Compromised Certificates	Confirmed
Verifying Domain Name Ownership	Confirmed
Verifying Email Address Control	Confirmed
Verifying Identity of Code Signing Certificate Subscriber	Confirmed
DNS names go in SAN	Confirmed
Domain owned by a Natural Person	Not applicable
OCSP	Confirmed