Bugzilla ID: 873118
Bugzilla Summary: Enable email trust bits for "DST Root X3" and "DST ACES X6"

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.
CA Contact Information	CA Email Alias: CA Phone Number: Title / Department:

Technical information about each root certificate

Certificate Name	DST Root CA X3	DST ACES CA X6

Certificate Issuer Field	CN = DST Root CA X3
	O = Digital Signature Trust Co.
		CN = DST ACES CA X6
		OU = DST ACES
		O = Digital Signature Trust
		C = US

Certificate Summary	The request is to enable the email trust bit for this root cert that was included via Bugzilla Bug# 359069.	The request is to enable the email trust bit for this root cert that was included via Bugzilla Bug# 359069.
Root Cert URL	Already included	Already included
SHA1 Fingerprint	DA:C9:02:4F:54:D8:F6:DF:94:93:5F:B1:73:26:38:CA:6A:D7:7C:13	40:54:DA:6F:1C:3F:40:74:AC:ED:0F:EC:CD:DB:79:D1:53:FB:90:1D
Valid From	2000-09-30	2003-11-20
Valid To	2021-09-30	2017-11-20 – expiry coming up. Need renewed cert soon.
Cert Version	3	3
Cert Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption	PKCS #1 SHA-1 With RSA Encryption
Signing key parameters	2048	2048
Test Website	https://www.identrustssl.com/	https://sslacesvalid.identrust.com/
CRL URL	http://crl.identrust.com/DSTROOTCAX3.crl http://crl.identrust.com/trustid/trustidcaa51.crl	http://crl.identrust.com/publicsectorroot1.crl http://crl.identrust.com/acespublicsector1.crl

	(NextUpdate: 24 hours) TrustID CPS section 4.9.7: twenty-four hours	(NextUpdate: 24 hours) ACES CPS section 4.4.5.1: 18 to 24 hours
OCSP URL	http://ocsp.identrust.com http://ocsp.identrust.com	https://publicsector.ocsp.identrust.com http://aces.ocsp.identrust.com
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) – this request	Websites (SSL/TLS) Email (S/MIME) – this request
SSL Validation Type	OV	OV
EV Policy OID	Not applicable. Not requesting EV treatment.	Not applicable. Not requesting EV treatment.
Non-sequential serial numbers and entropy in cert	Confirm that new cert issuance has sufficient entropy… 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	List, description, and/or diagram of all intermediate CAs signed by this root. Identify which subCAs are internally-operated and which are externally operated.	List, description, and/or diagram of all intermediate CAs signed by this root. Identify which subCAs are internally-operated and which are externally operated.
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.
Cross-Signing	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate. If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate. If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	Documents are in English. TrustID Document Repository: https://secure.identrust.com/certificates/policy/ts/ ACES Document Repository: https://secure.identrust.com/certificates/policy/aces/ TrustID CPS: https://secure.identrust.com/certificates/policy/ts/identrust_trustid_cps_v2.1_20121218.pdf For "DST Root CA X3". 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-aces-cps-addendum-ssl-v20121218.pdf For "DST ACES CA X6".
Audits	Audit Type: WebTrust CA Auditor: Ernst & Young Audit Report: https://cert.webtrust.org/SealFile?seal=1360&file=pdf (2012.07.20)
Baseline Requirements	ACES CPS Addendum 2012.12.18 Not found in TrustID CPS. (see Baseline Requirement #8.3) – The websites trust bit is enabled for this root, so need compliance with BRs. ACS CPS 2012 Addendum includes updates for the Baseline Requirements.
Organization Verification Procedures	Trust ID CPS section 3.2: Initial Identity Validation (Note: RAs and LRAs) For server certificates organizational verification is required as per section 3.2.2. ACES CPS Addendum section 3.1.8: Authentication of Sponsoring Organization Identity
SSL Verification Procedures	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) orIP 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 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. The Domain Name registrant will also be asked if they would like to provide the names other potential PKI Sponsor(s) that may request the same type of Certificate. 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. 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 extension and 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. 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 Procedures	Trust ID CPS section 3.2.5: Email verification when required can be done in two ways; 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. For the ACES root (ACES CPS and ACES CPS addendum) I did not find how the email address to be included in the certificate is verified to be owned/controlled by the certificate subscriber. If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Code Signing Subscriber Verification Procedures	Not applicable. Not requesting the code signing trust bit.
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices TrustID CPS section 5 and 6.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes. See above.
CA Hierarchy	?
Audit Criteria	Yes. See above.

Document Handling of IDNs in CP/CPS	?
Revocation of Compromised Certificates	?
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	?
Domain owned by a Natural Person	?
OCSP	Yes

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

Long-lived DV certificates	SSL certs are OV
Wildcard DV SSL certificates	SSL certs are OV Are wildcard certs allowed?
Email Address Prefixes for DV Certs	SSL certs are OV
Delegation of Domain / Email validation to third parties	? Are LRA's third parties?
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	?
Distributing generated private keys in PKCS#12 files	Not for SSL certs, Correct? TrustID CPS section 3.2.1: In the case where Key generation is performed by IdenTrust or an RA either (1) directly on the Certificate Holder's hardware or software Cryptomodule, or (2) in a Key generator that benignly transfers the Key to the party's Cryptomodule, then proof of possession is not required. If the End Entity is not in possession of the Token when the Key is generated, then the Token will be delivered immediately to the End Entity via a trustworthy and accountable method.
Certificates referencing hostnames or private IP addresses	?
Issuing SSL Certificates for Internal Domains	?
OCSP Responses signed by a certificate under a different root	No
CRL with critical CIDP Extension	No. CRLs import without error into Firefox.
Generic names for CAs	Cert Subject contains DST and Digital Signature Trust http://www.identrust.com/company/company_profile.html "In March 2002, IdenTrust acquired Digital Signature Trust Company (DST)…"
Lack of Communication With End Users	