AFFIRMTRUST'S RESPONSE TO MOZILLA'S "CA RECOMMENDED PRACTICES" – February 22, 2010

As part of its root certificate program, Mozilla has published a list of "CA Recommended Practices" at https://wiki.mozilla.org/CA:Recommended_Practices. AffirmTrust is in compliance with these recommended practices, as demonstrated below.

CA Recommended Practices

This page contains a draft set of recommended practices for CAs wishing to have their root CA certificates included in Mozilla products. In some cases these practices are specified or implied by the Mozilla CA certificate policy and are mandatory for a CA to have its root certificate(s) included. In other cases the recommended practices are not mandatory per policy, but will help speed up a CA's application for inclusion and maximize the chances of its application being approved.

Mozilla list of CA Recommended Practices: **Publicly Available CP and CPS**	**AffirmTrust Response**
CAs should supply the complete Certification Policy (CP) and Certification Practice Statement (CPS) containing sufficient information to determine whether and how the CA complies with the Mozilla policy requirements.	AffirmTrust does not maintain a CP (see CPS Section VII.A) but publishes its CPS at http://www.affirmtrust.com/resources/
The CP/CPS should be publicly available from the CA's official web site.	See CPS at http://www.affirmtrust.com/resources/
The format of the CP/CPS document should be PDF or another suitable format for reading documents. CAs should *not* use Microsoft Word or other formats intended primarily for editable documents.	Our CPS is published in PDF format.
The CP/CPS should be available in an English version.	Our CPS is in English.
The CA should provide references to the CP/CPS sections (e.g., by section number and/or page number) that address the requirements of the Mozilla policy.	Our cross references between our CPS and Mozilla policy are presented below.

CA Hierarchy	
A hierarchical structure of a single root with intermediate certs (subroots) is preferred. The single top-level root's public certificate is supplied for Mozilla's root list; the subroots are not. See CA:Recommendations_for_Roots	AffirmTrust meets this standard. See root and subroot hierarchy at CPS Section V.A.
CAs that issue certificates under multiple subordinate CAs (i.e., under a root CA whose CA certificate is being requested for inclusion) or under multiple CA hierarchies (i.e., rooted at multiple root CAs, one or more of whose certificates is being requested for inclusion) should provide additional information as noted:	
The CA should provide a graphical or textual description of the CA hierarchy or hierarchies, including which subordinates are under which root CAs	A textual description of the CA hierarchy is provided at CPS Section V.A.
The CA should indicate the general types of certificates (i.e., for SSL/TLS servers, email signing/encryption, and code signing) issued by each subordinate CA under each root.	See CPS Sec. I.C 1 and 2.
Where a CP/CPS applies to multiple subordinate CAs and/or multiple CA hierarchies, the CA should indicate whether particular sections of the CP/CPS apply to different subordinates and/or hierarchies and, if so, what the differences are.	All sections of AffirmTrust's CPS apply equally to all roots and subroots.
Audit Criteria	
CAs should supply evidence of their being evaluated according to one or more of the criteria accepted as suitable per the Mozilla policy.	See WebTrust and EV WebTrust audits dated January 31, 2010 submitted to Mozilla Bug 543639
The CA should indicate exactly which criteria they are being evaluated against (i.e., which of the criteria listed in the Mozilla policy).	Our audit reports are based on the criteria of WebTrust for CAs and WebTrust for CAs – Extended Validation Criteria.
All documents supplied as evidence should be publicly available.	Our audits are posted on Mozilla Bug 543639 and at our website http://www.affirmtrust.com/resources/
Documents purporting to be from the CA's auditor (or other	Our auditors will respond to any request from Mozilla

evaluator) should be available directly from the auditor (e.g., as documents downloadable from the auditor's web site).	for authentication of the audit reports and/or provide a copy of the reports directly to Mozilla.
Document Handling of IDNs in CP/CPS	
If a CA allows the use of internationalized domain names (IDNs) in certificates (e.g., as issued for SSL/TLS-enabled servers), the CA should address the issue of homographic spoofing of IDNs in their CP/CPS, even if primary responsibility for dealing with this issue falls on domain registries. (This doesn't mean that the CAs must prevent such spoofing. It merely means that a CA should describe how it handles the issue of spoofing when authenticating the owner of a domain.)	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. See CPS Sec. I.C.1. We follow EV Guideline Sec. 10.6.2(4), which provides as follows: "**Mixed Character Set Domain Names:** EV Certificates MAY include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. The CA MUST visually compare any Domain Names with mixed character sets with known high risk domains. If a similarity is found, then the EV Certificate Request MUST be flagged as High Risk. The CA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization."
Revocation of Compromised Certificates	
CAs should revoke certificates with private keys that are known to be compromised, or for which verification of subscriber information is known	See AffirmTrust's certificate revocation procedures at CPS III.I.1.

to be invalid.	
Verifying Domain Name Ownership	
WHOIS may be used by some CAs as a source of information for checking ownership/control of the domain name for SSL certificate applications. WHOIS information may be subject to compromise. CAs are responsible for implementing appropriate methods to reduce the risk of compromise. For example, direct command line, HTTPS to the original registrar, or correlating multiple sources. The CA should include information in their CP/CPS about the method that they use to validate the integrity of the data.	AffirmTrust only issues EV certificates, and follows the authentication procedures specified in the CA/Browser Forum Extended Validation Guidelines. See CPS Sec. I.C.1. The Guidelines contain multiple processes for verifying subscriber information and domain control.
Verifying Email Address Control	
Section 7 of the Mozilla CA Certificate Policy states: “for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate”	Not applicable – AffirmTrust only issues SSL server certificates. See CPS I.C.1.
The recommended way to satisfy this requirement is to perform a challenge-response type of procedure in which the CA sends email to the email address to be included in the certificate, and the applicant must respond in a way that demonstrates that they have control over that email address. For instance, the CA may send an email to the address to be included in the certificate, containing secret unpredictable information, giving the applicant a limited time to use the information within.	Not applicable – see above.