CA/QUANTIFYING VALUE STATEMENT

What Kinds of Benefits can Your CA provide to Mozilla?

TrustCor's Certificate Authority is a critical component of TrustCor's business offerings, which are dedicated to providing state-of-the-art, simple to use, privacy enhancing products and services. For example, our popular MsgSafe.io communications privacy service delivers user-friendly simplification of encryption, including S/MIME. Among other advantages, we provide a unique positive effect for the Mozilla community in offering the most comprehensive, standards-based (S/MIME vs. proprietary or GnuPG-based) email encryption service available worldwide. Ours is also the only service that allows users to transition smoothly between both S/MIME and GnuPG standards, a challenge if unmet hinders widespread adoption of email encryption systems. S/MIME encryption and this type of standards-based service is only valuable if users can depend on it to work ubiquitously, which requires root program membership. While that might be achievable through partnership, as has been the case historically with S/MIME, business challenges and economics hinder widespread adoption which makes our continued root program membership absolutely critical. Our services are already used by more than a million customers around the world and we hope to continue to expand our reach to cross-market TLS server certificate sales, as well as leveraging our custom built API to support certificate resellers from all over (emphasizing LatAm).

We have innovated and lead the market in the adoption of TLS server certificate issuance for one of the longest-running and most respected dynamic DNS services worldwide and the positive impact this move has made cannot be overstated. Dynamic DNS services are a critical aspect of home-based IoT and "private cloud" solutions which have a dramatic and important positive impact on personal privacy and security. Instead of sending all your data to the cloud, dynamic DNS services allow users to self-host their video cameras, data storage and IoT home automation solutions in their home or small business, to enhance their privacy and security. Until our partnerships in this area, obtaining server certificates that operate properly with these private home systems relying upon dynamic DNS was elusive, complex to implement, and therefore the market was completely underserved. Finally, as a natively multi-lingual and multi-national staff from the outset, our mission includes (and we are well positioned to be) making certificate adoption more accessible to a number of communities including the LatAm community.

We have an excellent track record as far as requiring little oversight and until this inquiry, no negative implications for the Mozilla community. We have also been helpful to other organizations that have come after us, to assist them in their ascension into root programs successfully, and our volunteer contributions within the CA/B Forum should also not be overlooked.

What Information can a CA Provide to Plead their Case?

TrustCor has maintained inclusion and good standing in the Root Certificate Programs of the following browsers:

- Microsoft, since February 2015;
- Mozilla, since January 2018; and
- Apple, since January 2019.

We have maintained consecutive WebTrust Audits annually since 2014 from auditors who have always been listed as enrolled WebTrust practitioners. We have also been contributing members of the CA/Browser Forum since January of 2016, conforming to all versions of the Baseline Requirements since and staying ahead of industry trends and security standards. TrustCor has had a very low rate of compliance incidents since becoming a member of the CA/B forum, all of which formal responses be found publicly on our website: https://trustcor.com/resources/issuance-incidents/ and we continue to execute our business objective of being a diligent, competent certificate authority.

Reasons Why Applicant is Applying for Inclusion

1. **Why does the applicant want its root CA certificate(s) to be included by default in Mozilla's root store?**

   The continued inclusion of TrustCor's roots in Mozilla's root store is crucial for us to maintain strong public trust and securing the wide range of websites with TrustCor certificates visited by Firefox users. Inclusion with Mozilla also represents a pledge of confidence to our customers and general public for not only usability and interoperability, but also from Mozilla's strict rules and requirements that this chain of trust brings.

Whether the Applicant Commits Sufficient Resources to Compliance

1. **Who are the applicant's beneficial owners?**

   TrustCor is a privately-held, employee-owned company, and currently I am its largest equity-holder in the employee-owned company program. The CA business unit is controlled by the company's CA Approving Officials whereas other business unit executives or equity-holders are excluded from access-to or control-over the CA and any CA Business Operations as per TrustCor's exclusion provision.

2. **What is the applicant's investment in CA infrastructure and personnel?**

   TrustCor's investment, specific to the CA business unit, includes a portion of the overall data center facilities, hardware and software, personnel, operating expenses, and professional services including audits.

2018	2019	2020	2021	2022 EST
$ 1,387K USD	$ 1,067K USD	$ 937K USD	$ 1,030K USD	$ 1,150K USD

3. **What is the applicant's long-term commitment to investing in CA infrastructure and personnel?**

   TrustCor began investing in CA infrastructure in 2014 and has been engaged in the Root Certificate Programs since 2015. We have demonstrated a strong commitment to CA infrastructure over the past 8+ years and as the business volume grows annually, we commit that infrastructure and personnel investment will continue to match growth while maintaining or increasing quality.

4. **What system development resources have been allocated to ensure compliance, and how are they sufficient?**

   TrustCor has personnel responsible for overseeing compliance, identity validation, customer support, development, and IT; systems, network, and database administration. TrustCor maintains separate development, staging, and production environments. TrustCor's structured architecture and compliance-based processes allow phased deployment (rollout), testing, and rollback.

5. **What is the CA's compliance budget? How is it determined? Is it constrained by rules, processes, or procedures that will hamper the allocation of sufficient resources for compliance?**

   Compliance is at the core of every aspect of the TrustCor certificate business unit. Our compliance budget is determined primarily by estimating the expenses required to remain verifiably compliant with WebTrust, industry standards, and best practices. This includes primarily; the cost of personnel dedicated to monitoring, audit, vulnerability assessment, and portions of our facilities management and infrastructure operations budgets specific to the CA business unit.

   Additionally, our compliance budget is increased by projects identified during our risk assessment process, audits, and industry trends. We commit that the compliance budget and related personnel investment will continue to match growth while maintaining the quality of compliance outcomes.

Whether the Applicant Employs Skilled Personnel

1. **How well and closely does the CA track changes to industry requirements? How does the CA plan to stay informed and compliant with the ever-changing requirements?**

   TrustCor maintains representation in various CA/Browser Forum groups and weekly meetings, consistently reviewing the CA/Browser Forum mailing lists and ballots, monitoring the m.d.s.p. thread, the CCADB public list, Bugzilla, and WebTrust for CA Principles and Criteria updates. Development also reviews industry requirements as well as RFC's, linters and other relevant items as necessary. We have implemented best practices in our internal procedures for reviewing all updates to the Baseline Requirements and root store changes against current operations and we are able to deploy changes through our change management process as needed in a timely manner.

2. **Who are applicant's personnel who are familiar with CABF and IETF standards? How much PKI domain experience do these skilled employees have? What is the depth of their understanding and knowledge? (Risks arise when CAs stop investing in training or employ people who aren't as qualified as the people who the CA presented during the inclusion process.)**

   CA business unit operations staff include, but are not limited to, senior systems and network engineers, seasoned developers, compliance manager, and validation specialists; all of which have expertise in PKI and IETF standards and knowledge in WebTrust and CA/B Forum Baseline Requirements. Our team includes former GoDaddy and American Express employees familiar with their PKI implementations, active and contributing members of the CA/B Forum, Network Security Working Group, Server Certificate Working Group, S/MIME Certificate Working Group, Code Signing Certificate Working Group, and Validation Subcommittee.

   Each individual's PKI experience ranges from years to decades and we still employ many of the talented resources who have been active in TrustCor's CA business since its inception.

   As part of our CA practices, TrustCor completes periodic reviews of all job qualification standards to ensure that they are best fit for the positions in question and are consistent with business necessity. In addition, we ensure that prior to engagement in any trusted role, all personnel have the qualifications and necessary experience to perform such duties.

   TrustCor has full-time employees and resources dedicated to the CA business unit. Some examples of the CA operations staff training and certifications include:

   - SafeNet HSM Training
   - PrimeKey SignServer Training
   - Certified Internet Security Specialist
   - SonicWALL Systems Administrator Certification
   - Red Hat Server Administrator Certification
   - Microsoft Certified Professional Desktop & Server / MCSE Certification
   - Annual ID verification training for validation specialists
   - Many others…

3. **To what extent have CA personnel reviewed the CA incidents that have been reported in Bugzilla over the past several years? How have systems been designed to avoid similar mistakes?**

   Reviewing CA incidents reports on Mozilla's Bugzilla is part of TrustCor's compliance strategy. Our compliance team is tasked to monitor all Bugzilla items and meet to discuss relevance of issues to our CA. For example, https://bugzilla.mozilla.org/show_bug.cgi?id=1772644 led to a review of our CRL processes and how we described our actions in the CP and CPS. As a result of this review, we clarified our

actions in our documentation. We also develop and maintain our own software API for automating CA operations and make regular adjustments to this API based on incidents reported by/about other CAs and discussed in Bugzilla.

Whether the Applicant's Operations are Designed for Continued Compliance

1. **How are the CA's systems designed?**

   TrustCor's CA system is designed with reference to the relevant requirements of the CA/Browser Forum and IETF/RFC regulations to ensure the continuous improvement of our processes meeting security, quality and compliance requirements.

   Each service of the CA system is network-isolated in different firewall zones and VLAN'd to reduce risk, and requires 2FA. A log integrity and retention system ensures that system logs are sound, and monitoring systems are in place to track the security, availability, and performance of the CA at all times.

   TrustCor maintains separate development, staging, and production environments. TrustCor's structured architecture and compliance-based processes allow phased deployment (rollout), testing, and rollback.

2. **How well are CA processes documented and programmatically enforced for compliance with industry requirements?**

   All of TrustCor's practices and policies, related to operation and maintenance processes are documented thoroughly in accordance with the Baseline Requirements and WebTrust standards. Certificate issuance is fully automated with validation programmatically enforced. Many of our main CA processes are also programmatically enforced and include automated system and network audit logging; automated backup procedures, security monitoring, and vulnerability scanning; automated CRL issuance and OCSP responses; and partially automated configuration changes and patch management procedures.

3. **How does the applicant reduce operational risk and maintain an error-free, compliant operation?**

   TrustCor implements a variety of processes and procedures that are more strict than the industry requires. For example, TrustCor has issued DV SSL certificates for a maximum validity period of 398 days since 2016, long before it was standard practice. As mentioned earlier, TrustCor has dedicated personnel responsible for compliance which includes, but is not limited, to monitoring industry requirements and publicly reported incidents and TrustCor maintains separate development, staging, and production environments.

4. **What pre-issuance lint testing does the CA use? What other automation does the CA use to reduce risk?**

   TrustCor's pre-issuance process includes validation against various industry lint checks (zlint, certlint, x509Lint) to ensure certificate compliance before issuance. This linting is

also executed after CT logging of pre-certificates have been completed to make sure that the pre-certificates with embedded SCTs also comply with these linters.

TrustCor also uses automated validators to reduce risk. For each and every certificate request, we check the public key in the SKI against various databases and external services, such as: pwnkeys.com, roca, littleblackbox, debian-blacklist, and our own internal database of known compromised keys. We also try to factor the key with Fermat's factorization algorithm.

We do not cache CAA and zone delegation verifications, when certificates are issued for subdomains based on the ownership of a parent domain. We perform these checks for each and every certificate request.

Whenever a TrustCor issued certificate is revoked for "keyCompromise" reason, we automatically revoke certificates which share the same SKI to that of the certificate being revoked.

We issue new CRLs and OCSP responses within 2 hours (ideally within 30 minutes) of certificate revocation.

We keep identity verification challenge timeframes to as minimum as possible. Domain verification challenges are only valid for 48 hours and mailbox challenges are valid for 24 hours. All challenges have a unique challenge value (random value). Also, the domain/mailbox ownership verification is only valid 30 days; post which customers are required to provide the ownership again.

Organization and Individual verifications are valid for no more than 365 days. Anything post 365 days, customers are required to re-verify again.

We have an automated crt.sh checker to verify that the certificates published on crt.sh were actually issued by us. This helps to detect any mis-issuance of certificates.

We have developed a work-in-progress custom linter for S/MIME certificates to comply with the upcoming S/MIME BRs, since the above linters do not support S/MIME certificates yet.

5. **What mechanisms ensure that the CA system is agile to change when required for privacy, security, or compliance reasons?**

TrustCor’s CA systems are designed to comply with all current privacy, security, and compliance requirements in accordance with industry standards. Using our change management process, our dedicated CA compliance staff can quickly apply new configuration modifications and update software when necessary. All changes and deployments go through Q&A testing and approval before being applied into the production environment.

TrustCor's structured architecture and compliance-based processes allow phased deployment (rollout), testing, and rollback. Our platform is based on a microservice architecture that allows us to deploy specific components, reducing the risk and amount of change to the entire infrastructure.

Business logic is driven by user-defined configurations excepting compliance measures, which are hard-coded into service logic, which aids in rapid configuration updates.

6. **What is the quality of execution? What measures does the CA implement to quickly address compliance incidents?**

   If and when TrustCor CA becomes aware of a compliance incident, the TrustCor CA Security Incident Team is assigned to review, investigate, and respond to in a timely fashion. The incident team will also coordinate the relevant personnel to make the issuance known by submitting an incident Bug to Bugzilla including the description of the incident, listing the certificate identifiers involved (if applicable), a root cause analysis of the incorrect issuance, and the remediation steps taken to address the compliance issue.

   Once an incident has been investigated and remedial action scheduled and completed, a further review as to possible effects on other systems, or possible customer facing impacts is required by TrustCor's policies before marking the incident as resolved. Incidents will also be brought to the attention of auditors, once the incident has been closed, in order for the auditor to make a determination as to whether the incident impacts the perception of maintaining suitable controls.

Whether the Applicant has a Good Compliance Management Program

1. **How robust is the applicant's compliance and risk management program?**

   In addition to the public Certificate Policy and Certificate Practice Statement, TrustCor has a variety of internal policies and procedures in place covering everything from risk assessment, training, trusted roles and responsibilities to governance and protection of certificate information, confidentiality of customer data, integrity and availability of TrustCor CA's information and computing base. Personnel in trusted roles include a dedicated position for digital certificate compliance that works closely with oversight from TrustCor's Policy Authority. Technical enforcement of industry requirements have been implemented via linters, monitoring and self-audits.

   Additionally, TrustCor conducts periodic vulnerability scans and penetration tests, as required by NetSec (Network and Certificate System Security Requirements), on all CA systems. TrustCor treats, with high priority, all recommended changes originating from these systems/reports.

2. **What evidence can the applicant provide to demonstrate that it has a good compliance program in place? How long has such program been operational? On what compliance framework is it based?**

   TrustCor has had a dedicated compliance team and program in place since 2014. TrustCor's policies and practices are based on the following compliance framework: the latest versions of the Certificate Authority/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") and Network and Certificate System Security Requirements, the latest versions of WebTrust Principles and Criteria for Certification Authorities, WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security, and WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements, IETF RFC3647, and NIST 800-63.

3. **How familiar is the applicant with the annual risk assessment required by section 5 of the Baseline Requirements? (Note that it requires 1. the identification of foreseeable internal and external threats; 2. an assessment of the likelihood and potential damage of these threats; and 3. an assessment of the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.)**

   All of TrustCor's annual audits, both internal and external, include risk assessments. TrustCor has never missed an external audit, conducted by an accredited WebTrust auditor, since our first CA business unit audit in 2014. TrustCor's annual audits include all required elements.

4. **How does the applicant exercise care when deciding to take on risks? What are applicant's processes for mitigating or accepting risks?**

   TrustCor maintains an internal Risk Assessment Policy, with steps for our risk control team to perform on an annual basis, at minimum, to identity and rate all risks and evaluate the impact on TrustCor's business and CA. TrustCor's Policy Authority reviews all risks and votes to accept or reduce each risk. We record all acceptance decisions, together with a list of the individual assessments and rationales behind each.

Whether a Knowledgeable Third Party has Reviewed the CA Systems

1. **What initial assessments (e.g. a detailed controls review) have been conducted on CA systems? What criteria were used? Were assessments performed by a knowledgeable assessor?**

   TrustCor received pre-assessments for each of its CA business unit offerings prior to obtaining corresponding accreditations, and since has received annual audit reports incorporating the standards of WebTrust for CAs, CA/B Forum Baseline Requirements, and AICPA verified by a CPA Canada certified auditor.

2. **What are the auditor's qualifications for previous and current audit statements?**

   TrustCor's WebTrust audit is performed by Princeton Audit Group, Inc. ("PAG"), with the accreditation found here:

   https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/licensed-webtrust-practitioners-international

   PAG's lead auditor is Vijay Khosla and PAG's team of auditors carry CISA and CISM certifications and relevant in-house training.

   Average years of experience, in trust services or similar information systems, for the audit team includes 34 years in IT Audit Audits, 10 years in SOC 1,2,3 reporting, 5 years in SOX, 10 years in WebTrust Audits.

Qualifications include: over 10 years in: IT and Infrastructure Audit, SDLC and Risk Assessment; Data Center Audits; Encryption training; Cost Accounting Experience; Physical Security; Network Security; and Cloud Computing.

Credentials include: CPA, CISA, CISM, AICPA, CPA Canada

PAG audit team members are bound by law to comply with standards applicable to their respective qualifications and also as required for e.g. AICPA, CISA, CISM and CPA Canada.

As of TrustCor's 2021 audit period, PAG does not rely on any third-party specialists or affiliate audit firms.