Bugzilla ID: 1025095
Bugzilla Summary: OpenTrust: add new root CA certificates

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	OpenTrust / Keynectis
Website URL	http://www.opentrust.com/en/
Organizational type	Private corporation. The company is known as Keynectis, with a new branding OpenTrust. Also own Certplus brand.
Primark Market / Customer Base	Any type of customer (public or private corporations, associations). Focus is mainly in EMEA even if certificates can be used worldwide. This may be different in the future depending on sales representatives that can be geographically based in other regions. Types of certificates issued: Signature and authentication for users (S/MIME, signature of documents, SSL authentication…), SSL certificates for servers, VPN certificate, OCSP certificate, timestamping certificate, code signing cert… See § 1.4.1.4 of the RCA CP.
Impact to Mozilla Users	Renew already registered root certificate (Certplus Class 2 expiring in 2019) with five different CA certificates for the next 24 years based upon different characteristics: - Two brandings: existing one "Certplus" and the new one "OpenTrust" - Different technologies about keys and algorithms: RSA/ECC, SHA 256 / 512 / ECC
Inclusion in other major browsers	http://social.technet.microsoft.com/wiki/contents/articles/14218.windows-and-windows-phone-8-ssl-root-certificate-program-april-2012-h-t.aspx (Keynectis and CertPlus) In the process of registering the new roots with other major browsers.
CA Primary Point of Contact (POC)	Erwann Abalea – erwann.abalea@opentrust.com - +33 1 55 64 22 07 Remi Pifaut – remi.pifaut@opentrust.com - +33 1 55 64 22 18 CA Email Alias – rcprogram@opentrust.com Switchboard phone number: +33 1 55 64 22 00 Customer service phone number: +33 1 55 64 22 33 Title / Department: ask for the customer service

Technical information about each root certificate – Certplus Brand

Cert Name	Certplus Root CA G1	Certplus Root CA G2
Cert Issuer Field	CN = Certplus Root CA G1 O = Certplus C = FR	CN = Certplus Root CA G2 O = Certplus C = FR

Certificate Summary	This root certificate will replace the already included "Certplus Class 2", with our old brand name, and different crypto parameters (SHA512, RSA4096); certificates to be produced are TLS, Email, Code Signing.	This root certificate will replace the already included "Certplus Class 2", with our old brand name, and different crypto parameters (SHA384, ECC); certificates to be produced are TLS, Email, Code Signing.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=8446784	https://bugzilla.mozilla.org/attachment.cgi?id=8446790
SHA1 Fingerprint	22:FD:D0:B7:FD:A2:4E:0D:AC:49:2C:A0:AC:A6:7B:6A:1F:E3:F7:66	4F:65:8E:1F:E9:06:D8:28:02:E9:54:47:41:C9:54:25:5D:69:CC:1A
Valid From	2014-05-26	2014-05-26
Valid To	2038-01-15	2038-01-15
Certificate Version	3	3
Certificate Signature Algorithm	SHA-512	ecdsa-with-SHA384
Signing key parameters	4096	ECC, NIST P-384
Test Website URL	https://certplusrootcag1-test.opentrust.com Must use a new profile to test, see https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c18	https://certplusrootcag2-test.opentrust.com Must use a new profile to test, see https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c18
CRL URL	http://get-crl.certificat.com/public/certplusrootcag1.crl	http://get-crl.certificat.com/public/certplusrootcag2.crl
OCSP URL	http://get-ocsp.certificat.com/certplusrootcag1 What is the maximum expiration time of OCSP responses?	http://get-ocsp.certificat.com/certplusrootcag2 What is the maximum expiration time of OCSP responses?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV, and EV	DV, OV, and EV
EV Policy OID(s)	1.3.6.1.4.1.22234.2.5.2.3.1 Please do EV testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Note https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c20	1.3.6.1.4.1.22234.2.5.2.3.1 Please do EV testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Note https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c20
Non-sequential serial numbers and entropy in cert	Comment #9: all certificate serial numbers for Subscriber issued by CA shall have a random number on 16 bytes longs.	Comment #9: all certificate serial numbers for Subscriber issued by CA shall have a random number on 16 bytes longs.

Technical information about each root certificate – OpenTrust Brand

Cert Name	OpenTrust Root CA G1	OpenTrust Root CA G2	OpenTrust Root CA G3
Cert Issuer Field	CN = OpenTrust Root CA G1 O = OpenTrust C = FR	CN = OpenTrust Root CA G2 O = OpenTrust C = FR	CN = OpenTrust Root CA G3 O = OpenTrust C = FR
Certificate Summary	This root certificate will replace the already included "Certplus Class 2", with our new company name, and different crypto parameters (SHA256, RSA4096); certificates to be produced are TLS, Email, Code Signing.	This root certificate will replace the already included "Certplus Class 2", with our new company name, and different crypto parameters (SHA512, RSA4096); certificates to be produced are TLS, Email, Code Signing.	This root certificate will replace the already included "Certplus Class 2", with our new company name, and different crypto parameters (SHA384, ECC); certificates to be produced are TLS, Email, Code Signing.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=8446791	https://bugzilla.mozilla.org/attachment.cgi?id=8446792	https://bugzilla.mozilla.org/attachment.cgi?id=8446793
SHA1 Fingerprint	79:91:E8:34:F7:E2:EE:DD:08:95:01:52:E9:55:2D:14:E9:58:D5:7E	79:5F:88:60:C5:AB:7C:3D:92:E6:CB:F4:8D:E1:45:CD:11:EF:60:0B	6E:26:64:F3:56:BF:34:55:BF:D1:93:3F:7C:01:DE:D8:13:DA:8A:A6
Valid From	2014-05-26	2014-05-26	2014-05-26
Valid To	2038-01-15	2038-01-15	2038-01-15
Certificate Version	3	3	3
Certificate Signature Algorithm	SHA-256	SHA-512	ecdsa-with-SHA384
Signing key parameters	4096	4096	ECC, NIST P-384
Test Website URL	https://opentrustrootcag1-test.opentrust.com Must use a new profile to test, see https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c18	https://opentrustrootcag2-test.opentrust.com Must use a new profile to test, see https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c18	https://opentrustrootcag3-test.opentrust.com Must use a new profile to test, see https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c18
CRL URL	http://get-crl.certificat.com/public/opentrustrootcag1.crl	http://get-crl.certificat.com/public/opentrustrootcag2.crl	http://get-crl.certificat.com/public/opentrustrootcag3.crl
OCSP URL	http://get-ocsp.certificat.com/opentrustrootcag1 What is the maximum expiration time of OCSP responses?	http://get-ocsp.certificat.com/opentrustrootcag2 What is the maximum expiration time of OCSP responses?	http://get-ocsp.certificat.com/opentrustrootcag3 What is the maximum expiration time of OCSP responses?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL	DV, OV, and EV	DV, OV, and EV	DV, OV, and EV

Validation Type			
EV Policy OID(s)	1.3.6.1.4.1.22234.2.5.2.3.1 Please do EV testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Note https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c20	1.3.6.1.4.1.22234.2.5.2.3.1 Please do EV testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Note https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c20	1.3.6.1.4.1.22234.2.5.2.3.1 Please do EV testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Note https://bugzilla.mozilla.org/show_bug.cgi?id=1025095#c20
Non-sequential serial numbers and entropy	Comment #9: all certificate serial numbers for Subscriber issued by CA shall have a random number on 16 bytes longs.	Comment #9: all certificate serial numbers for Subscriber issued by CA shall have a random number on 16 bytes longs.	Comment #9: all certificate serial numbers for Subscriber issued by CA shall have a random number on 16 bytes longs.

CA Hierarchy information for each root certificate

CA Hierarchy	CA Hierarchy For each root CA, there have been one or two CAs created during key ceremony dated 26th of May 2014: • One existing EV SSL CA that has been cross certified with this new root CA (for EV SSL issuance). This CA is the one used to issue EV SSL certificates under the Certplus Class 2 already included within major browsers and OS • For some of the root CAs, one CA dedicated to Adobe AATL program (for Adobe compliant PDF signing certificates) OpenTrust Root CA G1 issued: • EV CA: KEYNECTIS Extended Validation CA • AATL CA: OpenTrust CA for AATL G1 OpenTrust Root CA G2 issued: • EV CA: KEYNECTIS Extended Validation CA • AATL CA: OpenTrust CA for AATL G2 OpenTrust Root CA G3 issued: • EV CA: KEYNECTIS Extended Validation CA • AATL CA: OpenTrust CA for AATL G3 Certplus Root CA G1 issued: • EV CA: KEYNECTIS Extended Validation CA Certplus Root CA G2 issued: • EV CA: KEYNECTIS Extended Validation CA
Cross-Signing	One existing EV SSL CA that has been cross-certified with this new root CA (for EV SSL issuance).

	This CA is the one used to issue EV SSL certificates under the Certplus Class 2 already included within major browsers and OS. Note: The "KEYNECTIS Extended Validation CA" intermediate cert is cross-signed with all 5 of the new root certs. Comment #19: We have processed the test certs this way to allow you to check these certs without delay. When we issue "production" certificates (once the roots will be added to main browsers), we will create other sub-CAs for that purpose (like the "KEYNECTIS Extended Validation CA" but with a new name, certainly with OpenTrust inside!). So there is no worry on that topic for production certificates to come.
Externally Operated SubCAs	Currently none, but the CP does allow for external CAs. RCA CP section 1.1: The CP presents the requirements, principles and procedures that OpenTrust implements to create and manage its own Root Certification Authority (RCAs), Intermediate Certification Authorities (ICAs) and internal or external Certification Authorities (CAs). Internal CAs are signing CAs Internal and External CAs only issue certificates to subscribers (CA signed by RCA or ICA cannot issue CA certificates): - An internal CA is only represented by OpenTrust - An External CA is always represented by a Customer of OpenTrust which has a valid contract with OpenTrust, to cover service(s) defined in the CP and who wishes to have its CA certified by OpenTrust. A CA or an ICA that is certified by an OpenTrust RCA or an ICA has to enforce the present CP. Prior to certify a CA or an ICA, OpenTrust verifies that the CA or the ICA that requests certification enforces a CP and a CPS approved by OpenTrust. In case a CA is not supported by a CP based on an identified standard as mentioned below it cannot be signed by a RCA or an ICA. The present CP defines goals and requirements for: - Practices (business, legal, and technical) enforced by RCAs and ICAs to provide certification services that covers X.509 certificate life cycle management, including enrolment, issuance, renewal and revocation of CA Certificates, - Practices (legal, organizational and technical) enforced by RCAs, ICAs and CAs to create and protect their private key.
Technical Constraints on Third-party Issuers	RCA CP section 1.3.4: CAs are either owned by OpenTrust or by OpenTrust Customers. RCA CP section 1.3.5: An RA is owned by an entity/entities designated by Customer or OpenTrust. RCA CP section 1.1: The present CP represents the common requirements that RCAs, ICAs and CAs have to enforce to be signed by a RCA or an ICA and designates standards to be implemented by a CA in order to issue Subscriber (or Subject) Certificates. OpenTrust manages its RCA certificates lifecycle as detailed in [ETSI 102 042] and [ETSI 101 456]. CAs signed by a RCA or an ICA shall be audited against ETSI standards (102 042 and/or 101 456) or WebTrust (http://www.webtrust.org/item64428.aspx) or according to rules defined by [Adobe] for all types of Subscriber certificates it issues and in the certification path of the RCA. In case the CA issues SSL and / or email certificates, as an alternative to the above audits, this CA may be technically constrained in the CA certificate and audited by Opentrust. An OpenTrust RCA owns a self-signed certificate and represents the common anchor of all trusted link (certification path) created by the CA, optionally the ICA it certifies. The trusted links are built as follow: - RCA trust common anchor: self-signed RCA certificate generated and managed by OpenTrust according to the CP. - (optionally) ICA certificate: certificate delivered by the RCA according to the CP. - CA certificate: certificate delivered by the RCA or an ICA according to the CP. - Subscriber certificate: certificates delivered by the CA according to its CP. RCA CP section 4.1.2.3: CA certificates must be authorized by the PMA prior to issuance. The issuance process will include documenting the following information to be contained in the CA certificate request: …

	For SSL/TLS Certificate and email certificate under [Mozilla] program, choice for the CA **certificate between "audit" against ETSI standards, or [CAB Forum] for SSL/TLS, (refer to section 8 below) or "technical constraint" (refer to section 10.3 below).** o If Subscribers are only internal: Customer may choose to have only "technical constraint". o If some Subscribers are external: Customer shall choose to have "audit" against ETSI standards (refer to section 8 below). o If "Technical constraint" choice is made, then following information shall be provided: § All the domain name to be set in extension "Name Constraint" for "dnsNames" if Subscriber Certificate are for SSL certificate and/or email protection to be set in the CA certificate (refer to section 10.3 below). § All the domain name to be set in extension "Name Constraint" for "rfc822names" if Subscriber Certificate are for email protection to be set in the CA certificate (refer to section 10.3 below). § All the possible "Extended Key Usage" that are set in the Subscriber Certificate in order to be set in the CA certificate (refer to section 10.3 below).

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.opentrust.com/en/certification-policy "OpenTrust root CA certification policy" and "New Certplus root CA certification policy" both link to this document: RCA CP (English): http://www.opentrust.com/images/stories/DMS_RCA_Program_OpenTrust_CP_v_1_0s.pdf This CP applies to Root CA (RCA), Intermediate CA (ICA), and CA life cycle management. This CP applies to the new Certplus roots as well as the new OpenTrust roots. "SSL Extended Validation CA certificate policy…" links to this document: EV CP (English): https://www.opentrust.com/PDF/FR/PC/DSQ_NT_KEYNECTIS_EV_SSL_CA_CPS_20090504s.pdf This CP applies to management of Subscriber **EV SSL certificate issued by the new Certplus and OpenTrust roots**. I still cannot figure out how to get to the following document from a link in http://www.opentrust.com/en/certification-policy SSL CP (French): https://www.opentrust.com/images/stories/OpenTrust_DMS_PC_Certificats_OpenTrust_SSL_RGS_et_ETSI_V1_1s.pdf This CP applies to management of Subscriber EV SSL (fulfilling French "RGS" requirements, ie for certificates to be used in relation with French government), **OV SSL and DV SSL certificate issued by the new Certplus and OpenTrust roots.** The SSL CP is present in general paragraph for SSL (named K.SSL / Club SSL / ISP SSL): the PC is named "SSL Extended Validation CA certificate policy version" and is associated to https://www.opentrust.com/PDF/FR/PC/DSQ_NT_KEYNECTIS_EV_SSL_CA_CPS_20090504s.pdf. Publicly Disclosed intermediate certs for currently included root: https://www.opentrust.com/ca-certificate-program-opentrust/ca-certificate-program-opentrust.html
Audits	Audit Type: ETSI TS 102 042 OVCP Auditor: LSTI

	Audit Statement: http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf Would you please ask LSTI to add an indicator for when the BR audit criteria is also used? E.g. PTC-BR or such? https://wiki.mozilla.org/CA:BaselineRequirements Audit Type: WebTrust for EV Auditor: LSTI Audit Statement: https://www.opentrust.com/ca-certificate-program-opentrust/Ind_Aud_rep_LSTI_S.pdf (2014.01.23) Audit Type: Key Ceremony (2014.05.26) Auditor: LSTI Audit Statement: https://bugzilla.mozilla.org/attachment.cgi?id=8446826 Our existing audit covering our current CA used for EV certificate issuance. This audit will include new CAs in its next version to be done by January 2015.
Baseline Requirements (SSL)	URL to BR audit statement: see above. RCA CP section 1.1: [CAB Forum]: https://cabforum.org/ RCA CP section 1.3.1: The CP and CPS shall be consistent with: … and [ETSI 102 042] and [CAB Forum] according the level of trust selected for each type of Subscriber Certificate. It's not clear to me if this means the BRs (https://cabforum.org/baseline-requirements-documents/) or the EV Guidelines (https://cabforum.org/extended-validation/) or both.
SSL Verification Procedures	SSL CP (French): https://www.opentrust.com/images/stories/OpenTrust_DMS_PC_Certificats_OpenTrust_SSL_RGS_et_ETSI_V1_1s.pdf Please translate into English SSL CP sections: 4.1.2.1 4.1.2.2 4.1.2.3 4.2 4.3 Comment #9: === Therefore as an example, please find below a very short synthesis on our main requirements for our procedures used to manage final SSL certificates. For DV certificate: We **use only information found in a WHOIS database to contact and authenticate the Applicant's ownership or control of all requested Domain Name(s). We can also use email address like; webmaster@domain.com, postmaster@domain.com,**

	admin@domain.com , administrator@domain.com or hostmaster@domain.com. **[I couldn't find this. Which section is it in?]** We control the existence and content of domain name using WHOIS database. In addition to that, the Applicant shall transmit a legible copy of a valid government issued national identity document or photo ID (driver's licence, national ID or equivalent) to the RA. **Applicant shall sign a certificate request using its email with a challenge (OTP code).** **[I couldn't find this. Which section is it in?]** All information is contained in the CP defined to manage DV certificate published by OpenTrust. OpenTrust manages certificate according ETSI 102 042 DVCP. OpenTrust's CP used to manage SSL/TLS certificates named: "DMS_PC Certificates OpenTrust SSL RGS et ETSI V1.1". For OV certificate: We use only information found in a WHOIS databe to contact and authenticate the Applicant's ownership or control of all requested Domain Name(s). We can also use email address like; webmaster@domain.com, postmaster@domain.com, admin@domain.com , administrator@domain.com or hostmaster@domain.com. In addition to that, the Applicant shall provide a legible copy of a valid government issued national identity document or photo ID (driver's licence, national ID or equivalent) to the RA. Applicant shall sign a certificate request using its email with a challenge (OTP code). In addition to DV verification, the legal existence, legal name, legal form and requested address of the organization is verified using one of the following: - A government agency in the jurisdiction of the Applicant; - A third party database that is periodically updated and trusted by OpenTrust has being reasonably accurate and reliable; or - An attestation letter confirming that orgnaisation identity is correct written by an accountant, lawyer, government official, or other reliable third party trusted by OpenTrust has being reasonably accurate and reliable. In addition to DV verification, RA authenticates the Applicant is authorized to represent the organization, for certificate request, wishing to be named as the Subject in the Certificate by performing a telephone challenge/response to the Applicant's organization using a telephone number from a reliable source. All information is contained in the CP defined to manage OV certificate published by OpenTrust. OpenTrust manages certificate according ETSI 102 042 OVCP. For RGS certificate (French requirements): CA follows the requirement of ETSI 102 042 OVCP and CAB Forum requirements and applies the verification method defined for OV above. OpenTrust's CP used to manage SSL/TLS certificates named: "DMS_PC Certificates OpenTrust SSL RGS et ETSI V1.1". For EV certificate: The EV Guidelines are followed. OpenTrust is certified against EV Guidelines. OpenTrust's CP used to manage EV certificates named: "DSQ_NT_KEYNECTIS_EV_SSL_CA_CPS_20090504s.pdf". ===
Organization Verification Procedures	Comment #9: For Organization Verification Procedures: Please refer to section "SSL Verification Procedures" above
Email Address	Which document describes the verification procedures for email (S/MIME) certificates? i.e. which section/document explains the

Verification Procedures	steps that must be taken to verify that the certificate subscriber owns/controls the email address to be included in the certificate?
Code Signing Subscriber Verification Procedures	Comment #9: For Code Signing Subscriber Verification Procedures: Please refer to section "SSL Verification Procedures" above. OpenTrust follow the EV code signing baseline requirements.
Multi-factor Authentication	CP section 6.5.1 I read through this section in the RCA CP, but I did not find anything about a second-factor of authentication (in addition to the password). BR 16.5: The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.
Network Security	RCA CP section 6.7

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

Publicly Available CP and CPS	Yes. See above.
CA Hierarchy	Yes. See above.
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	Comment #9: IDN not currently supported.
Revocation of Compromised Certificates	CP section 4.9.1.3
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	See above
DNS names go in SAN	SSL CP section 7.1.1.2
Domain owned by a Natural Person	Comment #9: domain owned by natural person is only possible for DV certificate (not authorized for OV, French RGS and EV SSL). SAN shall be filled with at least one entry and one of the entries shall be placed in the CN of the DN of the subject. SSL CP section 7.1.1.2.
OCSP	See above

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

Long-lived DV certificates	Comment #9: DV certificate can't have a life time longer than 3 years.
Wildcard DV SSL certificates	Comment #9: OpenTrust issues Wildcard certificate but follow all verification required by CAB Forum only for DV and OV. Wildcard is not authorized for EV and French RGS certificate. DV and OV Certificates include a wildcard asterisk character. Before issuing a Wildcard certificate, RA verifies that rules given in section "11.1.3 Wildcard Domain Validation" from CAB Forum requirements for SSL/TLS certificate are respected.
Email Address Prefixes for DV Certs	See above
Delegation of Domain / Email validation to	**Yes. Both external CAs and External RAs are allowed. See above.**

third parties	Comment #9: In addition to that and as already explained in this section and in the RCA's CP, OpenTrust's PMA audits and approves all procedures from external entities signed by RCA. This control covers all PKI component of the PKI whom CA is signed by OpenTrust's RCA or ICA (refer to section 8 of RCA's CP). Additionally to that, when external entity is only RA for OpenTrust's CA, a contract shall be established between OpenTrust and external entity and the contract reference the procedure approved by PMA and that have to be used by RA. A contract is also required when a CA wants to get signed by OpenTrust. RCA CP section 8.1: According level of trust chosen for each type of Subscriber Certificate, audit of the CA (means all PKI component used by CA and RA and sample of Local Registration authority according the need of audit) shall be conducted with the following rules: - CA issue Subscriber Certificate for External Subscriber: o For DV SSL certificate: level of Trust shall be [ETSI 102 042] for DVCP plus relevant "CA:Information checklist" as described in [Mozilla]. Customer shall be successfully audited against this standard by external qualified auditor according schema 1, 2 or 3. o For OV SSL certificate: level of Trust shall be [ETSI 102 042] for OVCP plus relevant "CA:Information checklist" as described in [Mozilla]. Customer shall be successfully audited against this standard by external qualified auditor according schema 1, 2 or 3. o For EV SSL certificate: level of Trust shall be at minimum [ETSI 102 042] for EVCP plus relevant "CA:Information checklist" as described in [Mozilla]. Customer may choose also [ETSI 102 042] for EVCP+. Customer shall be successfully audited against this standard by external qualified auditor according schema 1, 2 or 3. o For other type of Subscriber certificate: any level of trust among [ETSI 102 042] and [ETSI 101 456] plus relevant "CA:Information checklist" as described in [Mozilla]. One level of trust for each type of Subscriber Certificate. Customer shall be successfully audited against all required standards for each type of Subscriber Certificate by auditor approved by PMA according schema 1, 2, 3 or 4.
Issuing end entity certificates directly from roots	Comment #9: All RCA and ICA of OpenTrust shall be off-line CA has mentioned in RCA's CP. RCA can only issue certificate for OCSP responder as mentioned in RCA's CP. RCAs are not authorized to issue others kind of Subscriber certificate.
Allowing external entities to operate subordinate CAs	**Yes. See above.** RCA's CP describes how Root CA, ICA and all CA (OpenTrust's CA and Customer's CA) are audited. Please refer to section 1.4, 4.1, 4.2 and 8 of the RCA's CP.
Distributing generated private keys in PKCS#12 files	Comment #9: CAs may be authorized by OpenTrust to issue such key pair and associated certificate. OpenTrust's has a CA who provides Pkcs#12 key pair and the process is audited each year by external entity (LSTI) according RGS and ETSI rules (102 042) and uses a HSM certified EAL4+ or FIPS 140-2 level 3. But for SSL/TLS certificate, OpenTrust doesn't generate the key for Subscriber.
Certificates referencing hostnames or private IP addresses	Comment #9: This practice is not authorized by OpenTrust. A CA can't be signed by RCA or ICA of OpenTrust if it delivers such kind of certificate.
Issuing SSL Certificates for Internal Domains	Comment #9: This practice is not authorized by OpenTrust. A CA can't be signed by RCA or ICA of OpenTrust if it delivers such kind of certificate.
OCSP Responses signed by a certificate	???

under a different root	
CRL with critical CIDP Extension	Comment #9: Not applicable as OpenTrust uses only full CRLs.
Generic names for CAs	Comment #9: Not applicable as mentioned in RCA's CP (section 3.1.1). RCA, ICA and CA certificates shall contain at least the name of the legal entity which owns the CA.
Lack of Communication With End Users	Comment #9: OpenTrust and its Customer communicate in case of incident about identity towards Subscriber and Relying Party and software platform providers (where RCA is referenced) if the incident may have an effect on entity that relies on the issued certificate under RCA trust certification path.
Backdating the notBefore date	Comment #9: All new certificates are always issued with starting date in the future (means a starting date that is later than the date of the operation to issue the certificate). OpenTrust can issue ICA or CA certificate with a starting date beginning in the past: this operation may only occur sfor ICA and CA certificate renewal operation with the same key pair and same DN than it was used in the previous ICA or CA certificate (refer to section 4.6 and 4.8).