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 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	CN = Certplus Root CA G2 O = Certplus

	C = FR	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 Error: Firefox can't find the server at certplusrootcag1-test.opentrust.com.	https://certplusrootcag2-test.opentrust.com Firefox can't find the server at certplusrootcag2-test.opentrust.com.
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 Maximum expiration time of OCSP responses	http://get-ocsp.certificat.com/certplusrootcag2 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 If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	1.3.6.1.4.1.22234.2.5.2.3.1 If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
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	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)."	unpredictable random data (preferably in the serial number)."

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 Firefox can't find the server at opentrustrootcag1-test.opentrust.com.	https://opentrustrootcag2-test.opentrust.com Firefox can't find the server at opentrustrootcag2-test.opentrust.com.	https://opentrustrootcag3-test.opentrust.com Firefox can't find the server at opentrustrootcag3-test.opentrust.com.
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 Maximum expiration time of OCSP responses	http://get-ocsp.certificat.com/opentrustrootcag2 Maximum expiration time of OCSP responses	http://get-ocsp.certificat.com/opentrustrootcag3 Maximum expiration time of OCSP responses
Requested	Websites (SSL/TLS)	Websites (SSL/TLS)	Websites (SSL/TLS)

Trust Bits	Email (S/MIME) Code Signing	Email (S/MIME) Code Signing	Email (S/MIME) Code Signing
SSL Validation Type	DV, OV, and EV	DV, OV, and EV	DV, OV, and EV
EV Policy OID(s)	1.3.6.1.4.1.22234.2.5.2.3.1 If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	1.3.6.1.4.1.22234.2.5.2.3.1 If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	1.3.6.1.4.1.22234.2.5.2.3.1 If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
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)."	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)."	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)."

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
Externally Operated SubCAs	None. The CP does allow for external CAs.
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.
Technical Constraints on Third-party Issuers	CP section 1.1: "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."

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.opentrust.com/en/certification-policy CP (English): http://www.opentrust.com/images/stories/DMS_RCA_Program_OpenTrust_CP_v_1_0s.pdf This CP applies to the new Certplus roots as well as the new OpenTrust roots. 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/ETSI.pdf Would you please ask LSTI to add an indicator for when the BR audit criteria is also used? E.g. DVCP-BR, OVCP-BR or such? 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. CP section 1.1: [CAB Forum]: https://cabforum.org/ 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.
SSL Verification Procedures	It's still not clear to me exactly what steps are taken to verify that the certificate subscriber owns/controls the domain name to be included in the certificate. I think there should be a description of this (in addition to referencing the various documents) in the CP/CPS, because there are different ways you can meet the requirements of the various documents. CP section 1.4.1.3: Subscriber Certificates for machine that are SSL/TLS certificates (Organization Validated, Domain Validated and EV SSL) shall be issued in accordance with the requirements of the [CAB Forum] requirements and according to requirements defined in [ETSI 102 042] (OV, DV and EV certificate level). As described in RCA CP section; 1.4, 4.1.2.3 and 8.1, CA signed under ICA or RCA SHALL be compliant [ETSI 102 042 DVCP] and all "CA:Information checklist" as described in [Mozilla, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ and https://wiki.mozilla.org/CA:Information_checklist]. PMA has a established an audit program as described in section 8.1 in order to check the compliance of CA against [ETSI 102 042 DVCP] and all "CA:Information checklist" as described in [Mozilla]. These CA will be checked by PMA as compliant in its CP and CPS and practice for the requirements mentioned above. As described in RCA CP section; 1.4, 4.1.2.3 and 8.1, CA signed under ICA or RCA SHALL be compliant [ETSI 102 042 EVCP] and all "CA:Information checklist" as described in [Mozilla, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ and https://wiki.mozilla.org/CA:Information_checklist]. PMA has a established an audit program as described in section 8.1 in order to chek the compliance of CA against [ETSI 102 042 EVCP] and all "CA:Information checklist" as described in [Mozilla]. These CA will be checked by PMA as compliant in its CP and CPS and practice for the requirements mentioned above.
Organization Verification Procedures	It's still not clear to me exactly what steps are taken to verify the organization and identity of the certificate subscriber. I think there should be a description of this (in addition to referencing the various documents) in the CP/CPS, because there are different ways you can meet the requirements of the various documents. As described in RCA CP section; 1.4, 4.1.2.3 and 8.1, CA signed under ICA or RCA SHALL be compliant [ETSI 102 042 OVCP] and all "CA:Information checklist" as described in [Mozilla, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ and https://wiki.mozilla.org/CA:Information_checklist]. PMA has a established an audit program as described in section 8.1 in order to chek the compliance of CA against [ETSI 102 042 OVCP] and all "CA:Information checklist" as described in [Mozilla]. These CA will be checked by PMA as compliant in its CP and CPS and practice for the requirements mentioned above.
Email Address Verification	It's still not clear to me exactly what steps are taken to verify that the certificate subscriber owns/controls the

Procedures	email address to be included in the certificate. I think there should be a description of this (in addition to referencing the various documents) in the CP/CPS, because there are different ways you can meet the requirements of the various documents. As described in RCA CP section; 1.4, 4.1.2.3 and 8.1, CA signed under ICA or RCA SHALL be compliant [ETSI 102 042] or [101 456] and all "CA:Information checklist" as described in [Mozilla, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ and https://wiki.mozilla.org/CA:Information_checklist]. PMA has a established an audit program as described in section 8.1 in order to chek the compliance of CA against [ETSI 102 042] or [ETSI 101 456] and all "CA:Information checklist" as described in [Mozilla]. These CA will be checked by PMA as compliant in its CP and CPS and practice for the requirements mentioned above.
Code Signing Subscriber Verification Procedures	It's still not clear to me exactly what steps are taken to verify that the certificate subscriber owns/controls the domain name to be included in the certificate. I think there should be a description of this (in addition to referencing the various documents) in the CP/CPS, because there are different ways you can meet the requirements of the various documents. As described in RCA CP section; 1.4, 4.1.2.3 and 8.1, CA signed under ICA or RCA SHALL be compliant [ETSI 102 042] or [101 456] and all "CA:Information checklist" as described in [Mozilla, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ and https://wiki.mozilla.org/CA:Information_checklist]. PMA has a established an audit program as described in section 8.1 in order to chek the compliance of CA against [ETSI 102 042] or [ETSI 101 456] and all "CA:Information checklist" as described in [Mozilla]. These CA will be checked by PMA as compliant in its CP and CPS and practice for the requirements mentioned above.
Multi-factor Authentication	CP section 6.5.1
Network Security	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	???
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	???
Domain owned by a Natural Person	???
OCSP	See above

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

Long-lived DV certificates	

Wildcard DV SSL certificates	
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	
Issuing end entity certificates directly from roots	
Allowing external entities to operate subordinate CAs	
Distributing generated private keys in PKCS#12 files	
Certificates referencing hostnames or private IP addresses	
Issuing SSL Certificates for Internal Domains	
OCSP Responses signed by a certificate under a different root	
CRL with critical CIDP Extension	
Generic names for CAs	
Lack of Communication With End Users	
Backdating the notBefore date	