Bugzilla ID: 543639
Bugzilla Summary: Add AffirmTrust root certificates

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.
AffirmTrust has provided a table showing their conformance to the Recommended Practices: https://bugzilla.mozilla.org/attachment.cgi?id=428780.

General Info	Data
CA Name	AffirmTrust LLC
Website URL	http://www.affirmtrust.com/
Organizational type	Private Corporation
Primary market / customer base	AffirmTrust is a new Certificate Authority based in the US. AffirmTrust plans to offer certificates for web-based and mobile applications including microbanking, debit cards and smartcards, mobile phone applications, new media, cloud computing, social networking, etc.
CA Contact Information	CA Email Alias: pkipolicv@affirmtrust.com CA Phone Number: 503-243-5405 Title / Department: PKI Policy Administrator

Info Needed	Data
Certificate Name	AffirmTrust is requesting the inclusion of 4 root certificates: 1. AffirmTrust Commercial 2. AffirmTrust Networking 3. AffirmTrust Premium 4. AffirmTrust Premium ECC
Cert summary / comments	Each root will sign internally-operated sub-CAs which will sign end-entity certificates. AffirmTrust initially plans to only issue EV SSL certificates, but may in the future issue DV SSL, OV SSL, email (S/MIME), and code signing certificates under different sub-CAs of each root.
Root Cert URL	AffirmTrust Commercial: https://bugzilla.mozilla.org/attachment.cgi?id=425501 AffirmTrust Networking: https://bugzilla.mozilla.org/attachment.cgi?id=425506 AffirmTrust Premium: https://bugzilla.mozilla.org/attachment.cgi?id=425507 AffirmTrust Premium ECC: https://bugzilla.mozilla.org/attachment.cgi?id=425513
SHA-1 fingerprint	AffirmTrust Commercial: F9:B5:B6:32:45:5F:9C:BE:EC:57:5F:80:DC:E9:6E:2C:C7:B2:78:B7 AffirmTrust Networking: 29:36:21:02:8B:20:ED:02:F5:66:C5:32:D1:D6:ED:90:9F:45:00:2F AffirmTrust Premium: D8:A6:33:2C:E0:03:6F:B1:85:F6:63:4F:7D:6A:06:65:26:32:28:27 AffirmTrust Premium ECC: B8:23:6B:00:2F:1D:16:86:53:01:55:6C:11:A4:37:CA:EB:FF:C3:BB

Valid from	2010-01-29 (all four roots)
Valid to	AffirmTrust Commercial and AffirmTrust Networking: 2030-12-31 AffirmTrust Premium and AffirmTrust Premium ECC: 2040-12-31
Cert Version	3
Modulus length or type of signing key	AffirmTrust Commercial and AffirmTrust Networking: 2048 AffirmTrust Premium: 4096 AffirmTrust Premium ECC: Elliptic Curve secp384r1 (1 3 132 0 34)
Test Websites	AffirmTrust Commercial - https://commercial.affirmtrust.com/ AffirmTrust Networking - https://networking.affirmtrust.com:4431/ AffirmTrust Premium - https://premium.affirmtrust.com:4432/ AffirmTrust Premium ECC – https://premiumecc.affirmtrust.com:4433/
CRL URLs	http://crl.affirmtrust.com/crl/AffirmTrustCommercial.crl http://crl.affirmtrust.com/crl/aftcomev2.crl (NextUpdate: 7 days) http://crl.affirmtrust.com/crl/AffirmTrustNetworking.crl http://crl.affirmtrust.com/crl/aftnetworkev2.crl (NextUpdate: 7 days) http://crl.affirmtrust.com/crl/AffirmTrustPremium.crl http://crl.affirmtrust.com/crl/aftpremev2.crl (NextUpdate: 7 days) http://crl.affirmtrust.com/crl/AffirmTrustPremiumECC.crl http://crl.affirmtrust.com/crl/aftpremeccev2.crl (NextUpdate: 7 days) CPS Section II.I: End-entity certificate CRLs will be updated and reissued at least every seven days, and the nextUpdate field value will not be more than ten days, except as otherwise provided in AffirmTrust's Business Continuity Plan. AffirmTrust shall post the CRLs online at www.affirmtrust.com/resources at the interval stated in the previous sentence (but also within 24 hours of a Certificate revocation) in a DER format.
OCSP	* AffirmTrust Commercial: http://ocsp.affirmtrust.com/commev * AffirmTrust Networking: http://ocsp.affirmtrust.com/ntwkev * AffirmTrust Premium: http://ocsp.affirmtrust.com/premev * AffirmTrust Premium ECC: http://ocsp.affirmtrust.com/premeccev CPS Section II.I: AffirmTrust shall provide revocation information for end-entity EV Certificates via an OCSP service that is updated at least every four days, and OCSP responses from this service will have a maximum expiration time of ten days.
CA Hierarchy	Each root only signs internally-operated subordinate CAs that sign the end-entity certificates. The subordinate CAs for SSL certificates distinguish the level of authentication. Currently each root only has one subordinate CA, for issuing EV SSL certificates. There are provisions in Appendix A of the CPS for issuing additional subordinate CAs and types of certificates in the future.

	AffirmTrust Commercial planned sub-CAs: • AffirmTrust Commercial Extended Validation – for signing EV SSL end-entity certs. • AffirmTrust Commercial OV Sub-CA – for signing Organization Validated end-entity certs. • AffirmTrust Commercial DV Sub-CA – for signing Domain Validated end-entity certs. • End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Commercial *[additional information re sub-CA and authentication method]*. Key length will be 2048 bits. AffirmTrust Networking planned sub-CAs: • AffirmTrust Networking Extended Validation – for signing EV SSL end-entity certs. • AffirmTrust Networking OV Sub-CA – for signing Organization Validated end-entity certs. • AffirmTrust Networking DV Sub-CA – for signing Domain Validated end-entity certs. • End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Networking *[additional information re sub-CA and authentication method]*. Key length will be 2048 bits. AffirmTrust Premium planned sub-CAs: • AffirmTrust Premium Extended Validation – for signing EV SSL end-entity certs. • AffirmTrust Premium OV Sub-CA – for signing Organization Validated end-entity certs. • AffirmTrust Premium DV Sub-CA – for signing Domain Validated end-entity certs. • End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Premium *[additional identity information re sub-CA and authentication method.]* Key length will be 4096 bits. AffirmTrust Premium ECC planned sub-CAs: • AffirmTrust Premium ECC Extended Validation – for signing EV SSL end-entity certs. • AffirmTrust Premium ECC OV Sub-CA – for signing Organization Validated end-entity certs. • AffirmTrust Premium ECC DV Sub-CA – for signing Domain Validated end-entity certs. • End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Premium ECC *[additional identity information re sub-CA and authentication method.]* Key length will be 384 bits.
Sub-CAs operated by third parties	No sub-CAs will be operated by third parties now or in the near future. If that changes, AffirmTrust will amend their CPS as stated at CPS Sec.V.A, and also follow Mozilla's checklist at that time. CPS V.A: AffirmTrust has not authorized any external sub-CAs to be operated by third parties at the present time. In the event AffirmTrust decides to authorize any external sub-CAs to be operated by third parties in the future, AffirmTrust intends to amend this

	CPS to impose legal, technical, attestation and audit, and other requirements on the sub-CAs substantially equivalent to those followed by AffirmTrust for similar certificates. In the event an external sub-CA is authorized to issue EV Certificates, AffirmTrust intends to state in its CPS AffirmTrust's practices following all relevant rules as stated in the EV Guidelines concerning external sub-CAs operated by third parties (as such rules may be amended from time to time in the Guidelines), including but not limited to EV Guidelines 7.1.2(3), 8.2.2, 10.12, 11.1.1(1), 12.2.2, and 15.2.2.
Cross-signing	None, and none in plan.
Requested Trust Bits	Websites
SSL Validation Type	DV, OV, EV CPS section III.B: At the present time, AffirmTrust issues only Extended Validation Server Certificates and only to Private Organizations created in the United States as defined in the EV Guidelines. AffirmTrust does not presently issue Domain Validated (DV) Certificates (SSL/TLS), Organization Validated (OV) Certificates (SSL/TLS), Email (S/MIME) Certificates, or Code Signing Certificates. In the event AffirmTrust decides to issue one or more of these other Certificate types, it will amend its CPS at that time to include generally the authentication and issuing procedures listed in Appendix A, as applicable for each Certificate type, as well as all applicable CA/Browser Forum guidelines.
EV Policy OIDS	AffirmTrust Commercial: 1.3.6.1.4.1.34697.2.1 AffirmTrust Networking: 1.3.6.1.4.1.34697.2.2 AffirmTrust Premium: 1.3.6.1.4.1.34697.2.3 AffirmTrust Premium ECC: 1.3.6.1.4.1.34697.2.4
CP/CPS	AffirmTrust document repository: http://www.affirmtrust.com/resources/ AffirmTrust Certification Practice Statement (English): http://www.affirmtrust.com/repo/AffirmTrust_CPS_v1.1_12-23-2010.pdf Relying Party Agreement: http://www.affirmtrust.com/repo/AffirmTrust_Relying_Party_Agreement_v1.1_12-23-2010.pdf
AUDIT	Audit Type: WebTrust CA Auditor: IS Partners, LLC, which is part of Interactive Solutions, LLC Auditor Website: http://www.ispartnersllc.com, http://www.interactivesolutionsllc.com/ Audit Report: https://bugzilla.mozilla.org/attachment.cgi?id=428774 (2010.01.31) Audit Type: WebTrust EV Auditor: IS Partners, LLC, which is part of Interactive Solutions, LLC Auditor Website: : http://www.ispartnersllc.com, http://www.interactivesolutionsllc.com/ Audit Report: https://bugzilla.mozilla.org/attachment.cgi?id=428776 (2010.01.31) Subject: Re: Verifying Authenticity of AffirmTrust audit reports Date: Fri, 26 Feb 2010 18:01:56 +0000 From: dbell@interactivesolutionsllc.com We did indeed perform the audits you have inquired about. If you go to the Webtrust website, you will find us as an approved provider to perform WebTrust and SysTrust. … The folks at the CICA are also very familiar with our work.

Organization Identity Verification for EV SSL certs	CPS Section II.D: When AffirmTrust issues an EV Certificate, AffirmTrust represents and warrants to the EV Certificate Beneficiaries, during the period when the EV Certificate is Valid, that AffirmTrust has followed the requirements of the EV Guidelines and its EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate ("EV Certificate Warranties"). The EV Certificate Warranties specifically include, but are not limited to, the following: (1) Legal Existence. AffirmTrust has confirmed with the incorporating or registration agency in the Subject's jurisdiction of incorporation or registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the jurisdiction of incorporation or registration; (2) Identity. In accordance with the procedures stated in the EV Guidelines, AffirmTrust has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the incorporating or registration agency in the Subject's jurisdiction of incorporation or registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its place of business; (3) Right to Use Domain Name. AffirmTrust has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use the domain name(s) listed in the EV Certificate; (4) Authorization for EV Certificate. AffirmTrust has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate; (5) Accuracy of Information. AffirmTrust has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued; (6) Subscriber Agreement. The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with AffirmTrust that satisfies the requirements of the EV Guidelines or the Applicant Representative has acknowledged and accepted the Terms of Use (if applicable);
Organization Identity Verification for non-EV SSL certs	CPS Appendix A.3.2: Whenever an organization name is included in the Certificate (e.g., for OV Certificates), AffirmTrust will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. AffirmTrust will ensure the following: (a) the Organizational Name appears in conjunction with a country and possibly a state or province of other locality to sufficiently identify its place of registration or a place where it is currently doing business; and (b) in the case of an Organization that could reasonably be expected to be registered with a local, state or national authority, in certain circumstances AffirmTrust will obtain, view and verify copies of the registration documents. For instance, AffirmTrust may (a) verify the validity of the registration through the authority that issued it, or (b) verify the validity of the registration through a reputable third party database or other resource, or (c) verify the validity of the Organization through a trusted third party data source, or (d) confirm that the Organization exists if such Organization is not the type that is typically registered or is capable of being verified under clause (b).
Domain Name Ownership / Control for EV SSL Certs	CPS Section I.C.1: AffirmTrust Extended Validation Server Certificates are X.509 Certificates with SSL Extensions that chain to the following AffirmTrust's Certificate Authority trusted roots: AffirmTrust Commercial, AffirmTrust Networking, AffirmTrust Premium, and AffirmTrust Premium ECC, and which facilitate secure electronic commerce by providing limited authentication of a Subscriber's server and permitting SSL encrypted transactions between a Relying Party's browser and the Subscriber's server. AffirmTrust conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates ("Guidelines") published at http://www.cabforum.org, and implements the EV Guidelines through this CPS and AffirmTrust's other EV Policies. In the event of any inconsistency between AffirmTrust's EV Policies and the EV Guidelines, the EV Guidelines take precedence.

	CPS Section II.D: When AffirmTrust issues an EV Certificate, AffirmTrust represents and warrants to the EV Certificate Beneficiaries, during the period when the EV Certificate is Valid, that AffirmTrust has followed the requirements of the EV Guidelines and its EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate ("EV Certificate Warranties"). The EV Certificate Warranties specifically include, but are not limited to, the following: (3) Right to Use Domain Name. AffirmTrust has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use the domain name(s) listed in the EV Certificate;
Domain Name Ownership / Control for non-EV SSL Certs	AffirmTrust currently only issues EV SSL certificates. If, in the future they decide to issue non-EV SSL certificates, then they will follow Appendix A of their CPS. Appendix A, section 3.3 Authentication of Domain Name When a domain name is included in a Certificate together with an organization name (e.g., for OV Certificates), AffirmTrust will verify that the Subscriber had the right to use the domain name submitted by the Subscriber at the time it submitted its application. For instance, AffirmTrust may perform this verification by confirming that the Subscriber is the same person or entity that holds the domain name registration from the relevant domain name registrar or that the Subscriber is otherwise authorized to use such domain name. When a domain name is included in a Certificate without authentication of the entity owning the domain name (e.g., for DV Certificates), AffirmTrust will verify that the Subscriber has control over such domain name at the time it submitted its enrollment form by accessing a third party database of domain names and their owners. To do this, AffirmTrust will send an e-mail message to one of the following e-mail addresses requesting confirmation of the Certificate order and authorization to issue the Certificate in the domain name: (a) an e-mail address listed as the administrative or technical contact for the domain name in an official InterNIC domain name registry that includes the domain name, (b) a limited list of the most commonly used generic e-mail addresses for authorized persons at domain names (e.g., "*admin@domain.com*," or "*hostmaster@domain.com*" for the domain name domain.com), or (c) using a manual process conducted by AffirmTrust, to another e-mail address containing the domain name that is listed as the Common Name in the enrollment form. Upon receipt of a confirming e-mail message authorizing issuance of the Certificate, AffirmTrust will issue the Certificate as described below. Additionally, a confirmatory phone call to the applicant may be performed for Domain Control Certificate applications.
Email Address Ownership / Control	Not applicable – AffirmTrust currently only issues SSL server certificates.
Identity of Code Signing Subscriber	Not applicable – AffirmTrust currently only issues SSL server certificates.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices AffirmTrust provided a table detailing their compliance: https://bugzilla.mozilla.org/attachment.cgi?id=428781 Below is a summary. • Long-lived DV certificates ○ CPS Section I.C.2: At the present time, AffirmTrust issues only Extended Validation Server Certificates. AffirmTrust Extended Validation Server Certificates have an Operational Period of 379 days from the date of issuance unless the Certificate is revoked prior to the expiration of the Certificate's Operational Period.

	○ In the event this CPS is amended and AffirmTrust issues Organization Validated (OV) Certificates, Domain Validated (DV) Certificates, or other Certificate types, the operational period for such certificates will be specified at that time, and will comply with all applicable CA/Browser Forum guidelines. • Wildcard DV SSL certificates ○ CPS Section I.C.1: AffirmTrust does not issue wildcard certificates, or issue certificates referencing hostnames or private IP addresses. • Delegation of Domain / Email validation to third parties ○ CPS III.B: AffirmTrust does not delegate any of its Extended Validation authentication functions to subordinate CAs, RAs, Enterprise RAs, and subcontractors at the present time. In the event AffirmTrust decides to delegate any of its Extended Validation authentication functions to such parties in the future, AffirmTrust intends to amend its CPS to follow all relevant rules as stated in the EV Guidelines concerning authentication by such parties (as such rules may be amended from time to time in the Guidelines), including but not limited to EV Guidelines 12.2, 14.1.2, and 14.1.3, and to disclose its requirements concerning appropriate attestations and/or audits to confirm compliance by such parties. ○ In the event AffirmTrust decides to delegate any of its authentication functions for non-EV Certificates to such parties in the future, AffirmTrust intends to amend its CPS to disclose its requirements concerning appropriate attestations and/or audits from the parties to confirm compliance by such parties. • Issuing end entity certificates directly from roots ○ CPS section V.A: End-entity certificates are not issued off AffirmTrust's root certificates, but are issued off intermediate certificates • Allowing external entities to operate unconstrained subordinate CAs ○ CPS section V.A: AffirmTrust has not authorized any external sub-CAs to be operated by third parties at the present time. In the event AffirmTrust decides to authorize any external sub-CAs to be operated by third parties in the future, AffirmTrust intends to amend this CPS to impose legal, technical, attestation and audit, and other requirements on the sub-CAs substantially equivalent to those followed by AffirmTrust for similar certificates. In the event an external sub-CA is authorized to issue EV Certificates, AffirmTrust intends to state in its CPS AffirmTrust's practices following all relevant rules as stated in the EV Guidelines concerning external sub-CAs operated by third parties (as such rules may be amended from time to time in the Guidelines), including but not limited to EV Guidelines 7.1.2(3), 8.2.2, 10.12, 11.1.1(1), 12.2.2, and 15.2.2. • Distributing generated private keys in PKCS#12 files ○ CPS III.C: Subscribers submit their Public Key to AffirmTrust for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other package digitally signed by the Subscriber's Private Key in a session secured by Secure Sockets Layer (SSL). ○ CPS III.L: AffirmTrust does not provide Subscriber Key Pair generation or Subscriber Private Key protection for the Certificates. • Certificates referencing hostnames or private IP addresses ○ CPS section I.C.1: AffirmTrust does not issue wildcard certificates, or issue certificates referencing hostnames or

	private IP addresses.
	• OCSP Responses signed by a certificate under a different root
	  o Test websites have OCSP URI in the AIA, and they load without error into my Firefox browser with OCSP enforced.
	• CRL with critical CIDP Extension
	  o AffirmTrust does not plan to issue CRLs with critical CIDP extensions
	  o All of the CRLs imported into the Firefox browser without error.