Print this page

Mozilla - CA Program

Case Information

Case Number	00000074	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	TrustCor Systems	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Include TrustCor Root Certificates	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1231853

General information about CA's associated organization

CA Email Alias 1	registrar@trustcor.ca		
CA Email Alias 2			
Company Website	http://www.trustcorsystems.com	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Canada, Global	**Verified?**	Verified
Primary Market / Customer Base	TrustCor develops privacy protection services and issues certificates to its customers in support of such services.	**Verified?**	Verified
Impact to Mozilla Users	Firefox and Thunderbird users may encounter SSL certs that chain up to some of these roots.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_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	* CA Hierarchy: https://www.trustcorsystems.com/resources * Document Handling of IDNs in CP/CPS: At the current time, TrustCor only issues domain name certificates whose character set is representable within US--ASCII. * Revocation of Compromised Certificates: CPS Section 4.9 * Verifying Domain Name Ownership: CPS Section 3.2.2.1 * Verifying Email Address Control: CPS Section 3.2.2.1 * DNS names go in SAN: All DNS names which form part of the CN are stored as dnsNames in the SAN section as well. * Domain owned by a Natural Person: TrustCor does not issue DV SSL certificates	**Verified?**	Verified

to natural persons, only domain names. OV SSL certificates are issued only to registered bodies, not natural persons, and the CN is set to a DNS name. S/MIME "DV" certificates are issued to email addresses, and OV S/MIME certificates are issued to email addresses for which we have evidence that the controller of the email address is authorized to assert the organizational information present in the certificate.
* OCSP: The status of any certificate issued by TrustCor is discoverable via OCSP. OCSP revocation information is updated at least every day, and OCSP responses are valid for no more than 4 days.

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_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	*Long-lived DV certificates: DV certificates issued by TrustCor have a maximum validity period of 12 months. * Wildcard DV SSL certificates: CPS section 3.2.2.6, TrustCor does not issue wildcard DV certificates. * Email Address Prefixes for DV Certs: CPS Section 3.2.2.1 -- "admin", "administrator", "hostmaster", "postmaster" and "webmaster". * Delegation of Domain / Email validation to third parties: TrustCor validates domain and email addresses in house. No external RA functions are used. * Issuing end entity certificates directly from roots: TrustCor does not issue end--entity certificates from its root, only subordinate CAs. * Allowing external entities to operate subordinate CAs: TrustCor has a subordinate CA/RA capability which can only issue technically constrained certificates. No external entity to TrustCor can issue arbitrarily named certificates chaining to TrustCor's Root CA certificates. * Distributing generated private keys in PKCS#12 files: TrustCor does not generate private keys for its customers. * Certificates referencing hostnames or private IP addresses: TrustCor does not issue certificates containing IP spaces at all. All DNS names embedded in issued certificates must be subordinate to domains which chain to entities on the public suffix list. * Issuing SSL Certificates for Internal Domains: TrustCor does not treat '.int' as signifying a private domain. All DNS names in issued certificates must be contained within the https://www.publicsuffix.org/list/ list. * OCSP Responses signed by a certificate under a different root: TrustCor does not sign OCSP responses under a different root. * CRL with critical CIDP Extension: TrustCor issues only "full" CRLs. * SHA--1 Certificates: TrustCor does not issue, and never has issued, certificates using SHA--1 as a digest algorithm. * Generic names for CAs: TrustCor embeds its company name into the CN of all issuing certificates issued and does not use generic names. * Lack of Communication With End Users: TrustCor maintains (24x7) a helpdesk ticketing service on https://support.trustcor.ca which escalates tickets to senior management which have not elicited a response hitherto. The escalation time depends on ticket severity but is at least 4 days. Critical tickets must be picked up and responded to within 2 hours. Tickets can be submitted via a portal, emails to support@trustcor.ca . TrustCor publishes phone numbers which can be used to generate support tickets by the appropriate TrustCor personnel. Backdating the notBefore date TrustCor does not issue backdated certificates to subscribers for any reason.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	TrustCor RootCert CA-1	**Root Case No**	R00000101

Request Status	Ready for Public Discussion	**Case Number**	00000074

Certificate Data

Certificate Issuer Common Name	TrustCor RootCert CA-1
O From Issuer Field	TrustCor Systems S. de R.L.
OU From Issuer Field	TrustCor Certificate Authority
Valid From	2016 Feb 04
Valid To	2029 Dec 31
Certificate Serial Number	00da9bec71f303b019
Subject	CN=TrustCor RootCert CA-1, OU=TrustCor Certificate Authority, O=TrustCor Systems S. de R.L., C=PA
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	FF:BD:CD:E7:82:C8:43:5E:3C:6F:26:86:5C:CA:A8:3A:45:5B:C3:0A
SHA-256 Fingerprint	D4:0E:9C:86:CD:8F:E4:68:C1:77:69:59:F4:9E:A7:74:FA:54:86:84:B6:C4:06:F3:90:92:61:F4:DC:E2:57:5C
Certificate Fingerprint	EB:38:B7:02:A2:D8:DD:36:CC:C9:9E:8A:51:33:84:F9:C4:C1:04:E2:AE:CC:E7:71:75:7E:10:38:B0:24:76:CE
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root issues internally-operated SubCAs which issue SSL and S/MIME certificates.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8716896	**Verified?**	Verified
CRL URL(s)	http://crl.trustcor.ca/ http://crl.trustcor.ca/root/ca1.crl http://crl.trustcor.ca/sub/ca1-site.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.trustcor.ca/root/ca1 http://ocsp.trustcor.ca/sub/ca1-site Maximum expiration time of OCSP responses: 4 days	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://catest1.trustcor.ca/	**Verified?**	Verified
Test Website - Expired	https://catest1-expired.trustcor.ca/		
Test Website - Revoked	https://catest1-revoked.trustcor.ca/		

Example Cert	
Test Notes	

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

Revocation Tested	https://certificate.revocationcheck.com/catest1.trustcor.ca no errors	**Verified?**	Verified
CA/Browser Forum Lint Test	No errors (cert not found by CT)	**Verified?**	Verified
Test Website Lint Test	Tested. No Errors.	**Verified?**	Verified
EV Tested	Not requesting EV treatment for this root	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	This root issues internally-operated SubCAs which issues SSL and S/MIME certificates. CPS section 1.3.1: The Basic Root Certificate (CA-1) - used to ultimately be the root of trust for all certificates issued under the Basic Assurance programme. This certificate currently signs the subordinate CAs: - Basic Secure Email CA (Subordinate CA1-Email) - Basic Secure Site CA (Subordinate CA1-Site) - Basic Secure Site CA [Restricted Key Size] (Subordinate CA1-Site-2048)	**Verified?**	Verified
Externally Operated SubCAs	This root does not and will not have any subCAs that are operated by external third parties.	**Verified?**	Verified
Cross Signing	None. None planned	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No third parties can issue certificates signed by this root. The Enterprise Root Certificate (ECA-1) is the only root allowed to issue externally-operated subCAs. CPS section 1.3.2: External RAs are not entitled to perform general domain or organizational validation; they are strictly limited to registration for credentials to domains and principals assigned to their specific organization.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English	**Verified?**	Verified
CA Document Repository	https://www.trustcorsystems.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.trustcorsystems.com/static/webtrust/cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.trustcorsystems.com/static/webtrust/cps.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	Princeton Audit Group (PAG)	**Verified?**	Verified

Auditor Website	http://princetonauditgroup.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2169&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	12/15/2016	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2163&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	12/15/2016	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8860163	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.1: For Basic Secure Site certificates, any of the following methods may be used to establish authority to use the domain name requested: 1. Check that the relevant domain name registrar via WHOIS and validate that the name on the certificate matches that of the requestor. 2. Using the registrar supplied details, communicate with the registrant using email, telephone or postal mail to ensure that the request was genuine. ... 3. Failing the above, send an email to the well known administrative email addresses for a domain, pruning such components from the FQDN until a registered domain is reached. The administrative mailboxes will be “admin”, “administrator”, “hostmaster”, “postmaster” and “webmaster”. ... 4. Asking of the Applicant that a website page, hosted at FQDN requested contain a base64 randomly generated 128 bit request token (supplied by TrustCor CA) ... If the request token can be fetched from the URI, practical web site control is deemed to have been demonstrated. TrustCor CA must be able to fetch that request token within 7 days from its generation and communication to the Applicant. 5. Asking of the Applicant that a DNS change for the zone containing the FQDN contains a new record (usually of type TXT) is published, whose record set contains a base64 encoded 128 bit request token generated by TrustCor CA with the text “trustcorca-“ prepended. ...	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	Only DV certificates issued in this CA hierarchy.	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2.1: For Secure Email certificates, a challenge email is sent to the mailbox requested in registration. If the mailbox owner is capable of seeing and replying to the email, whether by clicking a link contained within the challenge or returning an acceptable reply via email to the challenge, the email identity is deemed validated. Challenge URIs and/or tokens are randomly generated per validation request and time out after a period not exceeding 7 days (although TrustCor CA may shorten that period at its discretion).	**Verified?**	Verified

	If the request was for a Basic Secure Mail certificate, the validation process is complete, and the certificate can be issued, assuming that it would pass the normal checks for uniqueness, key strength and so on.		
Code Signing Subscriber Verification Pro	Mozilla is no longer enabling the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS section 5.2.3	**Verified?**	Verified
Network Security	CPS section 6.5 and 6.7	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	TrustCor RootCert CA-2	**Root Case No**	R00000102
Request Status	Ready for Public Discussion	**Case Number**	00000074

Certificate Data

Certificate Issuer Common Name	TrustCor RootCert CA-2
O From Issuer Field	TrustCor Systems S. de R.L.
OU From Issuer Field	TrustCor Certificate Authority
Valid From	2016 Feb 04
Valid To	2034 Dec 31
Certificate Serial Number	25a1dfca33cb5902
Subject	CN=TrustCor RootCert CA-2, OU=TrustCor Certificate Authority, O=TrustCor Systems S. de R.L., C=PA
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	B8:BE:6D:CB:56:F1:55:B9:63:D4:12:CA:4E:06:34:C7:94:B2:1C:C0
SHA-256 Fingerprint	07:53:E9:40:37:8C:1B:D5:E3:83:6E:39:5D:AE:A5:CB:83:9E:50:46:F1:BD:0E:AE:19:51:CF:10:FE:C7:C9:65
Certificate Fingerprint	93:E4:63:5F:12:77:A2:CC:AB:30:9F:14:15:17:C7:73:AF:43:55:FC:F2:FD:E8:BC:F4:50:19:43:CC:00:5E:59
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root issues internally-operated SubCAs which issue SSL and S/MIME certificates.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8716897	**Verified?**	Verified
CRL URL(s)	http://crl.trustcor.ca/ http://crl.trustcor.ca/root/ca2.crl http://crl.trustcor.ca/sub/ca2-site.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.trustcor.ca/root/ca2 http://ocsp.trustcor.ca/sub/ca2-site Maximum expiration time of OCSP responses: 4 days	**Verified?**	Verified

Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://catest2.trustcor.ca/	**Verified?**	Verified
Test Website - Expired	https://catest2-expired.trustcor.ca/		
Test Website - Revoked	https://catest2-revoked.trustcor.ca/		
Example Cert			
Test Notes			

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

Revocation Tested	https://certificate.revocationcheck.com/catest2.trustcor.ca no errors	**Verified?**	Verified
CA/Browser Forum Lint Test	No errors (cert not found by CT)	**Verified?**	Verified
Test Website Lint Test	Tested. No errors.	**Verified?**	Verified
EV Tested	Not requesting EV treatment	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	This root issues internally-operated SubCAs which issues SSL and S/MIME certificates. CPS section 1.3.1: The Enhanced Root Certificate (CA-2) - used as the root of trust for certificates issued under the Enhanced Assurance programme. Currently two subordinate CA are issued under this root: - Enhanced Secure Email CA (Subordinate CA2-Email) - Enhanced Secure Site CA (Subordinate CA2-Site)	**Verified?**	Verified
Externally Operated SubCAs	This root does not and will not have any subCAs that are operated by external third parties.	**Verified?**	Verified
Cross Signing	None. None planned	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No third parties can issue certificates signed by this root. The Enterprise Root Certificate (ECA-1) is the only root allowed to issue externally-operated subCAs. CPS section 1.3.2: External RAs are not entitled to perform general domain or organizational validation; they are strictly limited to registration for credentials to domains and principals assigned to their specific organization.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English	**Verified?**	Verified
CA Document Repository	https://www.trustcorsystems.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.trustcorsystems.com/static/webtrust/cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.trustcorsystems.com/static/webtrust/cps.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	Princeton Audit Group (PAG)	**Verified?**	Verified
Auditor Website	http://princetonauditgroup.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2169&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	12/15/2016	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2163&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	12/15/2016	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8860163	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.1: For Basic Secure Site certificates, any of the following methods may be used to establish authority to use the domain name requested: 1. Check that the relevant domain name registrar via WHOIS and validate that the name on the certificate matches that of the requestor. 2. Using the registrar supplied details, communicate with the registrant using email, telephone or postal mail to ensure that the request was genuine. ... 3. Failing the above, send an email to the well known administrative email addresses for a domain, pruning such components from the FQDN until a registered domain is reached. The administrative mailboxes will be “admin”, “administrator”, “hostmaster”, “postmaster” and “webmaster”. ... ... For Enhanced Secure Site certificates, all of the FQDNs requested must be validated by the above process, although a single validation may cover multiple FQDNs if they share a domain. Note that this validation is necessary, but not sufficient for an Enhanced Secure Site certificate.	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization	CPS sections 3.2.2, 3.2.3, and 3.2.5.	**Verified?**	Verified

Verification Procedures			
Email Address Verification Procedures	CPS section 3.2.2.1: For Secure Email certificates, a challenge email is sent to the mailbox requested in registration. If the mailbox owner is capable of seeing and replying to the email, whether by clicking a link contained within the challenge or returning an acceptable reply via email to the challenge, the email identity is deemed validated. Challenge URIs and/or tokens are randomly generated per validation request and time out after a period not exceeding 7 days (although TrustCor CA may shorten that period at its discretion). If the request was for a Basic Secure Mail certificate, the validation process is complete, and the certificate can be issued, assuming that it would pass the normal checks for uniqueness, key strength and so on.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer enabling the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS section 5.2.3	**Verified?**	Verified
Network Security	CPS section 6.5 and 6.7	**Verified?**	Verified

Root Case Record # 3

Root Case Information

Root Certificate Name	TrustCor ECA-1	**Root Case No**	R00000103
Request Status	Ready for Public Discussion	**Case Number**	00000074

Certificate Data

Certificate Issuer Common Name	TrustCor ECA-1
O From Issuer Field	TrustCor Systems S. de R.L.
OU From Issuer Field	TrustCor Certificate Authority
Valid From	2016 Feb 04
Valid To	2029 Dec 31
Certificate Serial Number	0084822c5f1c62d040
Subject	CN=TrustCor ECA-1, OU=TrustCor Certificate Authority, O=TrustCor Systems S. de R.L., C=PA
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	58:D1:DF:95:95:67:6B:63:C0:F0:5B:1C:17:4D:8B:84:0B:C8:78:BD
SHA-256 Fingerprint	5A:88:5D:B1:9C:01:D9:12:C5:75:93:88:93:8C:AF:BB:DF:03:1A:B2:D4:8E:91:EE:15:58:9B:42:97:1D:03:9C
Certificate Fingerprint	76:C9:69:C4:BA:3E:3C:6D:05:6E:B7:08:CB:6C:CF:1A:1D:B9:AC:3D:43:73:09:B7:47:B5:29:7B:AB:C3:16:36
Certificate Version	3

Technical Information about Root Certificate

Certificate	There will be externally-operated subCAs	**Verified?**	Verified

Summary	chaining up to this root.		
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8716898	**Verified?**	Verified
CRL URL(s)	http://crl.trustcor.ca/ http://crl.trustcor.ca/root/eca1.crl http://crl.trustcor.ca/sub/eca1-external.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.trustcor.ca/root/eca1 http://ocsp.trustcor.ca/sub/eca1-external Maximum expiration time of OCSP responses: 4 days	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://valid.epki.external.trustcor.ca/	**Verified?**	Verified
Test Website - Expired	https://expired.epki.external.trustcor.ca/		
Test Website - Revoked	https://revoked.epki.external.trustcor.ca/		
Example Cert	https://ecatest1.trustcor.ca/		
Test Notes			

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

Revocation Tested	https://certificate.revocationcheck.com/ecatest1.trustcor.ca no errors	**Verified?**	Verified
CA/Browser Forum Lint Test	No errors (no cert found via CT)	**Verified?**	Verified
Test Website Lint Test	Tested. No errors.	**Verified?**	Verified
EV Tested	Not requesting EV treatment.	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CPS section 1.3.1: The Enterprise Root Certificate (ECA-1) - used as the ultimate root for enterprise PKIs issuing credentials to their principals in restricted namespaces. There is one subordinate CA under this root: - Enterprise External PKI CA (Subordinate ECA1-External) TrustCor CA undertakes to ensure that all operations conducted using these certificates, including registration of entities, validation of same, issuance and revocation of certificates are performed in accordance with the strictures of this document, the governing CP. Note that Enterprise Subordinate CA certificates are still TrustCor CA certificates, and TrustCor CA is responsible for their issuance,	**Verified?**	Verified

	insofar as the enterprise subscriber agreements is obeyed. TrustCor CA is responsible for revoking an enterprise subordinate CA should it discover substantive violations of its enterprise agreements.		
Externally Operated SubCAs	There will be subCAs that are operated by external third parties in this CA hierarchy. CPS section 1.3.2: External RAs are present where external Enterprise CAs have been licensed to issue name restricted TrustCor CA certificates; such RAs must adhere to the terms of registration, validation and publication as noted in this document as well as the Enterprise Subscriber Agreement between TrustCor CA and the subscribing organization. External RAs are not entitled to perform general domain or organizational validation; they are strictly limited to registration for credentials to domains and principals assigned to their specific organization. CPS section 4.2: For Enterprise Subordinate CAs, the processing is done by the RA belonging to the enterprise subscriber, and issuance is done under the technically restricted CA software under the enterprise subscriber's control.	**Verified?**	Verified
Cross Signing	CPS section 3.2.6: TrustCor CA may cross-certify other CA certificates, subject to a specific agreement between TrustCor CA and another party. The cross-signed certificates will be made available under the same terms as TrustCor CA's own CA certificates on the repository specified in Section 2.1.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS section 7.1.2.2: For Enterprise Subordinate CAs, there will also be a NameConstraints extension, which represents the following information: - permittedSubtree: -- dNSName: (repeated for each domain owned by the subscriber's enterprise) -- dirName: C=, ST=, L=, O= - excludedSubTree: -- IP: 0.0.0.0/0.0.0.0 -- IP: 0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English	**Verified?**	Verified
CA Document Repository	https://www.trustcorsystems.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.trustcorsystems.com/static/webtrust/cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.trustcorsystems.com/static/webtrust/cps.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	Princeton Audit Group (PAG)	**Verified?**	Verified
Auditor Website	http://princetonauditgroup.com/	**Verified?**	Verified

Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2169&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	12/15/2016	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2163&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	12/15/2016	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1.1 CPS section 4.9.1.2, Reasons for Revoking a Subordinate CA: An Enterprise Subordinate CA cannot maintain its operations consistent with behavior required in the Baseline Requirements.	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8860163	**Verified?**	Verified
SSL Verification Procedures	CPS section 4.2: For Enterprise Subordinate CAs, the processing is done by the RA belonging to the enterprise subscriber, and issuance is done under the technically restricted CA software under the enterprise subscriber's control. Enterprise subordinate CAs are technically constrained via Name Constraints as described in CPS section 7.1.2.2.	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	CPS section 3.3.1: Enterprise Subordinate CAs may only be re-keyed via a manual process involving reassessment of the original documents and policies that the subscriber has submitted to TrustCor CA. CPS section 4.1.1: Application for Enterprise Subordinate CA certificates may be initiated via email, but the process of registration and validation then requires postal/courier communications, as well as possible site visit scrutiny from TrustCor CA.	**Verified?**	Verified
Email Address Verification Procedures	Enterprise subordinate CAs are technically constrained via Name Constraints as described in CPS section 7.1.2.2.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer enabling the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS section 5.2.3	**Verified?**	Verified
Network Security	CPS section 6.5 and 6.7	**Verified?**	Verified