Bugzilla ID: 1037590
Bugzilla Summary: Add Renewal IdenTrust root 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	IdenTrust
Website URL	http://www.identrust.com/
Organizational type	Public Corporation
Primark Market / Customer Base	IdenTrust is a for-profit corporation serving the private, commercial, and government sectors.
Impact to Mozilla Users	Renew root certificates that were included via Bug #394733.
Inclusion in other major browsers	The original roots are in all the major browsers.
CA Primary Point of Contact (POC)	Contact #1: Name: Renne Rodriguez CA Email Alias: roots@identrust.com Phone Number: (801) 384-3522 Title / Department: Trust Infrastructure, Product Manager Contact #2: Name: Eric Halbritter CA Email Alias: roots@identrust.com Phone Number: (801) 384-3516 Title / Department: Director, PKI Operations

Technical information about each root certificate

Cert Name	IdenTrust Commercial Root CA 1	IdenTrust Public Sector Root CA 1
Certificate Issuer Field	CN = IdenTrust Commercial Root CA 1 O = IdenTrust C = US	CN = IdenTrust Public Sector Root CA 1 O = IdenTrust C = US
Certificate Summary	This SHA-256 root will replace the SHA-1 "DST Root X3" certificate that was included via Bug #394733. The intent is to issue email and SSL certificates.	This SHA-256 root will replace the SHA-1 "DST ACES X6" certificate that was included via Bug #394733. The intent is to issue email and SSL certificates.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=8473319 http://validation.identrust.com/roots/commercialrootca1.p7c	http://validation.identrust.com/roots/publicrootca1.p7c
SHA1 Fingerprint	DF:71:7E:AA:4A:D9:4E:C9:55:84:99:60:2D:48:DE:5F:BC:F0:3A:25	BA:29:41:60:77:98:3F:F4:F3:EF:F2:31:05:3B:2E:EA:6D:4D:45:FD

Valid From	2014-01-16	2014-01-16
Valid To	2034-01-16	2034-01-16
Certificate Version	3	3
Certificate Signature Algorithm	SHA-256	SHA-256
Signing key parameters	4096	4096
Test Website	https://sha2ssl-trustidvalid.identrustssl.com/ When OCSP hard-fail is set, get error: An error occurred during a connection to sha2ssl-trustidvalid.identrustssl.com. Invalid OCSP signing certificate in OCSP response. (Error code: sec_error_ocsp_invalid_signing_cert) https://wiki.mozilla.org/CA:Recommended_Practices#OCSP For testing of revoked and invalid certificates see: http://testssl.identrust.com/ , where a comprehensive list is available	https://sha2ssl-acesvalid.identrust.com/ For testing of revoked and invalid certificates see: http://testssl.identrust.com/ , where a comprehensive list is available
CRL URL	http://validation.identrust.com/crl/commercialrootca1.crl http://validation.identrust.com/crl/trustidcaa52.crl (CRL NextUpdate: 24 hours) TrustID CPS section 4.9.7: twenty-four hours	http://validation.identrust.com/crl/publicrootca1.crl http://validation.identrust.com/crl/acesca2.crl (CRL NextUpdate: 24 hours) ACES CPS section 4.4.5.1: 18 to 24 hours
OCSP URL	http://commercial.ocsp.identrust.com	http://public.ocsp.identrust.com
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	Organization Validated	Organization Validated
EV Policy OID(s)	Not applicable. Not requesting EV treatment at this time.	Not applicable. Not requesting EV treatment at this time.
Non-sequential serial numbers and entropy in cert	IdenTrust issues certificate with non-sequential serial numbers with 20 bits of entropy. TrustID CPS Section 7.1.3: For all Certificates, IdenTrust generates a non-sequential serial number that exhibits at least 20 bits of entropy.	IdenTrust issues certificate with non-sequential serial numbers with 20 bits of entropy. ACES CPS Addendum Section 7.1: For all Certificates, IdenTrust generates a non-sequential serial number that exhibits at least 20 bits of entropy.

CA Hierarchy information for each root certificate

Root Cert	IdenTrust Commercial Root CA 1	IdenTrust Public Sector Root CA 1
CA Hierarchy	The intent is to generate the subordinate CA Certificates that will support our current lines of business under the root being replaced. At this time not all of the subordinate CA certificates have been generated (names may change) – [Internal]TrustID CA A52 (s/mime certificates) – [Internal]TrustID CA A12 (Device/SSL Certificates)	At the time of generation of this document, the intent is to generate the following subordinate under this root: – [Internal]IdenTrust ACES CA 2 (s/mime, device/SSL certificates)
Externally Operated SubCAs	No externally operated subordinate CA has been issued off this root at this time. In the future, there is the possibility of issuance of externally operated CAs under this root. In such case, IdenTrust will favor the independently audited and publicly disclose subordinate CA model of operation. Are there any externally-operated subordinate CAs that have been signed by the "DST Root X3" root?	There are no plans to have externally operated subordinate CAs off this root at this time Are there any externally-operated subordinate CAs that have been signed by the "DST ACES X6" root?
Cross-Signing	This root is not cross-certified	This root is not cross-certified
Technical Constraints on Third-party Issuers	There are no third-party issuers for this root. Are there any third-party issuers (e.g. RAs) that can cause the issuance of certs in the CA hierarchy of the "DST Root X3" root? Who is the TrustID CP intended for? TrustID CP section 4.2, Certificate Application Validaiton: No Stipulation. TrustID CPS section 1.3.3: IdenTrust may subcontract registration and I&A functions to an Organization that agrees to fulfill the functions of an RA IdenTrust validates Domains for SSL certificates issued and does not delegate such validation. TrustID CPS section 3.2.7.2: IdenTrust verifies that the PKI Sponsor has the right to use or has control of the FQDN (s) or IP address(es) listed in the Certificate application Email certificates: IdenTrust allows Trusted Agents to, in particular cases, manually validate the email of certificates. Trusted Agents are employees of the organizations requesting the certificate and are under	There are no third-party issuers for this root. Are there any third-party issuers (e.g. RAs) that can cause the issuance of certs in the CA hierarchy of the "DST ACES X6" root? IdenTrust validates Domains for SSL certificates issued and does not delegate such validation. See TrustID CPS section 3.2.7.2 and ACES CPS Addendum 3.1.9.4.

	agreement with IdenTrust. Trusted Agents validation is limited to emails within their organization and only in circumstances where automatic validation is not possible. See TrustID CPS section 3.2.5 and ACES CPS Addendum section 3.1.9.7 for detail.	

Verification Policies and Practices

Root Cert	IdenTrust Commercial Root CA 1	IdenTrust Public Sector Root CA 1
Policy Documentation	Documents are in English. TrustID Document Repository: https://secure.identrust.com/certificates/policy/ts/ TrustID CPS: https://secure.identrust.com/certificates/policy/ts/identrust_trustid_cps_v2.3_20140109.pdf TrustID CP: https://secure.identrust.com/certificates/policy/ts/TrustID_CP_v1.6.1_20130912.pdf	Documents are in English. ACES Document Repository: https://secure.identrust.com/certificates/policy/aces/ ACES CPS: https://secure.identrust.com/certificates/policy/aces/dst-aces-cps-v20040617.pdf ACES CPS Addendum: https://secure.identrust.com/certificates/policy/aces/IdenTrust-Addendum-2013-11-26.pdf
Audits	Auditor: Ernst & Young Audit Type: WebTrust CA 2.0 Audit Report: (2013.07.16) https://cert.webtrust.org/SealFile?seal=1552&file=pdf Audit Type: WebTrust Baseline Requirements BR Audit Report: (2013.09.30) https://secure.identrust.com/certificates/policy/ts/baseline-requirements-audit-2012.pdf	Auditor: Ernst & Young Audit Type: WebTrust CA 2.0 Audit Report: (2013.07.16) https://cert.webtrust.org/SealFile?seal=1552&file=pdf Audit Type: WebTrust Baseline Requirements BR Audit Report: (2013.09.30) https://secure.identrust.com/certificates/policy/ts/baseline-requirements-audit-2012.pdf
Baseline Requirements (SSL)	TrustID CP section 3.1.8: When issuing this type of Certificate, the Issuing CA shall conform to "the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" available in appendix A and published at http://www.cabforum.org. In the event of any inconsistency between this CP and those requirements set forth in appendix A take precedence over this document.	ACES CPS Addendum section 1.1: This CPS also includes practices satisfying requirements prescribed in the CA/Browser Forum document named Baseline Requirements for the Issuance and management of Publicly-Trusted Certificates ("CA/B Forum Baseline Requirements"), which has industry-wide acceptance and has been adopted by browsers as part of the pre-requisites to include a Root CA Certificate in their crypto stores.
Organization Verification Procedures	Trust ID CPS section 3.2.2.1, Verification of Sponsoring Organization Legal Existence TrustID CPS section 3.2.2.2, Authentication of the Individual-Organization Affiliation	ACES CPS Addendum section 3.1.8: Authentication of Sponsoring Organization Identity
SSL Verification Procedures	TrustID CPS section 3.2.7.1: To ensure that requests for TrustID SSL Certificates are properly verified, IdenTrust and RAs conduct two additional checks when necessary: (1) IdenTrust and RAs maintain internal lists of prior denied	ACES CPS Addendum section 3.1.9.4: Verification of Authorization by Domain Name Registrant IdenTrust verifies that the PKI Sponsor has the right to issue or has control of the Fully-Qualified Domain Name(s) from the SAN

	applications identified as posing a risk; and (2) IdenTrust and RAs will check high risk domain requests against an authoritative third party list prior to issuance. Information returned from such checks is used during the application process by an LRA within IdenTrust or an RA when identifying potentially illegitimate Certificate requests. If an RA is elected to perform verification processes, IdenTrust will verify that the RA's processes used to identify high risk domain requests and prior denied requests provide a level of assurance that is equal to or exceeds the same level of assurance provided by the process described below. TrustID CPS section 3.2.7.2: IdenTrust verifies that the PKI Sponsor has the right to use or has control of the FQDN(s) or IP address(es) listed in the Certificate application by following the steps listed below. The LRA confirms the Domain registrant's rights by doing the following: 1) The Domain(s) supplied by the PKI Sponsor is placed into a search engine (e.g. WHOIS) and the LRA records the contact information for the Domain Name Registrant. 2) Once the Domain Name registrant is identified from a database record he or she is contacted via email. In this email the Domain Name registrant will be asked: a. to confirm or deny the right of the PKI Sponsor to be issued a Device Certificate for the Domain Name(s) for which the PKI Sponsor has applied; b. if they would like to provide the names other potential PKI Sponsor(s) that may request the same type of Certificate; and c. with respect only to applications for Wildcard Certificates, to confirm or deny control over the entire Domain Namespace of the FQDN provided and that such control is rightful. If the PKI Sponsor applies for a Domain Name that contains a two-letter country code (ccTLD) (e.g. www.identrust.uk as opposed to www.identrust.com), this confirmation will be sought from the Domain Name level to which the ccTLD applies. This means that the LRA cannot obtain verification from www.identrust.com if the PKI Sponsor is applying for a Domain Name from www.identrust.uk.	extension and public IP address(es) listed in the Certificate application by following the steps listed below. The LRA confirms the rights by the Domain Registrant by doing the following: (1)The domain(s) supplied by the PKI Sponsor is placed into a search engine (e.g. WHOIS) and the LRA records the contact information for the Domain Name Registrant. (2) Once the Domain Name Registrant is identified from a database record he or she are contacted via email to confirm the information provided by the PKI Sponsor to confirm or deny the right of the PKI Sponsor to be issued the certificate for the Domain Name(s) for which the PKI Sponsor has applied. It is through this process that IdenTrust ensures that SSL Certificates are issued with the consent of the owner of each FQDN contained within the Certificate.During this exchange the Domain Name Registrant will have the opportunity to name other potential PKI Sponsor(s). If the PKI Sponsor applies for a domain that is a two-letter country code (ccTLD), this confirmation will be sought from the Domain Name level to which the ccTLD applies.
Email Address Verification	Trust ID CPS section 3.2.5: Email verification when required can be done in two ways;	ACES Addendum section 3.1.9.7 Email verification when required can be done in two ways;

Procedures	electronically and manually through a list submitted by a Trusted Agent. If the application for a Certificate requires email verification the application cannot be approved until the specified steps for electronic or manual verification is complete. - Electronic Verification of Email: When an Applicant/PKI Sponsor submits an application through a secure online form, an automated email is sent to the personal email address provided in the application. Within that automated email message there is a link that guides the Applicant/PKI Sponsor to a server-authenticated SSL/TLS secured web site and instructions to provide out-of-band information, including an Account Password. This Account Password was created during the application by the Applicant/PKI Sponsor and it is secure only to the Applicant/PKI Sponsor. When the Applicant/PKI Sponsor provides and submits the Account Password created during the application accurately the verification of the email address is completed and the verification status is automatically updated within the Applicant/PKI Sponsor's application record. - Manual Verification of Email: When a Trusted Agent provides the list of authorized Applicants/PKI Sponsors, the email address is validated by the Trusted Agent based on the internal knowledge of the Sponsoring Organization. The Trusted Agent may use internal databases and directories to ensure the email accuracy.	electronically and manually through a list submitted by a Trusted Agent. If the application for a Certificate requires email verification the application cannot be approved until the specified steps for electronic or manual of verification is complete. Electronic Verification of Email: When an Applicant/PKI Sponsor submits an application through a secure online form, an automated email is sent to the Applicant/PKI Sponsor's email address provided in the application. Within that automated email message there is a link that guides the Applicant/PKI Sponsor to a server-authenticated SSL/TLS secured web site and instructions to provide out-of-band information, including in Account passphrase Password. This Account Password was created during the application by the Applicant/PKI Sponsor and it is secure only to the Applicant/PKI Sponsor. When the Applicant/PKI Sponsor provides and submits the passphrase Account Password created during the application accurately the verification of the email address is completed and the verification status is automatically updated within the Applicant/PKI Sponsor's application record. Manual Verification of Email: When a Trusted Agent provides the list of authorized Applicants/PKI Sponsors, the email address is validated by the Trusted Agent based on the internal knowledge of the Sponsoring Organization. The Trusted Agent may use internal databases and directories to ensure the email accuracy.
Code Signing Subscriber Verification Procedures	Not applicable. Not requesting the code signing trust bit.	Not applicable. Not requesting the code signing trust bit.
Multi-factor Authentication	*The answers below apply to the controls for both roots whose inclusion is being requested.* • For each account that can access the certificate issuance system, do you have the log-in procedure require something in addition to username/password? o *Yes. Two-factor authentication based on digital-certificate-based access and access control lists (ACLs) are used to access the system capable of issuing a certificate.* • Specify the form factor that you use. – o *For humans approving certificates: Hardware tokens; FIPS 140-1/2 Level 2-validated hardware.* o *For automated RA: Hardware or software cryptomodules* • This must apply to all accounts that can cause the approval and/or issuance of end-entity certificates, including your RAs and sub-CAs, unless there are technical controls that are implemented and controlled by the CA to restrict certificate issuance	

	through the account to a limited set of pre-approved domains or email addresses. – ○ *Confirmed; All RAs are required to use digital certificates and be in the ACL.* • If technical controls are used instead of multi-factor auth for any accounts, then specify what those technical controls are: ○ *Multi-factor authentication based on certificates is used.*	
Network Security	Commercial Root CA • Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements. ○ *TrustID CPS section 6.7 NETWORK SECURITY CONTROLS* • Check for miss-issuance of certificates, especially for high-profile domains. – ○ *TrustID CPS Sections 8 COMPLIANCE AUDITS AND OTHER ASSESSMENTS and 8.5.1 Actions Taken as a Result of Internal Audit Deficiency.* • Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. – ○ *TrustID CPS sections 6.6.2 Security Management Controls and 6.7 NETWORK SECURITY CONTROLS.* • Ensure Intrusion Detection System and other monitoring software is up-to-date. – ○ *TrustID CPS sections 6.6.2 Security Management Controls and 6.7 NETWORK SECURITY CONTROLS.* • Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion. – ○ *IdenTrust has security incident response and compromise handling policies and procedures (See TrustID CPS Section 5.7.1) that include disabling issuance functionality in a timely manner if the severity of the threat requires it.*	Public Root CA • Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements. – ○ *ACES CPS section 6.7 NETWORK SECURITY CONTROLS* • Check for mis-issuance of certificates, especially for high-profile domains. – ○ *ACES CPS Addendum Section 6.5.1.1 - Internal Audits.* • Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. – ○ *ACES CPS section 6.7 NETWORK SECURITY CONTROLS* • Ensure Intrusion Detection System and other monitoring software is up-to-date. – ○ *ACES CPS section 6.7 NETWORK SECURITY CONTROLS* • Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion. ○ *IdenTrust has security incident response and compromise handling policies and procedures (See TrustID CPS Section 5.7.1) that include disabling issuance functionality in a timely manner if the severity of the threat requires it.*

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	Yes. See above.
Document Handling of IDNs in CP/CPS	Yes. TrustID CPS: 3.2.7.1 Verification against High Risk and Denied Request Lists ACES Master Addendum: Section 3.1.9.4 – Authentication of Component Identity

Revocation of Compromised Certificates	Yes TrustID CPS: 4.9 CERTIFICATE REVOCATION AND SUSPENSION ACES CPS: 4.4 CERTIFICATE REVOCATION
Verifying Domain Name Ownership	Yes. See above.
Verifying Email Address Control	Yes. See above.
Verifying Identity of Code Signing Certificate Subscriber	Not applicable.
DNS names go in SAN	DNS names are included in the SAN extension. The name included in the CN is replicated in the SAN.
Domain owned by a Natural Person	IdenTrust issues SSL certificates only to organizations. The existence of the organization is validated. For Commercial root see TrustID CPS section 3.2, the table that establishes what is validated and sections 3.2.2 and 3.2.2.1, and ACES CPS Addendum 3.1.8.
OCSP	Yes. See above.

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

Long-lived DV certificates	Currently, IdenTrust does not issue Domain Validated certificates. If, in the future, DV certificates are issued, they will comply with current policy that limits certificates to 39 months.
Wildcard DV SSL certificates	TrustID CPS section 3.1.2: The entire Domain Namespace in Wildcard Certificates must be rightfully controlled by the Subscriber Organization. Currently, IdenTrust does not issue Domain Validated certificates. Wildcard SSL Certificates for the commercial root are OV.
Email Address Prefixes for DV Certs	Currently, IdenTrust does not issue Domain Validated certificates therefore this practice is not implemented.
Delegation of Domain / Email validation to third parties	IdenTrust validates Domains for SSL certificates issued and does not delegate such validation. See TrustID CPS section 3.2.7.2 and ACES CPS Addendum 3.1.9.4. IdenTrust allows Trusted Agents to, in particular cases, manually validate the email of certificates. Trusted Agents are employees of the organizations requesting the certificate and are under agreement with IdenTrust. Trusted Agents validation is limited to emails within their organization and only in circumstances where automatic validation is not possible. See TrustID CPS section 3.2.5 and ACES CPS Addendum section 3.1.9.7 for detail.
Issuing end entity certificates directly from roots	IdenTrust does not issue end entity certificates directly from roots.
Allowing external entities to operate subordinate CAs	Commercial Root CA: Not at this time. There is a possibility of externally operated subordinate CAs. In such case, IdenTrust will favor the externally audited and publicly disclose model of operation. Public Root CA: No
Distributing generated private keys in	IdenTrust does not generate private keys for SSL certificates

PKCS#12 files	For email certificates that are used only for encryption and whose key is escrowed, IdenTrust may generate the private key and deliver in a PKCS#12. See TrustID CPS section 6.1.1.3 and ACES CPS Addendum section 4.2.1.
Certificates referencing hostnames or private IP addresses	Practice is Prohibited: TrustID CPS: 3.2.7.3 Verification of DBA or Tradename: "…IdenTrust does not and will not issue SSL Certificates to reserved IP addresses or internal server names. " ACES Master Addendum: 1.3.2.3.1 – Agency and Relying Party Application SSL Server Certificates: "…IdenTrust does not and will not issue SSL Certificates to reserved IP addresses or internal server names. "
Issuing SSL Certificates for Internal Domains	Same answer as above – practice is prohibited.
OCSP Responses signed by a certificate under a different root	IdenTrust signs responses with a certificate issued under the same CA that issued the certificate being validated.
CRL with critical CIDP Extension	No
Generic names for CAs	No
Lack of Communication With End Users	No. IdenTrust has an active customer support team that answers questions through email and telephone for both customers and other members of the public should they have questions. Contact information is available 24/7 on the IdenTrust website located here: http://www.identrust.com/contact_us.html