BUG 102376 - NOTES BY MOZILLA	RESPONSE BY LAWTRUST (CA)
Organisation Type	LAWtrust is a private company, registered in terms of the laws of South Africa with registration number 2001/004386/07
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?	The relevant Registration Authority (RA) enrolment and verification officer are responsible for doing identity verification including email addresses of end users for SMIME certificates
OCSP URL not in the AIA of the certificates.	Please check the test certificate AIA in the email to Kathleen.
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.	Any subordinate CA chained into the LAWtrust root CA is operated by LAWtrust personnel. LAWtrust never allows a third party customer to setup and manage a subordinate CA chained into the root themselves. All subordinate Cass are established and maintained from the audited LAWtrust trust centre.
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	To clarify, the LAWtrust root CA does not issue end-user certificates for example SMIME or signing certificates. It only issues certificates to subordinate CAs managed by LAWtrust.

below.	
Test website URL (SSL) or example cert - Not requesting Websites trust bit, so do not need a test website. Please provide an example cert.	
This root currently has two intermediate 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?	Yes, these two CAs are owned and managed by LAWtrust.
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.	This is incorrect. LAWtrust owns all subordinate CAs chained into the LAWtrust root CA and never allows third party subordinate CAs.
Has this root been involved in crosssigning with any other root certificates?	No, it has not
1. What contractual and/or technical controls are in place for external subCAs and external RAs? 2. What rules must external subCAs and RAs follow in regards to verifying and issuing end-entity certificates?	1. There are no external CAs. The RA software that allows for certificate management on the subordinate CAs chained into the LAWtrust root, is deployed in the LAWtrust trust centre. The technical controls for RA administrators performing the certificate lifecycle

	functions via the RA software portals are stipulated in the RA charters. 2. The rules are stipulated in the RA charters.
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	Take note: When reviewing the root CA CPS, it must be kept in mind that the root only issued subordinate CA certificates. There will therefore be no mention of end-user certificates other than subordinate CA certificates. The CPS for the subordinate CAs chained into the LAWtrust root CA, will stipulate the rules in question, for example the AESign CPS in the LAWtrust repository.

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.	
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.	Please see the responses above, stating that the LAWtrust root can only issue subordinate CA certificates. As the root CA does not issue end-user certificates but only subordinate CA certificates, the email address is not an attributing factor that needs to be verified.
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?	The Entrust RA component does not impact the CA hierarchy at all. It is merely a software portal that exposes the certificate lifecycle for an subordinate CA to the certificate administrators .
CPS section 5. QUESTION: What about the externally-operated subCAs -- what requirements are placed on how they operate their intermediate certs?	LAWtrust has no externally operated CAs chained into the root CA.