WebTrust Security Framework for CCA

Principles and Criteria for Certification Authorities

C-DAC Bangalore

Introduction to WebTrust

- **Trust Services:** Audit and assurance services.
- Set of principles and criteria put forth jointly by AICPA and CICA.
- WebTrust taskforce is an associate member of CA|B forum.
- Consistent with standards developed by the American National Standards Institute (ANSI), International Organization for Standardization (ISO), and Internet Engineering Task Force (IETF).

Trust Services Principles

- **Security**: The system is protected, both logically and physically, against unauthorized access.
- **Availability**: The system is available for operation and use as committed or agreed to.
- **Processing Integrity**: System processing is complete, accurate, timely, and authorized.
- **Confidentiality**: Information that is designated "confidential" is protected as committed or agreed.
- **Privacy**: Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with the privacy principles

WebTrust Audit Schemes

Scheme	Version	Release Date
WebTrust for CA	2.2.1	1-Nov-20
WebTrust for CA	2.2.2	1-Jun-21
WebTrust for CA - Extended Validation - SSL	1.7.3	1-Nov-20
WebTrust for CA - Extended Validation - SSL	1.7.8	31-Jan-22
WebTrust for CA - SSL Baseline with Network Security	2.5	1-Nov-20
WebTrust for CA - SSL Baseline with Network Security	2.6	31-Jan-22
WebTrust for CA - Code Sign Baseline Requirements	2.0	1-Nov-20
WebTrust for CA - Code Sign Baseline Requirements	2.7	31-Jan-22
WebTrust for CA- Verified Mark Certificates	1.0	1-Dec-21
WebTrust for RA	1.1	1-Nov-20

Intended Use of the WebTrust Principles and Criteria

- The WebTrust Principles and Criteria for CAs can be used as a control framework to assess the adequacy of the CA systems, policies and procedures.
- It provides a basis for self-assessment for either development or maintaining strong PKI systems.
- Assessors / practitioners can use the framework as a benchmark for performing an internal or independent assessment.

Principles and Criteria for Certification Authorities

- **CA business practices disclosure:** Disclosure of key and Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement & Certificate Policy

  CP and CPS documents in accordance with *IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

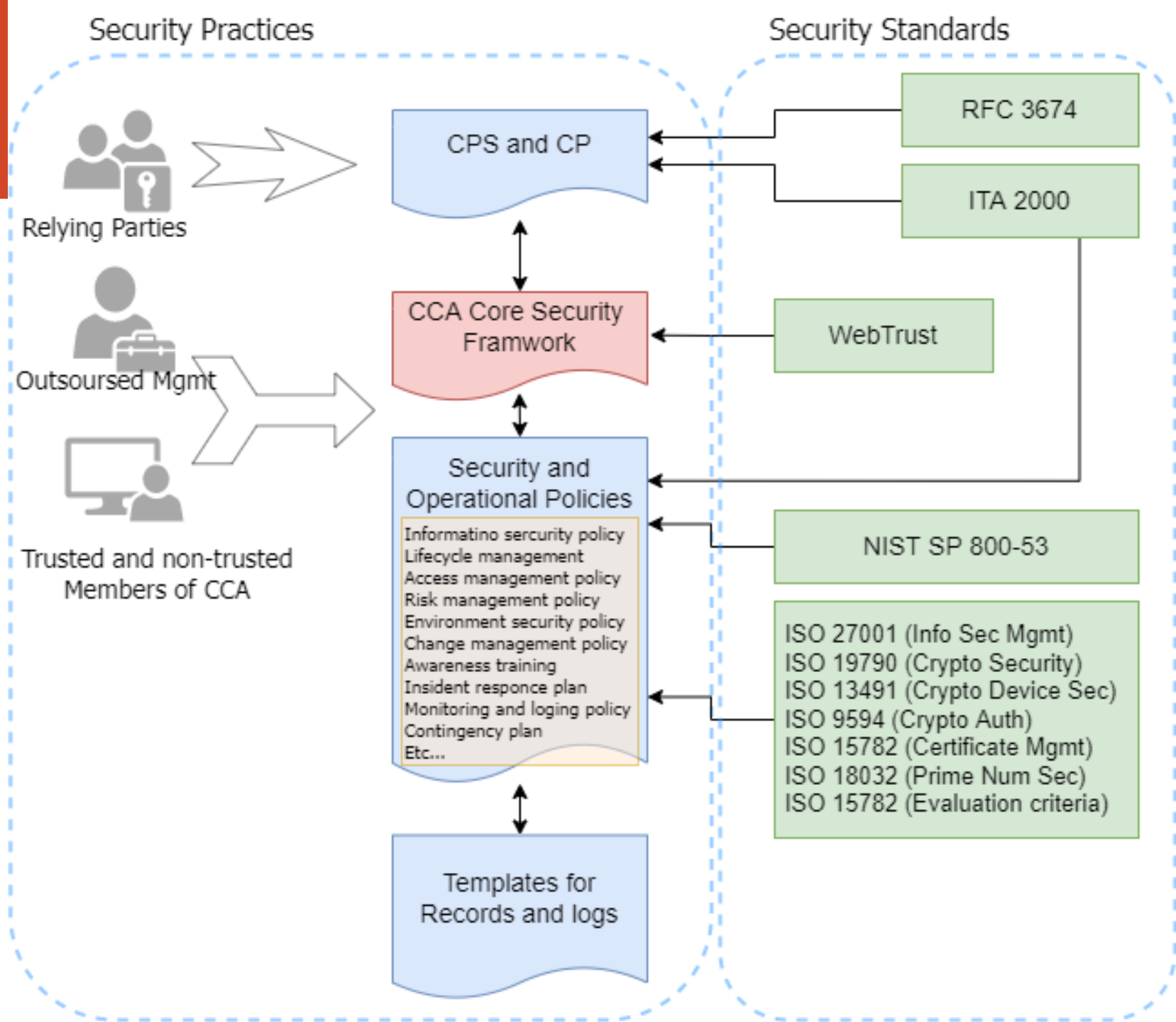
- **Service integrity:** The integrity of keys and certificates it manages is established and protected throughout their life cycles

- **CA environmental controls:** Logical and physical access to CA systems & data is restricted and CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity

Criteria and Illustrative Controls

1. Business Practices Disclosure (2 Disclosers)
2. Business Practices Management (3 Criteria, 15 Illustrative controls)
3. CA Environmental Controls (28 Criteria, 151 Illustrative controls)
4. CA Key Lifecycle management Controls (12 Criteria, 68 Illustrative controls)
5. Subscriber Key Lifecycle Controls (19 Criteria, 64 Illustrative controls)
6. Certificate Lifecycle management (10 Criteria, 97 Illustrative controls)
7. Subordinate CA and Cross Certificate Lifecycle management Controls (7 Criteria, 13 Illustrative controls)

Security framework Architecture for CCA



Core Security Framework

- Security activities and controls organized and customized based on WebTrust Principles and Criteria.
- Designed to cover the breadth of security objectives for CCA, while not being detailed.
- Refers to policy and procedure for depth of security objectives which are derived with standard references from ISO, NIST and ITA.

Policy and procedures

1. Information Security Management
2. Asset Management
3. Human Resources Security
4. Physical and Environmental Security
5. Media and Operations Management
6. Access Control Management
7. Maintenance and Change management.
8. Business Continuity Management
9. Monitoring and logging policy
10. Risk Management
11. Roles and responsibility
12. Incident Management
13. Incident response procedure
14. Key lifecycle management
15. Certificate lifecycle management
16. Awareness and Training

CA Environmental Controls / Security Management

Criteria	Illustrative Controls	Policy and procedures with Informative Reference
Information security policy	• An information security policy document published and communicated • information security, its overall objectives and scope, and the importance • review process for maintaining the information security policy	Information Security Management PL-1 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
Information security infrastructure	• Management support to manage risks • Responsibilities for the protection of individual assets • process for new information processing	Information Security Management PM-2, PM-6, PM-29 5.1, 5.3, 9.2, A.6.1.1
Security of third party access	• Enforced to control physical and logical access by third parties • Risk assessment is performed to determine specific control requirements. • Formal contract containing necessary security requirements.	Information Security Management PE-2,PE-3,RA-3 A.12.6.1, A.11.1.1, A.11.1.2, A.11.1.13 Risk Management RA-3 6.1.2, 8.2

CA Environmental Controls / System Access Management

Criteria	Illustrative Controls	Policy and procedures with Informative Reference
User access management	• Roles, access permissions, authentication process and segregation of duties • procedure for access to systems software and network devices • Authentication procedure and privilege management	Roles and responsibility Asset Management
Network access control	• Access is authorized and controlled • Routing control and Isolation from any other domain • System configuration and compliance • Data confidentiality during transit	Asset Management Physical and Environmental Security Maintenance and Change management.
System software and network device access control	• Periodic review and update of System configuration • Patch management based on risk assessment • Secure login process • Unique User identification and individual accountability	Maintenance and Change management. Access Control Management
Application access control	• Application system functions are restricted • CA personnel are successfully identified and authenticated • Dedicated and isolated compute environment for Root CA	Access Control Management Physical and Environmental Security

Thank you