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

As part of its root certificate program, Mozilla has published a list of "Potentially Problematic CA Practices at https://wiki.mozilla.org/CA:Problematic_Practices. AffirmTrust is in compliance with (i.e., is not engaging in) this list of problematic practices, as demonstrated below.

Potentially problematic CA practices

This page contains draft comments about various CA practices that have been the subject of discussion in past CA evaluations. In general these practices are not explicitly addressed by the Mozilla CA certificate policy, and we do not necessarily consider them security risks. However we want to highlight them because they've occasioned controversy in the past and have in some cases caused approval of applications to be delayed. Some of these practices may be addressed in future versions of the policy.

Mozilla list of potentially problematic CA practices: **Long-lived DV certificates**	**AffirmTrust Response**
A domain-validated SSL certificate attests only to ownership and control of a domain name, and the owner of a domain name may have acquired it from others. It is therefore possible for the previous owner of the domain to have a still-valid DV certificate for the domain. If such a valid certificate (and associated private key) were to be used in conjunction with a DNS spoofing attack it would allow a malicious site to masquerade as a legitimate site and bypass the protection afforded by SSL.	AffirmTrust does not presently issue domain-validated SSL certificates, and so this is not an issue. See CPS Sec. I.C.1. In addition, certificates are to be revoked upon a change in ownership of a Subscriber's web server. See CPS Sec. III.I.1.
Some CAs issue DV SSL certificates that have expiration times several years in the future. This increases the time during which the possibility of such an attack exists.	See above.
Wildcard DV SSL certificates	
Some CAs issue domain-validated SSL certificates that can function as wildcard certificates, e.g., a certificate for *.example.com where the CA	AffirmTrust does not issue DV or wildcard certificates. See CPS Sec. I.C.1.

verifies only ownership and control of the example.com domain, and the certificate subscriber can then use the certificate with any site foo.example.com, bar.example.com, etc. This means that a subscriber could establish malicious SSL-protected web site that are deliberately named in imitation of legitimate sites, e.g., paypal.example.com, without knowledge of the CA. Concerns have been expressed that wildcard SSL certificates should not be issued except to subscribers whose actual identity has been validated with organizational validation (OV). (There are no EV wildcard certificates.)	
Delegation of Domain / Email validation to third parties	
Domain and Email validation are core-requirements of the Mozilla CA Policy and should always be incorporated into the issuing CAs procedures whenever possible. Registration Authorities (RA) or other third parties performing such functions must provide attestations about their procedures and/or should be audited together with the issuing CA. The CA must demonstrate clear and efficient controls attesting the performance of its RAs. Delegation of domain/email validation to third parties should generally be avoided.	AffirmTrust does not delegate any authentication procedures to external RAs. In addition, 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. Under EV Guideline 12.2.3, any future external RA must contractually commit to follow the EV Guidelines as to authentication of subscribers. Under EV Guideline 14.1.2 and 14.1.3(1), all external RAs are subject to the same self-audit and independent audit requirements of the CA. AffirmTrust will follow these rules if it uses an external RA in the future.
Issuing end entity certificates directly from roots	
Some CAs issue end entity certificates directly from the root (i.e., signed	AffirmTrust does not issue end-entity certificates

using the root CA private key). This is not as secure as using an offline root and issuing certificates using a subordinate CA.	directly from its roots, but instead issues them from its subordinate CAs. See CPS Sec. V.A.
Allowing external entities to operate unconstrained subordinate CAs	
Some CAs authorize external entities to operate their own CAs as subordinate CAs under the original CA's root. This raises concerns relating to whether or not such external entities are audited in a manner equivalent to the root CA, as well as what legal and technical arrangements constrain the external entities.	AffirmTrust has not authorized any external entities to operate their own CAs. In the event this changes, AffirmTrust will require the external entities to follow the same rules as AffirmTrust follows, and to document their compliance.
Distributing generated private keys in PKCS#12 files	
It is reported that some CAs generate the key pairs for their subscribers, rather than having the subscribers generate their own key pairs, and once generated, those CAs distribute the private key, together with the issued public key certificate and its chain, to the subscriber in a PKCS#12 file. The issues include:	AffirmTrust does not provide subscriber key pair generation services. See CPS Sec. III.L.
The user doesn't know or control who else possesses and can use his private key (decrypt his private messages or forge his signature), and	See above.
The distribution channels used (e.g. unencrypted email) may not be adequately secured.	See above.
Certificates referencing hostnames or private IP addresses	
The standard model for SSL on the web assumes that an SSL certificate references a domain name that is resolvable using the public DNS infrastructure (e.g., "www.example.com") or an IP address that is reachable from the public Internet. However it is also possible to include in a certificate a hostname not resolvable through the public DNS (e.g., "home") or a private IP address (e.g., 192.168.1.101); for example, this might be done for a corporate intranet with SSL-enabled servers behind a firewall and employees who don't want to enter fully-qualified domain names.	AffirmTrust does not issue certificates referencing hostnames or private IP addresses. See CPS I.C.1.
We consider this a problematic practice for a public CA because a	See above.

subscriber who obtains a certificate of this type could in theory use it in contexts other than the one for which the certificate was obtained, and in particular could use it to help enable an SSL MITM attack on users in other organizations who are using the same hostname or IP address for their own SSL-enabled servers. (Depending on the hostnames and private IP addresses used, this vulnerability might also affect users of home networks with SSL-enabled home gateway devices.)	
It is also a problematic practice to issue a certificate with non resolvable DNS or private IP and resolvable DNS addresses together.	See above.
Issuing SSL Certificates for Internal Domains	
It has come to our attention that some Certification Authorities may have mistakenly issued SSL certificates to non-existent .int domain names. This appears to have happened because the .int domain may have been confused with internal domain names, and not all of the CAs and RAs may be aware that .int is an ICANN approved TLD.	AffirmTrust only issues EV SSL certificates in compliance with the CA/Browser Forum Extended Validation Guidelines, and so would not be able to issue certs to a non-existent .int domain names under applicable EV Guidelines for authentication.
Section 7 of Mozilla's CA Certificate Policy states that CAs need to take "reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate." There are different interpretations as to what this means in regards to internal domain names such as non-valid TLDs, hostnames, and IP addresses. However, there is consensus that there are problems associated with issuing certificates for servers on internal networks under the same CA hierarchy as certificates for servers on public networks. Mozilla is currently discussing whether the CA Certificate Policy should be updated to add more explicit requirements on this practice, or even to disallow it altogether.	See above.
If you have issued certificates for internal domains within your CA hierarchy, Mozilla requests that you take the following actions:	See above.
1. Perform an internal audit to look for certificates that have been issued within your CA hierarchy which have .int domain names in the Common Name and/or as DNS Names in the subjectAlternativeName. For each of these certificates, check to see if the certificate subscriber owns/controls that domain name,	Not applicable – see above.

and revoke the certificate if they do not own/control that domain name.	
2. Review your controls/procedures (both internally and your RAs) for correct identification of internal and external domain names and verification that subscribers own/control the domain name to be included in their certificate. Please refer to these documents:	Not applicable – see above.
o Section 7 of Mozilla's CA Certificate Policy	
o Recommended practices for CAs	
Mozilla also recommends that you	
1. Implement automated checks to signal a red flag for domains such as .int and null characters in the Common Name and subjectAlternativeName of certificates.	Not applicable – see above.
2. Maintain your own list of ICANN approved TLDs that are eligible to be used for domains in certificates issued within your CA hierarchy. If a new TLD is created by IANA, make an explicit decision whether or not to add the new TLD to your list.	Not applicable – see above.
OCSP Responses signed by a certificate under a different root	
CAs are not required to use OCSP. However, CAs who issue certificates with OCSP URLs in AIA extensions should make sure that the OCSP responses conform to RFC 2560, and work correctly for Mozilla users without requiring the user to find and install the OCSP responder's certificate, that is, the certificate with which the OCSP response signatures are verified.	Not applicable - AffirmTrust does not presently support OCSP.
At least one CA has issued certificates with OCSP URLs that reference OCSP responders that do not serve queries from the general public, and/or send out responses that are signed with a certificate that is	See above.
not the certificate of the CA that issued the certificate in question; and	
not issued by the CA that issued the certificate in question.	

When an OCSP responder URL is included in end-entity certificates, Firefox 3 will by default attempt to check the certificate's status via OCSP. If the OCSP signer certificate is not the certificate of the CA that issued the certificate in question and is not issued by the CA that issued the certificate in question, the OCSP check will fail with an NSS error code for OCSP, such as SEC_ERROR_OCSP_UNAUTHORIZED_REQUEST or SEC_ERROR_OCSP_UNAUTHORIZED_RESPONSE.	See above.
CRL with critical CIDP Extension	
Currently Firefox handles "full" CRLs, but not "partitioned" CRLs. Partitioned CRLs are identified by the presence of a CRL Issuing Distribution Point (CIDP) extension flagged as critical. Firefox is not presently able to load CRLs with critical CIDP extensions. When attempting to load a CRL with a critical CIDP extension, Firefox will return the error code ffffe095, which is equivalent to the negative decimal number -8043. According to the NSS Error Codes this error corresponds to SEC_ERROR_CRL_UNKNOWN_CRITICAL_EXTENSION.	Not applicable – AffirmTrust issues only full CRLs, not partitioned CRLs.
The NSS team hopes to eventually implement partitioned CRLs, and when that work is done, Firefox should allow CRLs with critical CIDP extensions. However, even when that is done, older versions of Firefox will still not be able to load CRLs with critical CIDP extensions.	See above.
Our recommendation is to not put critical CIDP extensions into full CRLs, and to make full CRLs available for download when practical.	See above.
Generic names for CAs	
In various contexts Firefox and other Mozilla-based products display to users the names of root CAs, issuing CAs, and intermediate CAs in general. In some cases CA names are very generic, e.g., "Secure Server CA"; this makes it difficult for users to ascertain who operates the CA without undertaking a detailed investigation.	AffirmTrust's four root certificates are named AffirmTrust Commercial, AffirmTrust Networking, AffirmTrust Premium, and AffirmTrust Premium ECC. The subroots follow this same naming convention.
Our recommendation is that all CA names incorporate an organizational name or product brand name sufficiently unique to allow relatively straightforward identification of the CA.	AffirmTrust is in compliance – see above.

Lack of Communication With End Users	
CAs should be contactable by, and accept and act upon complaints made by, those relying on their assertions of identity. For CAs included in Mozilla, this will include being responsive to members of the general public, including people who have not purchased products from that CA.	AffirmTrust will respond to all complaints and inquiries, whether from customers or not. See CPS Sec. III.J.
Other considerations when updating the CA Certificate Policy	
Many of the descriptions of the practices above will provide food for thought when and if we are making further updates to the CA Certificate Policy. Other issues which might be considered at that time include:	
Root Count Restrictions	
It has been suggested that, when the CA cert policy is revised, we restrict the number of roots any one CA may have to e.g. 3. This is because more roots increases the download size of the product.	AffirmTrust has requested acceptance of three RSA roots with increasing security levels (RSA 2048 bit/SHA1, RSA 2048 bit/SHA 256, and RSA 4096 bit/SHA 384) and one ECC root (ECC 384 bit/SHA 384 with ECDSA) because AffirmTrust believes there will be a continuing need for greater security and higher strength certs in coming years, but there are still many applications in use that only function with the lower strength certs. AffirmTrust believes that this range of choices will best serve the Mozilla community. In addition, the fourth root (an ECC root) is very compact at 384 bits, so should not add a significant burden to users' downloads.
Restrict government roots to their TLDs	
A suggestion for a future revision of the policy is: we should restrict government run/sponsored roots to only issuing certificates for the corresponding TLD. There are, of course, questions such as:	At present, AffirmTrust does not issue certs to government entities. See CPS Sec. III.B.

What defines a government root What if they have all the necessary audits anyway and so on. These would need to be discussed.	
Minimum Key Sizes	
One suggestion for a future revision of the CA Cert Policy is that we should specify minimum key sizes, either just for roots or for roots, intermediates and end entity certificates.	See discussion at Root Count Restrictions above. AffirmTrust has limited the validity period of its RSA 2048 bit roots in compliance with NIST recommendations.
The exact restrictions would need to be discussed, but doubtless we would take into account the views of our crypto team and advice from places like NIST.	
Max Time Between Audits	
It has been suggested that, when the CA cert policy is revised, we specify the maximum period allowed between audits. WebTrust currently specifies 12 months, and the same is (I understand) recommended for ETSI audits.	AffirmTrust has just successfully completed its WebTrust and EV WebTrust audits. We will comply with all Mozilla requirements re maximum time between audits.
Actual Paperwork	
It has been suggested that CAs should submit some paperwork by postal mail as well as electronically. A formal inclusion request and general details from the CA in question might help Mozilla in the case of legal problems in the future.	AffirmTrust will gladly submit its root program request and other documentation to Mozilla in writing via US mail upon request.
Apparently Apple and Microsoft do require physical paperwork.	
Improve definition of "independent"; add idea of "trustworthy"	
Currently, the guidelines talk about an auditor having to be both "independent" and "competent". It has been suggested that the definition of independent should be changed to be more like that the inverse of the MPL's definition of You:	Not applicable.
"For legal entities, "You" includes any entity which controls, is controlled by,	Not applicable.

or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity."	
Additionally, a new "trustworthiness" requirement would be added, which would address some of the issues currently listed under "independent", such as being bound to render a true judgement. This is because one could imagine an auditor who was (under the above definition) independent and also competent, but may nevertheless always provide "the right result" on payment of a fee.	Not applicable.