IdenTrust CA Value – Mozilla

1 Whether the Applicant Commits Sufficient Resources to Compliance

- **Compliance Resources:**
  IdenTrust assigns dedicated resources to manage incidents from discovery through resolution, ensuring accountability and transparency. A SWAT team is in place for incident response, including Tech Ops, Bus Ops, Development, QA, and Management.
- **Compliance Budget:**
  Budget is in place to handle annual audits (WebTrust, SOC 2), continuous monitoring, and internal dedicated resources to manage CA/B F. compliance activities.
- **System Development Resources:**
  Development teams are actively involved in compliance processes, including linting updates and automation for certificate lifecycle management.
- **Long-Term Commitment:**
  IdenTrust's roadmap aligns with CA community goals, focusing on enhanced security, governance, and automation. We plan roots 3–5 years in advance and maintain continuous audit cycles.

2. Who are the Applicant's Beneficial Owners?

- IdenTrust is part of **HID Global**, which is the beneficial owner.

3 . Applicant's Investment in CA Infrastructure and Personnel

- IdenTrust Operates two trusted roots and is planning nine additional single-purpose roots.
- IdenTrust maintains global operations with offices in the U.S. and Europe.
- IdenTrust have in place dedicated teams for compliance, risk management, and development

4. Applicant's Long-Term Commitment

- Replacement roots are generated at least five years before expiration.
- Continuous participation in CA/B Forum and contribution to open-source ACME clients (Caddy, ACME.sh).
- Plans to implement ACME-compliant domain validation.

5. System Development Resources for Compliance

- Pre-issuance and post-issuance linting using **Zlint** and **PKIlint**.
- Automated blocking of issuance if linting fails.
- Updates to linting configurations within 90 days of release.

5. CA's Compliance Budget and Constraints

- Compliance activities include annual WebTrust and SOC 2 audits, internal audits, and risk assessments.
- We do not have constraints that would hamper compliance.

7 Whether the Applicant Employs Skilled Personnel

- Active CA/B Forum participation with engineering and infrastructure teams.
- Personnel familiar with CABF and IETF standards; development team monitors linter updates and RFC 5280 alignment.
- Risk management and compliance teams conduct annual assessments.

8 Review of CA Incidents and System Design

- SWAT team handles incidents with root cause analysis and revocation timelines.
- Incident disclosure within 72 hours and full report within 14 days.
- Systems designed for automation and error prevention (linting, change control).

9 Operations Designed for Continued Compliance

- Documented processes are reviewed annually.
- Automated linting pre- and post-issuance.
- Change control process for updates within 90 days.
- SLA-driven communication strategy for changes.

10 Compliance Management Program

- Based on WebTrust and SOC 2 frameworks.
- Annual risk assessments per Baseline Requirements section 5.
- Independent internal audits of non-accounting functions.

11 Knowledgeable Third-Party Review

- Annual audits under WebTrust and SOC 2 by qualified auditors.
- Continuous audit periods with no gaps.