Print this page

Mozilla - CA Program

Case Information

Case Number	00000054	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	LAWtrust	**Request Status**	Need Information from CA

Additional Case Information

Subject	LAWtrust Root Inclusion Request	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1023726

General information about CA's associated organization

Company Website	https://www.lawtrust.co.za	**Verified?**	Verified
Organizational Type		**Verified?**	Need Response From CA
Organizational Type (Others)	What type of organization is LAWtrust? e.g. a Private Corporation, Public Corporation, Government Agency?	**Verified?**	Need Response From CA
Primary Market / Customer Base	South Africa LAWtrust already provides end user certificates to the business banking customers of 3 of the four major banks in the country as well as the South African government employees. LAWtrust issues certificates to the general public and businesses.	**Verified?**	Verified
Impact to Mozilla Users	LAWtrust is the largest security integrator in South Africa with 13 years' experience in running a local trust centre and complying with the audit requirements and chaining requirements from VeriSign and Entrust. LAWtrust is implementing in-house and managed CA's for higher assurance and audited client certificates for digital signature and non-repudiation.	**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	LAWtrust has a Certificate Policy (internal document) and CPS's for the various CA's published in their repository accessible to relying parties and certificate users. LAWtrust revokes all compromised certificates as set out in their CPS's and RA Charters. I don't understand this statement: "LAWtrust is verifying end user applicant's email addresses before the issuance of a certificate as per the CPS's and RA Charters." WHO verifies end-user certificate requests? OCSP URI not in the AIA of the certificates.	**Verified?**	Need Clarification From CA

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	I don't understand what this means: "LAWtrust do not external entities to operate their own CAs as subordinate CAs under the LAWtrust Root Certification Authority 2048." My impression based on reading the CPS is that LAWtrust only issues intermediate certs to third parties, and it is the third parties who issue end-entity certs. LAWtrust do not issue SSL certificates. When end users request SMIME certificates via the Entrust Entillegence Security Provider (ESP) software, the LAWtrust CA receives via secure channel and P12 a copy of the decryption private key for backup purposes. These keys are securely stored in the CA database and are recovered under the control of the end user. All other end user certificate key pairs are generated at the end user and are solely under the control of the certificate user.	**Verified?**	Need Clarification From CA

Root Case Record # 1

Root Case Information

Root Case No	R00000071	**Case Number**	00000054
Request Status	Need Information from CA	**Root Certificate Name**	LAWtrust Root Certification Authority 2048

Additional Root Case Information

Subject	Include LAWtrust Root Certification Authority 2048 certificate

Technical Information about Root Certificate

O From Issuer Field	O = LAWtrust	**Verified?**	Verified

OU From Issuer Field	LAW Trusted Third Party Services PTY Ltd.	**Verified?**	Verified
Certificate Summary	According to the CPS, it appears that LAWtrust does not issue end-entity certs. Rather, LAWtrust issues intermediate certs to external third-parties who then issue end-entity certs. Please clarify CA hierarchy information below.	**Verified?**	Need Clarification From CA
Root Certificate Download URL	https://www.lawtrust.co.za/documents/LAWTRUST-ROOT-CA-CERTIFICATE.cer	**Verified?**	Verified
Valid From	2012 May 16	**Verified?**	Verified
Valid To	2032 May 16	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-1	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	Not requesting Websites trust bit, so do not need a test website. Please provide an example cert.	**Verified?**	Need Clarification From CA
CRL URL(s)	http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crlfile.crl http://aesigncrl.lawtrust.co.za/CRL/lawtrust_aesign_ca_crlfile.crl	**Verified?**	Verified
OCSP URL(s)	Not requesting Websites trust bit. So OK. No OCSP URI in the AIA of the intermediate cert. No OCSP URI in the AIA of the end-entity cert.	**Verified?**	Verified
Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
EV Policy OID(s)	Not requesting Websites trust bit.	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None. Only requesting Email trust bit.	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	33:5A:7F:F0:09:27:CF:2D:F2:78:E2:C9:19:2F:7A:4D:55:34:F8:0C	**Verified?**	Verified
SHA-256 Fingerprint	9B:14:E8:F5:F6:EA:16:76:66:E7:6D:CD:6B:EC:C1:90:86:1D:5E:89:70:B9:9A:94:70:F0:23:12:36:04:97:04	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root currently has two intermediate	**Verified?**	Need Clarification From CA

	certificates: 1) LAWtrust Certification Authority 2048 2) LAWtrust AeSign Certification Authority 2048 QUESTION: Are these owned and operated by LAWtrust? Or does a third-party own and operate these subordinate CAs?		
Externally Operated SubCAs	It appears that the LAWtrust CPS only explains the procedures for verifying and provisioning subordinate CA certificates. So, it appears that LAWtrust provisions subordinate CA certificates that are owned and operated by external third parties.	**Verified?**	Need Clarification From CA
Cross Signing	Has this root been involved in cross-signing with any other root certificates?	**Verified?**	Need Clarification From CA
Technical Constraint on 3rd party Issuer	What contractual and/or technical controls are in place for external subCAs and external RAs? What rules must external subCAs and RAs follow in regards to verifying and issuing end-entity certificates?	**Verified?**	Need Clarification From CA

Verification Policies and Practices

Policy Documentation	Documents are in English	**Verified?**	Verified
CA Document Repository	https://www.lawtrust.co.za/repository/	**Verified?**	Verified
CP Doc Language			
CP	CP Not Published	**Verified?**	Verified
CP Doc Language			
CPS	https://www.lawtrust.co.za/documents/LAWTRUST-ROOT-CPS.pdf	**Verified?**	Verified
Other Relevant Documents	https://www.lawtrust.co.za/documents/LAWTRUST-END-USER-LICENSE-AGREEMENT.pdf https://www.lawtrust.co.za/documents/LAWTRUST-RELYING-PARTY-AGREEMENT.pdf	**Verified?**	Verified
Auditor Name	KPMG	**Verified?**	Verified
Auditor Website	http://www.kpmg.com/ZA/en/Pages/default.aspx	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1664&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	4/29/2014	**Verified?**	Verified
BR Audit		**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable

BR Audit Statement Date		**Verified?**	Not Applicable
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply		**Verified?**	Not Applicable
SSL Verification Procedures	Not requesting the Websites trust bit.	**Verified?**	Not Applicable
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	QUESTION: It appears that the CPS does not state how the identity/authority of the end-entity certificate subscriber must be verified. Where is this documented? What rules must the subCAs follow when verifying and issuing end-entity certificates? CPS section 3: "Before issuing a LAWtrust Subordinate CA Certificate the LAWtrust OA verify the information, purpose and/or attributes of an Applicant to be published in a LAWtrust Subordinate CA Certificate. This section of the CPS establishes the criteria for an acceptable application for a LAWtrust Subordinate CA Certificate. CPS section 4: LAWtrust will perform the certificate lifecycle operations and management for all LAWtrust Subordinate CA's... CPS section 4.2.1: If the verification of the information submitted to the LAWtrust OA is successful, then - The LAWtrust OA shall schedule a key ceremony at the LAWtrust vault in the hosting facilities to establish the Subordinate CA; - Submit, during the key ceremony, a CSR from the Subordinate CA to the LAWtrust Root CA2048; - The LAWtrust Root CA will validate and sign the Subordinate CA CSR and issue the Subordinate CA Certificate; - Provide the Subordinate CA Certificate back to the Applicant for installation. After the issue of the LAWtrust Subordinate CA Certificate the LAWtrust Root CA 2048 will have no further obligation to perform any ongoing monitoring, investigation or verification of the information provided in the certificate application.	**Verified?**	Need Clarification From CA
Email Address Verification Procedures	The LAWtrust CPS only describes verification procedures for the subordinate CA certificates. It does not state verification procedures for end-entity certificates. Please provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist#CA_Policies_about_Third-Party_Subordinate_CAs and please note: https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control The CA's public documentation needs to provide sufficient information describing how the email address is verified to be owned/controlled by the certificate subscriber.	**Verified?**	Need Clarification From CA

Code Signing Subscriber Verification Pro	Not requesting the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	All registration authority administrators (natural persons or systems) require a username, in combination with a digital certificate and password to unlock the private key of the certificate required to access the Entrust Registration Authority components to perform certificate lifecycle processes. QUESTION: How does the Entrust RA components impact this CA Hierarchy?	**Verified?**	Need Clarification From CA
Network Security	CPS section 5. QUESTION: What about the externally-operated subCAs -- what requirements are placed on how they operate their intermediate certs?	**Verified?**	Need Clarification From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	Item #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Verified