Print this page

Mozilla - CA Program

Case Information

Case Number	00000100	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	IdenTrust Services, LLC	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Enable EV for IdenTrust Commercial Root CA 1	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1339292

General information about CA's associated organization

CA Email Alias 1	roots@identrust.com		
CA Email Alias 2	reportproblem@identrust.com		
Company Website	https://www.identrust.com/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	USA	**Verified?**	Verified
Primary Market / Customer Base	IdenTrust is a for-profit corporation serving the private, commercial, and government sectors.	**Verified?**	Verified
Impact to Mozilla Users		**Verified?**	Not Applicable

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text

			box below.
CA's Response to Recommended Practices	1. Publicly Available CP and CPS: Yes 2. Audit Criteria: Yes 3. Revocation of Compromised Certificates: CPS section 4.9.1.2 4. Verifying Domain Name Ownership: CPS section 3.2.7.5 5. Verifying Email Address Control: CPS section 3.2.7.1 6. DNS names go in SAN: CPS section 7.1.9.5 7. OCSP: CPS section 4.9.9 8. Network Security Controls: CPS section 6.7	**Verified?**	Verified

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	1. Long-lived Certificates: CPS section 6.3.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CPS section 3.2.7.5 3. Issuing End Entity Certificates Directly From Roots: No 4. Distributing Generated Private Keys in PKCS#12 Files: CPS section 3.2.1 5. Certificates Referencing Local Names or Private IP Addresses: CPS section 3.2.7.6 6. Issuing SSL Certificates for .int Domains: CPS section 3.2.7.6 7. OCSP Responses Signed by a Certificate Under a Different Root: No 8. Issuance of SHA-1 Certificates: CPS section 6.1.2 9. Delegation of Domain / Email Validation to Third Parties: CPS section 3.2.7.5	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	IdenTrust Commercial Root CA 1	**Root Case No**	R00000418
Request Status	Information Verification In Process	**Case Number**	00000100

Certificate Data

Certificate Issuer Common Name	IdenTrust Commercial Root CA 1
O From Issuer Field	IdenTrust
OU From Issuer Field	
Valid From	2014 Jan 16
Valid To	2034 Jan 16
Certificate Serial Number	0a0142800000014523c844b500000002
Subject	CN=IdenTrust Commercial Root CA 1, OU=null, O=IdenTrust, C=US
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	DF:71:7E:AA:4A:D9:4E:C9:55:84:99:60:2D:48:DE:5F:BC:F0:3A:25
SHA-256 Fingerprint	5D:56:49:9B:E4:D2:E0:8B:CF:CA:D0:8A:3E:38:72:3D:50:50:3B:DE:70:69:48:E4:2F:55:60:30:19:E5:28:AE
Certificate ID	89:B8:F1:17:18:82:FB:89:B2:3E:87:79:EA:C2:18:69:AC:06:C6:21:83:61:9A:22:34:0A:C1:4D:8B:E5:8E:EB
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	Enable EV treatment for the "IdenTrust Commercial Root CA 1" root certificate that was included via Bugzilla Bug #1037590.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8473319	**Verified?**	Verified
CRL URL(s)	http://validation.identrust.com/trustidcaa52.crl	**Verified?**	Verified
OCSP URL(s)	http://commercial.ocsp.identrust.com/	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified

Mozilla EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In	Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://ev-valid.identrustssl.com/	**Verified?**	Verified
Test Website - Expired	https://ev-expired.identrustssl.com/		
Test Website - Revoked	https://ev-revoked.identrustssl.com/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/ev-valid.identrustssl.com OK	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=1587&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01 OK	**Verified?**	Verified
Test Website Lint Test	See above	**Verified?**	Verified
EV Tested	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	NEED Identrust to explain their current CA hierarchy and audits. The record for the "Booz Allen Hamilton BA CA 01" intermediate cert says "Audits Same as Parent". It is not clear if this intermediate cert is internally-operated by IdentTrust, or if it is operated by BAH. Future audit statements must include the SHA-256 fingergerpritns of all root and	**Verified?**	Need Response From CA

	intermediate certs that were in scope of the audit. https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy#public-audit-information		
Externally Operated SubCAs	NEED Identrust to explain the discrepancy between their BR Self Assessment and their CP/CPS: Cross-certification with other, external CAs is allowed, per CP section 1.3.4. However, BR Self Assessment says: "There are no cross-certified entities for the TrustID program, therefore this requirement is not applicable."	**Verified?**	Need Response From CA
Cross Signing	NEED Identrust to explain the discrepancy between their BR Self Assessment and their CP/CPS: Cross-certification with other, external CAs is allowed, per CP section 1.3.4. However, BR Self Assessment says: "There are no cross-certified entities for the TrustID program, therefore this requirement is not applicable."	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED Identrust to explain the discrepancy between their BR Self Assessment and their CP/CPS: External RAs are allowed per CPS sections 1.3.3, 5.2.4; and CP sections 1.3.1.3, 2.1.3, 2.7.4, However, in the BR Self Assessment Identrust said: "IdenTrust does not allow for Delegated Third Parties".	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	Documents are in English.	**Verified?**	Verified
CA Document Repository	https://secure.identrust.com/certificates/policy/ts/	**Verified?**	Verified
CP Doc Language	English		
CP	https://secure.identrust.com/certificates/policy/ts/IdenTrust_TrustID_CP_v2.4_20180130.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://secure.identrust.com/certificates/policy/ts/IdenTrust_TrustID_CPS_v3.5_20180130.pdf	**Verified?**	Verified

Other Relevant Documents	See Agreements section of https://secure.identrust.com/certificates/policy/ts/	**Verified?**	Verified
Auditor (New)	Schellman & Company, Inc.	**Verified?**	Verified
Auditor Location (New)	United States	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2331&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	8/31/2017	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2334&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	9/18/2017	**Verified?**	Verified
EV SSL Audit	https://cert.webtrust.org/SealFile?seal=2335&file=pdf	**Verified?**	Verified
EV SSL Audit Type	WebTrust	**Verified?**	Verified
EV SSL Audit Statement Date	10/17/2017	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8948390	**Verified?**	Verified
SSL Verification Procedures	CPS sections 3.2.4, 3.2.7.5, 3.2.7.9	**Verified?**	Verified
EV SSL Verification Procedures	CPS seciton 3.2.7 and CP Annex B	**Verified?**	Verified
Organization Verification Procedures	CPS sections 3.2, 3.2.2, 3.2.3, 3.2.6,	**Verified?**	Verified
Email Address Verification Procedures	CPS sections 1.3.3.1, 3.2.5, 3.2.7	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS section 6.5.1	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified