What Kinds of Benefits can CommScope CA provide to Mozilla?

Communities served:

- Consumer users of mobile, broadband, and video devices (e.g., set-top boxes, cable modems, DSL modems, access points, mobile devices), service providers and manufacturers of such devices
    - We operate hundreds of private CAs that serve several tier-1 US providers of broadband and video (pay TV) services as well as CommScope
    - The certificates issued under these private CAs have been provisioned in hundreds of millions by CommScope's factory and field provisioning system into consumer devices such as digital set-top boxes, cable modems, home routers, and Wi-Fi extender devices
    - Users of such devices need to configure them via HTTPS through a browser, such as Firefox, or through a mobile app, which either fails or triggers security warnings when the device certificate is not issued by a trusted CA
    - Mozilla-trusted certificates would enable users to securely communicate with such devices with confidence, using a browser like Firefox or possibly other Mozilla products
    - CommScope has developed a bandwidth-saving video delivery solution in which a variety of devices downstream from a home gateway device can receive streaming content through the gateway through an HTTPS-protected interface on the gateway. With device certificates issued by a private CA, only devices specifically configured to trust the issuer will connect to a gateway. When device certificates are issued by a CA trusted by browsers and OS platforms, more devices and user applications (e.g. browsers) can be used for service access and device management.
- Consumers users of IoT ecosystems (e.g., smart home, medical devices and industrial IoT), service providers, manufacturers, and chip suppliers of such ecosystems
    - We are a private CA and operate a Matter root CA (PAA) for Legrand
    - We are partnering with STMicroelectronics to provision device certificates into a variety of IoT devices, include our device agent and proof of concept with certificate registration to AWS and Azure IoT controllers
    - Following approval we can provision Mozilla-trusted certificates to allow users to manage IoT devices with a Firefox browser and other products and services distributed and managed by Mozilla
- Users of containerized applications in public cloud and private Kubernetes-based cloud deployments
    - CommScope is currently field-provisioning end-entity certificates into containerized cloud applications; CommScope also provides a certificate

    - enrollment client integrated with white-box cryptography for private key protection
    - Publicly trusted certificates would enable users to manage containerized applications with a standard browser such as Firefox and possibly other Mozilla products

Quality of services offered:

- Capacity to provision over 30 billion device certificates annually in high-volume device manufacturing settings
- 24x7x365 monitored infrastructure with redundancy to ensure high availability
- Disaster recovery site compliant with CA/Browser Forum TLS Baseline Requirements and audited by an independent accredited auditor against WebTrust criteria
- Experienced no security breaches in over 25 years of operation

Risk management and risk reduction:

- Audited by an external, accredited auditor against WebTrust criteria, CA/Browser Forum TLS Baseline Requirements and other external ecosystem requirements for the last 5 years:
    - Risk management, vulnerability scanning, penetration testing and network security procedures
    - Staff members having "trusted person" status go through background checking before employment or transitioning into trusted roles
    - CA infrastructure housed in secure facilities protected with 4 or more layers of access-controlled physical perimeters, multi-person access control, motion sensors, 24x7 video surveillance, etc.

Lower rate of CA compliance incidents:

- We completed external audits against WebTrust and CableLabs for the last 5 years without any identified security breaches

Less time and effort needed for CA oversight:

- CommScope PKI Center has 25 years of accumulated experience in operating PKI services and managing certificate lifecycles, with fine-tuned processes and procedures.
- CommScope is already experienced with compliance to WebTrust and CA/Browser Forum TLS Baseline Requirements and have passed the corresponding external audits

Positive effects on Mozilla's reputation for privacy:

- CommScope take subscriber privacy very seriously and securely stores their private information in compliance with the confidentiality provisions of our CPS

Positive effects on Mozilla's reputation for security
Firefox user retention:

- See above regarding risk management and privacy
- Once our CA certificate is included in Mozilla's CA Certificate Program, the Firefox browser can be included as a recommended user application for securely accessing IoT devices, other CPE, and containerized services

Reasons Why Applicant is Applying for Inclusion

- Extend services to network operators to enable device configuration and management through Firefox and other Mozilla products
- To expand our PKI services to serve a broader customer base
- To expand the range of devices and applications that users can use to securely and seamlessly (without security warnings and the need for advanced configuration) access service delivery and device managements interfaces on CPE devices

Whether the Applicant Commits Sufficient Resources to Compliance

- We are an indirectly wholly-owned subsidiary of CommScope Holdings Company, Inc.
- CommScope PKI Center's staff includes 32 trusted persons; the PKI Center also has dedicated business and legal support from the business unit and CommScope Corporate
- CommScope already has long-term contracts to provide CA services that require WebTrust audits under CableLabs root and for WInnForum ecosystem and plan continue CA management and external audits into the foreseeable future
- Our CA has already been externally audited against CA/Browser Forum TLS Baseline requirements and our plan is to continue their operation for the long term – as long as we are able to obtain browser approvals
- To assure our customers the safety of their data and to avoid any appearance of conflict of interest, CommScope PKI Center has its own IT resources and IT department, separate from CommScope corporate IT resources. The PKI Center's IT department has operational autonomy and reports to different management than CommScope corporate IT.

Whether the Applicant Employs Skilled Personnel

- Our CA personnel have over 20 years of experience in PKI design, software development, deployment, ongoing security operations and managements.
- Our CA personnel regularly monitor CA/Browser Forum and Mozilla reflectors and their updated requirements. For example:
  - We have investigated, and have put on our roadmap, testing RSA public keys for ROCA vulnerability and vulnerability to Fermat's factorization method.
  - CommScope CA performs tests on public keys for Debian weak keys
  - We are monitoring advances in quantum computers, the future threat of breaking ECDSA and RSA crypto based on Shor's algorithm and NIST's standardization of quantum-safe public key algorithms
- Our CA personnel also monitor root CA program requirements from other browser developers, including Microsoft, Google and Apple.
- We have several Trusted Persons who are very familiar and follow CABF and IETF standards as well as train others within our department to ensure expertise is maintained for business continuity. We are very familiar with IETF standards that include OCSP, ACME, CMPv2, RFC 5280, RFC 9162 (certificate transparencies), etc.
- Our CA personnel have also been periodically monitoring Bugzilla incident reports at https://bugzilla.mozilla.org/query.cgi?format=advanced – monitoring bug reports related to CA compliance. CommScope performs certificate linting to verify correctness, as well as periodic internal audits of logs and issued certificates to identify any potential issues.

Operations are Designed for Continued Compliance

- CommScope CA infrastructure includes front-end and back-end systems.
  - Back-end infrastructure (including HSMs) is on an isolated network behind an additional firewall
  - Both back-end and front-end are housed inside multiple nested physical security perimeters protected by such security measures as multi-factor physical access control, multi-person control, motion sensors, and 24x7 video surveillance
  - Front-end is reachable from the Internet, but clients are authenticated with 2-factor authentication involving cryptographic hardware tokens
- Our CA operational processes and procedures are well-documented and strictly followed and audited annually by accredited external auditors against WebTrust criteria.
- Examples of pre-issuance validation and automation:

  - CSR validation, including DNS CAA record checking, is performed programmatically
  - We use the validation software (zlint) to check samples of certificates generated for a new customer account
  - Our software validates each submitted CSR against an applicable XML-based template, which specifies validity constraints a CSR for a particular type of certificate must satisfy.
- Publicly trusted certificate compliance is our top priority and when privacy, compliance or security issues arise we focus our development team to quickly address such issues with our agile software development process.
  - Our CA software has been architected based on the principles of modularity and mechanism-policy separation. Modular design enables components of our system to be modified independently most of the time, and generally tends to limit scope of the components that need to be modified to implement new requirements.
  - Separation between mechanism and policy allows many policy changes to be accommodated by configuration changes rather than code changes.
- CA system requirements are reviewed by development team, code is then reviewed for compliance with each new requirement in a software release and then tested by our dedicated QA staff.

Compliance Management Program

- CommScope CA application and system logs are reviewed annually by our internal external compliance auditors and resulted in very few compliance issues that were addressed to the satisfaction of both. Revocation was invoked as needed.
- Our compliance is based on our CommScope CP/CPS, WebTrust criteria, CA/Browser Forum TLS Baseline Requirements, as well as browser maker-specific trusted root CA program requirements. The most recent auditor reports can be downloaded through the WebTrust seals at https://www.pki-center.com/solutions/certificate-authority and past auditor reports are available upon request.
- We take a proactive approach to security by monitoring entities such as NVD, CISA & SANS for new & existing threats. Our risk assessment evaluates the threat landscape by identifying the risk, categorizing it, ranking the likeliness and severity of the impact and whether the threat was realized. Then we further evaluate what controls are in place to reduce the risk and if any other controls are required to control risk at an acceptable level. We track the residual risk and review each threat annually. The annual risk assessment also addresses the security policies, documentation and technology currently being used and whether it is sufficient for the current threat landscape. We have a security team that meets weekly to discuss

a variety of issues that affect the security of the PKI Center, including whether and how to proceed with taking on new risks.

External Audits by a Qualified Compliance Auditor

- A number of CAs we operate have been annually audited by BDO against WebTrust criteria, our CPS, and other external requirements
- Our CAs have also been audited against the CA/Browser Forum TLS Baseline Requirements for the last 2 years
- BDO is well-known in the industry and has audited other publicly trusted CAs in addition to CommScope. Information about BDO’s WebTrust audit practice can be found at: https://www.bdo.com/insights/assurance/bdo-knows-webtrust-for-certification-authorities.