WebTrust for CA - Auditee Views

Vijayakumar Manjunatha, eMudhra

WebTrust has been a Framework for a Globally Recognizable CA Setup.

Only other alternative is ETSI EN 319 411 (1 and 2), which is adopted by Europe.

emudhra
Trust Delivered

Areas Covered

The WebTrust for CAs program includes the principles listed below. Underlying each principle, there are a series of supporting criteria to which the CA has to conform.

1. CA Business Practice Disclosure (CP/CPS)
    - The Certification Authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices.
2. Service Integrity
    - Subscriber information was properly authenticated (for the registration activities performed by the CA) and
    - The integrity of keys and certificates it manages is established and protected throughout their life cycles.
3. CA Environmental Controls
    - Subscriber and relying party information is restricted and protected
    - Continuity of key and certificate management operations is maintained
    - CA systems development, maintenance and operation are properly authorized and performed to maintain CA systems integrity

Summary of WebTrust for CAs Criteria Topics

CA BUSINESS PRACTICES DISCLOSURE (CP/CPS)		
CA ENVIRONMENTAL CONTROLS	CA KEY MANAGEMENT	CERTIFICATE LIFE CYCLE MANAGEMENT
• CP/CPS Management • Security Management • Asset Classification and Management • Personnel Security • Physical and Environmental Security • Operations Management • System Access Management • Systems Development and Maintenance • Business Continuity Management • Monitoring and Compliance • Event Journaling	• CA Key Generation • CA Key Storage Backup and Recovery • CA Key Escrow (optional) • CA Key Usage • CA Key Archival • CA Key Destruction • CA Cryptographic Device Life Cycle Management • CA-Provided Subscriber Key Management Services (optional)	• Subscriber Registration • Certificate Rekey/ Renewal Certificate Issuance • Certificate Distribution • Certificate Revocation • Certificate Suspension (optional) • Certificate Status Information Processing • Integrated Circuit Card Life Cycle Management (optional)

**Indicative list only

emudhra Trust Delivered

The Audit Process: Participants

Personnel responsible for	Involvement typically includes	Level of involvement
• Security management • Personnel • Physical security • IT operations (e.g., network and system security, monitoring, change management) • CA business continuity management • CA key management operations • Registration authority activities	• Participation in interviews to discuss CA processes • Responding to requests for documented policies/procedures, lists of events occurring during the period, and supporting evidence for a sample of events selected by the auditor	• Typically the CA assigns an audit coordinator who spends 25 – 50% of their time coordinating meetings and the gathering of audit evidence during the fieldwork phase of the audit. • Other individuals are typically involved for a small portion of focused time.

Key areas of Importance for Auditees

1. **Functioning of Policy Authority**: Decision making for policy & practice change, supervision of audits, security report, etc.
2. **Services Isolation**: For separation of services like CM, TSA, OCSP, etc. And also the application/security layer like the database, HSM, etc
3. **Redundancy architecture / Fault Tolerance**: To have critical services to tolerate local failures, and hence capacity planning should provide zero downtime and operate in a buffer.
4. **Time Synchronization**: Importance to have accuracy of time across CA Infra with reliable time source.
5. **Performance & availability for critical services**: Uptime and response times of services like OCSP and CRLs.
6. CA Facility Administrative and Access Ownership.
7. Primary and DR Setup (BCP).
8. Certificate Linting Requirements
9. Incident Management mechanism & reporting.
10. Internal Audits and results.
11. Risk detection mechanism (Prominent Companies, Countries of suspicion, blacklists of UN / Terror / etc)
12. Weak key detection (Compromised keys / Weak keys)

India | Europe | USA | Mauritius | Singapore | UAE | Indonesia

Thank you!

eMudhra enables governments, enterprises and consumers to engage, exchange information and transact securely, efficiently and with enhanced customer experience.