CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

Introduction

Legal Name of CA: **TrustCor Systems, S. de R.L.**

Root and Subordinate certificates under consideration (with SHA-1 hashes of the certificate public keys)
TrustCor RootCert CA-1 (SHA-1 hash EE:6B:49:3C:7A:3F:0D:E3:B1:09:B7:8A:C8:AB:19:9F:73:33:50:E7)
Basic Email Subordinate CA (SHA-1 hash E4:0B:1D:5B:9A:AA:7E:C9:C6:6B:64:38:76:71:C0:76:CA:97:29:3A)
Basic Site Subordinate CA (SHA-1 hash B7:38:A7:99:92:D7:C6:AA:4E:FB:3E:D3:1C:4E:BD:19:C8:E9:92:4D)
Basic Site 2048 Subordinate CA (SHA-1 hash 70:89:27:66:D4:13:BB:EE:03:57:1D:89:52:94:89:09:19:7B:6D:17)
TrustCor RootCert CA-2 (SHA-1 hash D9:FE:21:40:6E:94:9E:BC:9B:3D:9C:7D:98:20:19:E5:8C:30:62:B2)
Enhanced Email Subordinate CA (SHA-1 hash A8:25:C6:DE:84:F4:28:7A:6C:7A:A6:03:65:94:51:0A:16:AC:C9:FE)
Enhanced Site Subordinate CA (SHA-1 hash 91:F7:F1:FC:8E:0A:76:BE:FA:E6:00:05:AF:D7:02:A2:24:CD:5A:9E)
TrustCor ECA-1 (SHA-1 hash 44:9E:48:F5:CC:6D:48:D4:A0:4B:7F:FE:59:24:2F:83:97:99:9A:86)
External PKI Subordinate CA (SHA-1 hash 66:C9:D2:44:CC:AD:A5:D6:96:D3:04:12:DF:1D:C5:88:0F:5C:8D:BA)

Version of BRs used: **1.4.4**

CA Documents Assessed: **CPS** [**Version 1.3.1;** https://www.trustcorsystems.com/resources/cps.pdf]; **CP** [**Version 1.3.1;** https://www.trustcorsystems.com/resources/cp.pdf]

Self-Assessment Update Policy: TrustCor CA will update this assessment once per year, or whenever a new version of the CP/CPS documents is published, whichever comes sooner

BR Section Number	**List the specific documents and section numbers of those documents which meet the requirements of each BR section**	**Explain how the CA's listed documents meet the requirements of each BR section.**
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	1.0.0 - [01-Jul-12] Document as a whole represents BR compliance 1.0.1 - [01-Jan-13] CPS, Section 8.2 1.0.2 - [08-Jun-12] CPS, Section 7.1.5 1.0.3 - [22-Jun-12] CPS, Sections 3.1.6, 4.1.1 1.0.4 - [01-Aug-13] CPS, Section 4.9.10 1.0.5 - [12-Sep-12] CPS, Section 3.1.2 1.1.0 - [14-Sep-12] Document as a whole represents BR compliance 1.1.1 - [07-Nov-12] CPS, Section 6.1.1.2 1.1.2 - [20-Feb-13] CPS, Sections 3.2.2.6, 3.1.2 1.1.3 - [21-Feb-13] CPS, Section 3.2.4, Section 7.1 1.1.4 - [03-May-13] CPS, Section 6.1.5 1.1.5 - [31-May-2013] CPS, Section 7.1.4.2 1.1.6 - [29-Jul-2013] CPS, Sections 1.3.1, 4.9.10, 4.9.1.2, 7.1.2.2 1.1.7 - [03-Apr-2014] CPS, Section 3.1.2 1.1.8 - [05-Jun-2014] CPS, Section 3.2.2.4 1.1.9 - [04-Aug-2014] CPS, Section 3.1.2 1.2.0 - [15-Apr-2015] CPS, Sections 4.2.1, 3.2.2.8 1.2.1 - [16-Jan-2015] CPS, Section 7.1.3 1.2.2 - [16-Oct-2014] CPS, Section 7.1.2.5 1.2.3 - [16-Oct-2014] CPS, Section 8.2 1.2.4 - [18-Feb-2015] CPS, Section 3.1.3 1.2.5 - [02-Apr-2015] CPS, Section 7.1.4.2 1.3.0 - [16-Apr-2015] CPS, Document as whole in RFC 3647 format 1.3.1 - [28-Sep-2015] CPS, Sections 7.1.6.1, 7.1.6.4 1.3.2 - [03-Dec-2016] CPS, Sections 1.5.2, 2.3, 2.4 1.3.3 - [04-Feb-2016] CPS, Sections 4.9.2, 4.9.6 1.3.4 - [15-Mar-2016] CPS, Section 3.1.3 1.3.5 - [10-May-2016] CPS, Sections 1.6, 4.9.9, 7.1.2.3 1.3.6 - [01-Jul-2016] CPS, Section 8.2 1.3.7 - [30-Sep-2016] CPS, Section 7.1 1.3.8 - [01-Mar-2017] CPS, Section 3.2.2.4 1.3.9 - [27-Nov-2016] CPS, Section 9.16.3 1.4.0 - [11-Sep-2016] CPS, Section 9.6.3 1.4.1 - [07-Sep-2016] CPS, Section 7.1.4.2 1.4.2 - [07-Jan-2017] CPS, Section 3.2.2.4 1.4.3 - [08-Mar-2017] CPS, Section 3.2.2.8 1.4.4 - [17-Mar-2017] CPS, Section 1.4.1	CP and CPS documents 1.0.0 were written in accordance with version 1.1.9 of the BR document. No certificates were issued prior to version 1.0.0 CPS being in force. 1.2.0 - CAA record checking was introduced as per CPS Section 4.2.1 1.2.1 - No certificates were ever produced using SHA-1 as a digest algorithm 1.2.2 - TrustCor CA does not currently publish to CT logs, so no precertificates have been published 1.2.3 - TrustCor CA uses WebTrust audits, so ETSI updates have no effect 1.2.4 - TrustCor CA does not publish EV certificates, and does not issue to .onion names, thus the change had no effect 1.2.5 - TrustCor CA root certificates always included org name and country code, and the subjects always had non-generic content. The change had no effect. 1.3.0 - Formatting change of BRs. No policy changes needed for CAs 1.3.1 - Resulted in CPS 1.1.0. OIDs incorporated into end-entity certs from Sep 2015 onwards. 1.3.2 - Resulted in CPS 1.2.0. CPS review requirements were always incorporated 1.3.3 - Third party CDP/OCSP stipulations were in 1.2.0. The BR change had no effect. 1.3.4 - No TrustCor end-entity certificate has, or has had, a lifetime in excess of 24 months. This change had no effect. 1.3.5 - These typographical changes had no effect on the CPS conditions, other than to replace RFC 2560 with RFC 6960, which was incorporated into version 1.2.1 of the CPS 1.3.6 - Since TrustCor does not use ETSI auditing, this change had no effect on the CPS conditions 1.3.7 - TrustCor had always used a 64 bit PRNG for serial numbers. This BR change produced no change in CPS stipulations. 1.3.8 - TrustCor did not support all of the DV validation methods listed in 3.2.2.4. The "any other method" clause was deleted in CPS version 1.2.0. The BR changes which did apply had no effect on existing DV validation methods. 1.3.9 - At the time of CPS issuance, no laws from the Republic of Panama have had any effect on TrustCor's issuance processes, thus the BR has had no effect. Neither has any revocation of Panamanian law affected issuance. 1.4.0 - TrustCor does not allow re-use of a PKCS10 submission, nor does it permit certificate modification (except for multi-SAN certificates, and that in very restricted fashion); thus the ability to keep using a private key if the certificate contains incorrect information would be inoperable. Revocation of a certificate means that a new private key pair would need to be generated in all circumstances. 1.4.1 - TrustCor certificates do not contain givenName and surName components, thus these conditions produce no behavioural changes. DV certificates have never contained those components, therefore no certificates were needed to be revoked. 1.4.2 - As per 1.3.8, not all of these changes were applicable to TrustCor (e.g. TLS over a random port, or test certificates). Those that were required no operational changes 1.4.3 - CAA checking was already part of TrustCor's issuance practice. No changes were necessary, although clarifying text regarding iodef handling has been added in CPS v1.3.1. 1.4.4 - The maximum lifetime of any TrustCor certificate was 24 months, falling within the 825 day limitation. Thus no CPS changes were needed, although '2 years' and '24 month' text has been replaced by 825 days in CPS v1.3.1 to avoid ambiguity.

1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	2013-01-01 - CPS 6.1.6 2013-01-01 - CPS 4.9.10 2013-01-01 - CPS 5, Management Assertion Letters 2013-08-01 - CPS 4.9.10 2013-09-01 - CPS 3.2.2.6 2013-12-31 - CPS 6.1.5 2015-01-16 - CPS 7.1.3 2015-04-01 - CPS 1.4.1, 6.3.2 2015-04-15 - CPS 3.2.2.8 2015-11-01 - CPS 3.2.2.5 2016-01-01 - CPS 7.1.3 2016-06-30 - CPS 7.1.2 2016-06-30 - CPS 1.4.1 2016-09-30 - CPS 4.3.1, 7.1 2016-10-01 - CPS 3.2.2.5 2016-12-03 - CPS 1, 2.2 2017-01-01 - CPS 7.1.3 2017-03-01 - CPS 3.2.2.4 2017-04-22 - CPS 4.2.1 2017-09-08 - CPS 3.2.2.8 2018-03-01 - CPS 1.4.1, 6.3.2	2013-01-01 - in compliance (software enforces RSA exponent choice) 2013-01-01 - in compliance (OCSP GET is supported) 2013-01-01 - in compliance (NetSec requirements are part of audit) 2013-08-01 - in compliance (OCSP responds with Extended Revoke for unissued certificates) 2013-09-01 - not applicable (TrustCor has not issued wildcard certificates) 2013-12-31 - in compliance (RSA 2048 is minimum permissible, and P-384 and P-521 are the only currently allowed curves) 2015-01-16 - in compliance (TrustCor has never used SHA-1 as a digest method for certificates) 2015-04-01 - in compliance (TrustCor has never issued a subscriber certificate with lifetime > 39 months) 2015-04-15 - in compliance (CPS support for CAA records since September 2015, before that CPS stated that CAA was not honoured) 2015-11-01 - not applicable (TrustCor has never issued IP certificates, so internal IP ranges are irrelevant) 2016-01-01 - in compliance (SHA-1 is not allowed as a digest method for certificates) 2016-06-30 - in compliance (all subscriber certificates are issued from Subordinate CAs) 2016-06-30 - in compliance (maximum allowable lifetime was always 3 years prior to the current CPS, but no certificate with a lifetime over 2 years has ever been issued) 2016-09-30 - in compliance (64 bit random serial numbers have always been used as the serial number algorithm) 2016-10-01 - not applicable (no IP certificates were issued, so none to revoke) 2016-12-03 - in compliance (adherence to latest BRs was always in CPS, and read-only public repository access was always the case) 2017-01-01 - in compliance (SHA-1 never used as certificate digest method, for any type of certificate, including OCSP) 2017-03-01 - in compliance (a selection of validation methods listed in the BRs are used for domain validation - no others are permissible) 2017-04-22 - in compliance (maximum age of validation source is stipulated as less than 825 days) 2017-09-08 - in compliance (CAA records always checked and honored) 2018-03-01 - in compliance (subscriber certificates are limited to 825 days, and none with longer validities currently exist)
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.	CPS, Section 1.3.2	External RAs are only allowed for technically constrained subordinate CAs under the External PKI business offering. TrustCor requires that external subordinate CAs are audited to the same standard as TrustCor itself, to ensure compliance with the BRs.

2.1. Repositories
Provide the direct URLs to the CA's repositories
	CPS, Section 2.1	Root Certificates: `http://www.trustcor.ca/certs/root`
		`Subordinate Certificates: http://www.trustcor.ca/certs/sub`
		`CP document: http://www.trustcor.ca/resources/cp.pdf`
		`CPS document: http://www.trustcor.ca/resources/cps.pdf`
		`CRLs: http://crl.trustcor.ca/root/ca1.crl`
		`http://crl.trustcor.ca/root/ca2.crl`
		`http://crl.trustcor.ca/root/eca1.crl`
		`http://crl.trustcor.ca/sub/ca1-email.crl`
		`http://crl.trustcor.ca/sub/ca1-site.crl`
		`http://crl.trustcor.ca/sub/ca1-site-2048.crl`
		`http://crl.trustcor.ca/sub/ca2-email.crl`
		`http://crl.trustcor.ca/sub/ca2-site.crl`
		`http://crl.trustcor.ca/sub/eca1-external.crl`

2.2. Publication of information
"The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest
published version."
Copy the specific text that is used into the explanation in this row. (in English)
AND
List the URLs to the three test websites for each root certificate under consideration, as per: "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired."
	CPS, Section 2.2	RootCert CA-1 valid: `https://catest1.trustcor.ca/`
		`RootCert CA-1 revoked: https://catest1-revoked.trustcor.ca/`
		`RootCert CA-1 expired: https://catest1-expired.trustcor.ca/`
		
		`RootCert CA-2 valid: https://catest2.trustcor.ca/`
		`RootCert CA-2 revoked: https://catest2-revoked.trustcor.ca/`
		`RootCert CA-2 expired: https://catest2-expired.trustcor.ca/`
		
		`ECA1-External valid: https://valid.epki.external.trustcor.ca/`
		`ECA1-External revoked: https://revoked.epki.external.trustcor.ca/`
		`ECA1-External expired: https://expired.epki.external.trustcor.ca/`

2.3. Time or frequency of publication Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.	CPS, Section 2.3	Published CP/CPS documents shall be updated as frequently as six months, or within seven days of internal approval.

2.4. Access controls on repositories Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.	CPS, Section 2.4, 8.6	All repositories have public read-only accessibility. Audit documents are published and linked directly from the WebTrust website.
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, indicate how your CP/CPS meets the requirements in this section of the BRs.	CPS, Sections 3.1.2, 3.2.2.1	Organizational names must be registered with a government body in the country of their incorporation, and must be live entities (ie, not defunct or dormant) within those registries. Alternatively, a trustworthy source must provide a signed declaration that the applicant is entitled to assert the organizational name.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, indicate how your CP/CPS meets the requirements in this section of the BRs.	CPS, Section 3.2.2.2	A government entity in the country of incorporation must attest that the tradename is valid and that the applicant is entitled to assert it.
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	CPS, Section 3.2.2.3	Where the country appears in the certificate, ISO-3166 codes are derived from the validation process in CPS Section 3.2.2.2.
3.2.2.4 Validation of Domain Authorization or Control Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.	CPS, Section 3.2.2.4	Methods of validation include: contact through WHOIS/RDAP information (email address, postal mail to physical address, and/or phone verification); verification email to administrative mailboxes (“admin”, “administrator”, “hostmaster”, “postmaster”, “webmaster”) @applicant-domain; agreed-upon change to website; DNS change for domain.
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS Section 3.2.2.4.1	Using WHOIS/RDAP protocols, domain records are matched against applicant details.
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.4.2	Email or Post to addresses listed in WHOIS/RDAP records. Replies to queries must contain uniquely derived tokens. Specify: (Fax or SMS are not used to validate Domain Contact identity).
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.4.3	WHOIS/RDAP registered telephone numbers may be used in validation process. Replies must confirm the details stipulated in the original application.

3.2.2.4.4 Constructed Email to Domain Contact
If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.
	CPS 3.2.2.4.4	Email to:
		`admin`
		`administrator`
		`hostmaster`
		`postmaster`
		`webmaster`
		@applicant-domain sent with challenge. Reply must go via website or email processing reflecting request token.

3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.4.5	CA does not rely upon domain authorization documents to validate applications.
3.2.2.4.6 Agreed−Upon Change to Website If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.4.6	Applicant must cause a successful URI to return (via a HTTP GET request). URI is http{s}://{applicant-domain}/.well-known/pki-validation/trustcor-ca.txt. Returned document must contain a unique request token, which expires after 7 days.
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.4.7	Applicant must post a TXT record containing the text `trustcor-ca={request token}` in its value. Token expires after 7 days.

3.2.2.4.8 IP Address If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.4.8	CA does not use IP Address validation.
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.4.9	CA does not use the test certificate validation method.
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.4.10	CA does not use this method of domain validation.
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.5	CA does not issue certificates containing IP address identities.
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS−ID, then indicate how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.6	CA does not issue wildcard certificates.
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	CPS 3.2.2.7	Sources rated based on liveness, primary authority of information, reliability of regulatory oversight. Regularly reviewed and sources added/removed based on those criteria.
3.2.3. Authentication of Individual Identity	CPS 3.2.3	Email certs require demonstrated control over mailbox (request token); enhanced email requires additional identity information (passport, photo ID) etc. Secure Site certificates do not establish individual identity.
3.2.5. Validation of Authority	CPS 3.2.5	Organizational applicants will have their details verified by the methods in 3.2.2.1 and 3.2.2.2, and those contact details used to establish a primary authority to designate an organization's technical contact set.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CPS 3.2.6	No current cross-certificates involving TrustCor exist.
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CPS 4.1.1	OFAC blacklist; Internal blacklist is used and maintained to identify suspicious requests, previously revoked requests, and suspected fraudulent usage.
4.1.2. Enrollment Process and Responsibilities	CPS 4.1.2	Applicant: creates account; submits PKCS#10; provides cert information, agrees to subscriber agreement, picks up certificate, places certificate in use, or rejects certificate TrustCor: validates details, validates public key, issues certificate.
4.2. Certificate application processing	CPS 4.2	Done by TrustCor CA, unless an External PKI Subordinate CA is processing a request under its constrained namespace, in which case the external partner performs the certificate request
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.	CPS 4.2.1	TrustCor maintains an internal database of forbidden domains (usually .gov, .mil types) to which it will not issue under any circumstances. Also contains a list of high value domains (google.com, microsoft.com). All domains are mapped via a set of confusables to a canonical form - if a requested domain is too similar to a high value domain, then a high risk flag is set which requires human intervention to approve certificate generation. Failure to approve indicates rejection and potential addition to customer blacklist if the request is seen as potentially fraudulent.
4.2.2. Approval or Rejection of Certificate Applications	CPS 4.2.2	Expired gTLDs cause auto-revocation within 30 days. gTLDs under consideration are not allowed, and TrustCor will not certify names not under publicsuffix.
4.3.1. CA Actions during Certificate Issuance	CPS 4.3.1, (qv 5.2.2)	Root CA issuance cannot be done automatically (the root CA HSMs are offline); thus explicit human interaction is needed for signature by a Root CA.
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	CPS 4.9.1.1	The CA may revoke a Subscriber Certificate if any of the following occur: compromise of private key and/or account, violation of agreement terms, identity assertions no longer applicable, trademark dispute, suspect of fraudulent or illegal conduct involving certificate, subscriber appearing on the OFAC list, and additional circumstances listed in 4.9.1.1.
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	CPS 4.9.1.2	The CA may revoke a Subordinate CA Certificate if any of the following occurs: compromise of private key, CA ceases operations, widespread misuse, violation of agreement terms, violation of BR.
4.9.2. Who Can Request Revocation	CPS 4.9.2	The following identities may request a certificate revocation: subscribers, the CA, representatives of root programs, CA/B.
4.9.3. Procedure for Revocation Request	CPS 4.9.3	The CA requests the following as procedure to consider a revocation: issuer DN, serial number of the certificate, and reason for revocation. The request must be submitted via email, ticketing system, or website.
4.9.5. Time within which CA Must Process the Revocation Request	CPS 4.9.5	24 hours, post validation of request for normal certificates; 1 hour for Subordinate CA revocation.

4.9.7. CRL Issuance Frequency	CPS 4.9.7	Issuance frequency: End-entity certificates: at least every 24 hours; Subordinate CA CRLs: at least every 6 months; No more than 24 hours if a subordinate CA under a root certificate is revoked.
4.9.9. On-line Revocation/Status Checking Availability	CPS 4.9.9	Multi-region, low latency, 24x7 availability. 99% uptime target
4.9.10. On-line Revocation Checking Requirements Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.	CPS 4.9.9, 4.9.10	GET/POST support, status change for certificate around 5 minutes from authoritative state change, RFC 6960 Extended Revoke protocol used for non-issued certificates.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	CPS 4.9.11	CA does not require subscriber to deploy OCSP stapling.
4.10.1. Operational Characteristics	CPS 4.10.1	Site certificates removed from CRL/OCSP 1 day after expiry; S/MIME certificates removed 7 years post expiry.
4.10.2. Service Availability	CPS 4.10.2	OCSP servers are available 24/7 in 4 separate geographies, with failover between each location, and lowest latency selection.
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS	CPS 5.	Each data center must have robust controls governing location, construction and operations. Data centers must periodically review security policy, have an incident response plan, and a disaster recovery plan. TrustCor's auditors review security policies and require/review reports.
5.2.2. Number of Individuals Required per Task	CPS 5.2.2	Highly trusted tasks: 2 people (not processes), Trusted tasks: 1 person, Equipment moving: 2 people (minimum)
5.3.1. Qualifications, Experience, and Clearance Requirements	CPS 5.3.1	Must not be on OFAC list of proscribed personnel; no conflicts of interest which would compromise CAs integrity; skill levels assessed by TrustCor management before role assignment.
5.3.3. Training Requirements and Procedures	CPS 5.3.3	Training prior to employment, familiarity with security and privacy policies; training recorded in company knowledge base.
5.3.4. Retraining Frequency and Requirements	CPS 5.3.4	Retraining required on process, best practice and/or standards changes, retraining recorded in knowledge base as per Section 5.3.3.
5.3.7. Independent Contractor Controls	CPS 5.3.6, 5.3.7	Contractors must undergo same background check and training as permanent employees. Sanctions include contract termination and possible recovery of damages.
5.4.1. Types of Events Recorded	CPS 5.4.1	Host Level, Network Level, Certificate Authority Internal and Publishing Events, Site, and Operational Events.
5.4.3. Retention Period for Audit Logs	CPS 5.4.3, 5.5.2	Audit logs are retained online for at least 3 months, with an archived backup of at least 7 years.
5.4.8. Vulnerability Assessments	CPS 5.4.8	Automated vulnerability assessments conducted monthly (daily for high security hosts); vulnerability lists read and assessed with reference to patching/remediation. Security patches applied at most 1 month (low risk) to 1 hour (critical) on hosts (post testing on parallel test hardware).
5.5.2. Retention Period for Archive	CPS 5.5.2	Archived records are maintained for a minimum of 7 years.
5.7.1. Incident and Compromise Handling Procedures	CPS 5.7.1	HIDS on all hosts/network equipment alerting to system administrators; ITIL workflow on ticketing system for incidents.
6.1.1. Key Pair Generation	CPS 6.1.1.1	All CA key pairs generated and stored on FIPS 140 L3 or EAL 4+ rated HSMs. Root keys require commissioning script, signed by TrustCor personnel and witnesses. Root HSMs are offline, physical presence required in data center.
6.1.2. Private Key Delivery to Subscriber	CPS 6.1.2	CA does not perform private key delivery to subscriber.
6.1.5. Key Sizes	CPS 6.1.5	RSA: 2048 bit minimum; Enterprise Subordinate: 4096 bits, ECC: P-384 or P-521 curves; DSA: not used.
6.1.6. Public Key Parameters Generation and Quality Checking	CPS 6.1.6	Weak keys are checked and rejected if found, post generation. RSA public key exponents must be an odd integer greater than or equal to 3.
6.1.7. Key Usage Purposes	CPS 6.1.7, 7.1.2	CA Key usage purposes listed in Sections 6.1.7 & 7.1.2.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CPS 6.2, 6.2.1	FIPS 140-L3/EAL 4+ equipment required for CA key storage (root or subordinate).
6.2.5. Private Key Archival	CPS 6.2.5	CA does not perform archival of private keys.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CPS 6.2.6	Transferred between HSMs as manufacturer requires; keys encrypted in flight and at rest
6.2.7. Private Key Storage on Cryptographic Module	CPS 6.2.7	FIPS 140-L3/EAL 4+ storage required
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	CPS 1.4.1, 6.3.2	End entity (subscriber) certificates are limited to 1 year for basic certificates and 2 years for enhanced grade certificates. External PKI end entity certificates are mandated to have a maximum lifespan of 825 days.
6.5.1. Specific Computer Security Technical Requirements	CPS 6.5.1	Multi-factor authentication is used on both high and medium sensitivity hosts (using SSH private keys and OTP authentication)
7.1. Certificate profile	CPS 7.1	X.509 certificates used. All serial numbers are 64 bit random values
7.1.1. Version Number(s)	CPS 7.1.1	X.509 v3 used
7.1.2. Certificate Content and Extensions; Application of RFC 5280	CPS 7.1.2	Extensions on certificates described in CPS
7.1.2.1 Root CA Certificate	CPS 7.1.2.1	Extensions described in accordance with BR
7.1.2.2 Subordinate CA Certificate	CPS 7.1.2.2	Extensions described in accordance with BRs. Note: current subordinate CA certs do not contain EKU designations, and are thus not technically constrained as per 7.1.5

7.1.2.3 Subscriber Certificate	CPS 7.1.2.3	Extensions described in accordance with BRs. Since OCSP stapling is not mandated, OCSP URIs are present in certificates.
7.1.2.4 All Certificates	CPS 6.1.7, 7.1, 7.1.2.4	Conformance with RFC 5280 stipulated. The only other certificate type is OCSP Responder certificates, described in 6.1.7
7.1.2.5 Application of RFC 5280	CPS 7.1.2.5	Currently no pre-certificates are issued.
7.1.3. Algorithm Object Identifiers	CPS 7.1.3	SHA-1 has never been used in any signature scheme for any certificate
7.1.4. Name Forms	CPS 7.1.4	Details are covered in subsections under 7.1.4.
7.1.4.1 Issuer Information	CPS 7.1.4.1	Issuer DNs are constrained to chain up to the root CA certificates.
7.1.4.2 Subject Information	CPS 7.1.4.2	Only verified information exists in subject DNs
7.1.4.3 Subject Information - Subordinate CA Certificates	CPS 7.1.4.1, 7.1.4.3	Subordinate CA DNs explicitly listed
7.1.5. Name Constraints	CPS 7.1.2.2, 7.1.5	Name Constraints only in External PKI Subordinate CA certificates (s. 7.1.2.2)
7.1.6. Certificate Policy Object Identifier	CPS 7.1.6	Details are covered in subsections under 7.1.6.
7.1.6.1 Reserved Certificate Policy Identifiers	CPS 7.1.6.1, 7.1.6.4	Basic Site Cert == DV OID, Enhanced Site Cert == OV OID, Enhanced Email Cert == IV OID
7.1.6.2 Root CA Certificates	CPS 7.1.6.2	Root CA certs have no policy OIDs
7.1.6.3 Subordinate CA Certificates	CPS 7.1.6.3	External PKI subordinate CAs have certificate policy OIDs. The other subordinate CA certs do not.
7.1.6.4 Subscriber Certificates	CPS 7.1.6.4	See 7.1.6.1. Subscriber Certs have the OID of the CPS document embedded within them, but also contain DV, OV, IV OIDs as per the BRs.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	CPS 8	Compliance stipulation included (BRs plus WebTrust).
8.1. Frequency or circumstances of assessment	CPS 8.1	Audits performed at least once per year, and audits cover 1 year of operations.
8.2. Identity/qualifications of assessor	CPS 8.2	Auditors must be from WebTrust list of certified practitioners.
8.4. Topics covered by assessment	CPS 8, 8.4	Topics listed - WebTrust for CAs as controlling standard.
8.6. Communication of results	CPS 8.6	Audit Reports published on WebTrust site, and seals linked to via TrustCor's website.
8.7. Self-Audits	CPS 8.7	Quarterly self audits performed on 3% of issued certificates in all categories. Results made available to external auditor for validation.
9.6.1. CA Representations and Warranties	CPS 9.6.1	Warranties listed.
9.6.3. Subscriber Representations and Warranties	CPS 9.6.3	Requirements for subscriber stipulations listed.
9.8. Limitations of liability	CPS 9.8	External PKI issued certificates are still bound to all terms and conditions of the CPS, and cannot disclaim warranties which would conflict with same.
9.9.1. Indemnification by CAs	CPS 9.9.1	Application Software Suppliers held harmless, subject to limitations.
9.16.3. Severability	CPS 9.16.3	Competent legal authority clause in force. To date, no legal compulsion has caused a change to issuing practice or CPS stipulations.