Bugzilla Summary:

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	TrustCor Systems S. de R.L.
Website URL	http://www.trustcorsystems.com
Organizational type	Commercial
Primary Market / Customer Base	TrustCor develops privacy protection services and issues certificates to its customers in support of such services.
Impact to Mozilla Users	Firefox and Thunderbird users may encounter SSL certs that chain up to some of these roots.
CA Contact Information	Contact: Neil Dunbar <ndunbar@trustcorsystems.com> CA Email Alias: registrar@trustcor.ca CA Phone Number: +44 1872 580534 Title / Department: CA Administrator/Certification Authority

Technical information about each root certificate

Certificate Name	TrustCor RootCert CA-1

Certificate Issuer Field	Country = PA
	StateOrProvince = Panama
	Locality = Panama City
	Organization = TrustCor Systems S. de R.L.
	Organizational Unit = TrustCor Certificate Authority
	Common Name = TrustCor RootCert CA-1

Certificate Summary	Root is offline. Used only to issue SubCAs, CRLs every 6 months (or more frequently as needed), and OCSP certificates.
Root Cert URL	https://www.trustcorsystems.com/certs/TrustCor_RootCert_CA1.der
SHA1 Fingerprint	EE:6B:49:3C:7A:3F:0D:E3:B1:09:B7:8A:C8:AB:19:9F:73:33:50:E7
Valid From	2014-12-03
Valid To	2029-12-31
Certificate Version	3
Certificate Signature Algorithm	SHA256WithRSA
Signing key parameters	RSA 2048, 256
Test Website URL (SSL) Example Certificate (non-SSL)	https://catest1.trustcor.ca/

CRL URL	URL: http://crl.trustcor.ca/root/ca1.crl
OCSP URL	URL: http://ocsp.trustcor.ca/root/ca1 *Maximum expiration time of OCSP responses*: 4 days
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	DV
EV Policy OID(s)	n/a

CA Hierarchy information for each root certificate

CA Hierarchy	Root will be used to issue internally-operated SubCAs which will issue SSL and S/MIME certificates.
Externally Operated SubCAs	This root does not and will not have any subCAs that are operated by external third parties.
Cross-Signing	n/a
Technical Constraints on Third-party Issuers	No third parties can issue certificates signed by this root.

Technical information about each root certificate

Certificate Name	TrustCor RootCert CA-2

Certificate Issuer Field	Country = PA
	StateOrProvince = Panama
	Locality = Panama City
	Organization = TrustCor Systems S. de R.L.
	Organizational Unit = TrustCor Certificate Authority
	Common Name = TrustCor RootCert CA-2

Certificate Summary	Root is offline. Used only to issue SubCAs, CRLs every 6 months (or more frequently as needed), and OCSP certificates.
Root Cert URL	https://www.trustcorsystems.com/certs/TrustCor_RootCert_CA2.der
SHA1 Fingerprint	D9:FE:21:40:6E:94:9E:BC:9B:3D:9C:7D:98:20:19:E5:8C:30:62:B2
Valid From	2014-12-03
Valid To	2034-12-31
Certificate Version	3
Certificate Signature Algorithm	SHA256WithRSA
Signing key parameters	RSA 4096, 256
Test Website URL (SSL) Example Certificate (non-SSL)	https://catest2.trustcor.ca/
CRL URL	URL: http://crl.trustcor.ca/root/ca2.crl
OCSP URL	URL: http://ocsp.trustcor.ca/root/ca2 *Maximum expiration time of OCSP responses*: 4 days
Requested Trust Bits	Websites (SSL/TLS)

	Email (S/MIME)
SSL Validation Type	OV
EV Policy OID(s)	n/a

CA Hierarchy information for each root certificate

CA Hierarchy	Root will be used to issue internally-operated SubCAs which will issue SSL and S/MIME certificates.
Externally Operated SubCAs	This root does not and will not have any subCAs that are operated by external third parties.
Cross-Signing	n/a
Technical Constraints on Third-party Issuers	No third parties can issue certificates signed by this root.

Technical information about each root certificate

Certificate Name	TrustCor ECA-1

Certificate Issuer Field	Country = PA
	StateOrProvince = Panama
	Locality = Panama City
	Organization = TrustCor Systems S. de R.L.
	Organizational Unit = TrustCor Certificate Authority
	Common Name = TrustCor ECA-1

Certificate Summary	Root is offline. Used only to issue SubCAs, CRLs every 6 months (or more frequently as needed), and OCSP certificates.
Root Cert URL	https://www.trustcorsystems.com/certs/TrustCor_ECA1.der
SHA1 Fingerprint	44:9E:48:F5:CC:6D:48:D4:A0:4B:7F:FE:59:24:2F:83:97:99:9A:86
Valid From	2014-12-03
Valid To	2029-12-31
Certificate Version	3
Certificate Signature Algorithm	SHA256WithRSA
Signing key parameters	RSA 2048, 256
Test Website URL (SSL) Example Certificate (non-SSL)	https://ecatest1.trustcor.ca/
CRL URL	URL: http://crl.trustcor.ca/root/eca1.crl
OCSP URL	URL: http://ocsp.trustcor.ca/root/eca1 *Maximum expiration time of OCSP responses*: 4 days
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	OV
EV Policy OID(s)	n/a

CA Hierarchy information for each root certificate

CA Hierarchy	Root will be used to issue internally-operated SubCAs which which in turn issue name constrained SubCA certificates; those in turn issue SSL and SMIME certificates for specified subdomains and email domains.
Externally Operated SubCAs	This root does will have subCAs that are operated by external third parties, but those parties are constrained to limited namespaces as per the CPS
Cross-Signing	n/a
Technical Constraints on Third-party Issuers	Each subCA cert contains restrictions on the type of certificates (Email Protection, Client/Server authentication) which it can issue. For S/MIME issuing subCAs, each one has a list of email domains for which it may issue certificates For SSL issuing subCAs, each one has a list of allowable domains. Unrestricted external subCAs are not permitted.

Verification Policies and Practices

Policy Documentation	*Language(s) that the documents are in*: English CP: https://www.trustcorsystems.com/static/webtrust/cp.pdf CPS: https://www.trustcorsystems.com/static/webtrust/cps.pdf
Audits	Audit Type: WebTrust for CA Auditor: Princeton Audit Group Auditor Website: https://princetonauditgroup.com/ URL to Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1800
Baseline Requirements (SSL)	*What is your status in regards to complying with the CAB Forum Baseline Requirements? (https://cabforum.org/wp-content/uploads/CAB-Forum-BR-1.3.0.pdf)* TrustCor complies with the BR document as per v1.3.0 of that document. *As per the CAB Forum Baseline Requirement # 8.3, where is the "Commitment to Comply" statement that should be in your CP or CPS?* Section 1.1 [Overview] of the CPS.
SSL Verification Procedures	*If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices* • *URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber.* ○ See http://www.trustcorsystems.com/resources/TrustCorCPS.pdf [Section 3.2

	Identity Validation] • If a challenge-response mechanism via email is used to confirm the ownership/control of the domain name, then provide the list of email addresses that are used for verification. ○ http://www.trustcorsystems.com/resources/TrustCorCPS.pdf [Section 3.2.2.1 Identity]. The list includes “admin‟, “administrator‟, “webmaster‟, “hostmaster‟, and “postmaster‟. • *Confirm that you have automatic blocks in place for high-profile domain names (including those targeted in the DigiNotar and Comodo attacks in 2011).* Confirmed. ○ *Specify the procedure for additional verification of a certificate request that is blocked*. Our certificate issuance API checks for a list of high profile domain names and flags the certificate request as needing manual supervision if such a domain is found in any of the names being requested. • *If OV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the identity, existence, and authority of the organization to request the certificate.* ○ See http://www.trustcorsystems.com/resources/TrustCorCPS.pdf [Section 3.2.2.2 DBA/Tradename] • If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate. ○ TrustCor does not currently issue EV certificates
Organization Verification Procedures	See above
Email Address Verification Procedures	*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* • See Section 3.2.2.1 [Identity] in http://www.trustcorsystems.com/resources/TrustCorCPS.pdf
Code Signing Subscriber Verification Procedures	*If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices* ○ *n/a*
Multi-factor Authentication	*Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance or specify the technical controls that are implemented by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.* • *For each account that can access the certificate issuance system, do you have the log-in procedure require something in addition to username/password?* Confirmed • *Specify the form factor that you use. Examples of multi-factor authentication include smartcards, client certificates, one-time-passwords, and hardware tokens.* Client certificates with private keys generated on FIPS 140 Level 2 smartcards. • *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. • *If technical controls are used instead of multi-factor auth for any accounts, then specify what those technical controls are.* All certificate issuing capable accounts use multi-factor auth; there are no exceptions.
Network Security	*Confirm that you have performed the actions listed in #7 of* *https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices* *Confirm that you have done the following, and will do the following on a regular basis:* • *Check for mis-issuance of certificates, especially high-profile domains.* Confirmed. • *Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.* Confirmed – performed on an ongoing basis. • *Ensure Intrusion Detection System and other monitoring software is up-to-date.* Confirmed: HIDS runs on all CA related systems, update is scheduled monthly. • *Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion.* Confirmed.

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

Publicly Available CP and CPS	Yes – see above.
CA Hierarchy	https://www.trustcorsystems.com/resources
Audit Criteria	See above (**Verification Policies and Practices:** Audits)
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	See Section 4.9 Certificate Revocation and Suspension in the CPS mentioned above.
Verifying Domain Name Ownership	See the CPS Section 3.2.2.1 [Identity]
Verifying Email Address Control	See the CPS Section 3.2.2.1 [Identity]
Verifying Identity of Code Signing Certificate Subscriber	TrustCor does not issue Code Signing Certificates
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 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.

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

Long-lived DV certificates	DV certificates issued by TrustCor have a maximum validity period of 12 months.
Wildcard DV SSL certificates	TrustCor does not issue wildcard DV certificates.

Email Address Prefixes for DV Certs	See the CPS, Section 3.2.2.1 [Identity]
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.
https://wiki.mozilla.org/CA:Problematic_Practices - 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.