Comparison of the new RFC to RFC 2527

Changes From RFC 2527

This framework represents an incremental improvement over RFC 2527. The new framework benefits from the experience gained in the course of deploying CP and CPS documents under RFC 2527. Further, this new framework is based on coordination with the American Bar Association Information Security Committee within the Section of Science and Technology Law. The ISC wrote the PKI Assessment Guidelines [ABA2], which embodies a great deal of technical, business, and legal experience in PKI operations. In particular, representatives of the ISC made changes to the framework to make it better suited to the legal environment and more accessible to lawyers.

From a technical perspective, the changes to the RFC 2527 framework were minimal and incremental, rather than revolutionary. Sections 3-7 have largely been preserved, with modest reorganization and new topics. For example, the new framework includes a revision of Section 4 of the framework to include a full treatment of the certificate life-cycle, the addition of key escrow, key encapsulation, and key recovery policies and practices, and OCSP. Section 2 audit functions now appear alone in Section 8, and Section 2 focuses exclusively on repository functions. The business and legal matters in RFC 2527's Section 2 now appear in a new Section 9.

From a legal perspective, the new Section 9 is useful because it places topics in the framework in an ordering that is similar to software licensing and other technology agreements and thus is familiar to technology lawyers. Moreover, the framework as a whole can double as a framework for a subscriber, relying party, or other PKI-related agreement. The changes are intended to make legal review of, and input into, CP and CPS documents more efficient. Section 9 also adds new legal topics, such as the privacy of personal information, liability terms, and duration of the effectiveness of the document.

Section 1 of the new framework is largely the same as RFC 2527, although it increases coverage of PKI participants by breaking out subscribers from relying parties and adding a section for other participants. It changes the "applicability" section to one covering appropriate and prohibited uses of certificates. Also, it moves CPS approval procedures from RFC 2527's Section 8.3 into a collected policy administration section. Finally, Section 1.6 adds a place to list definitions and acronyms.

Section 2 of the new framework is a reorganization of Section 2.6 of the old framework. Section 3 of the new framework is based on a division of the old Section 3.1 into two parts for naming and identification and authentication issues. It adds new issues, such as the permissibility of pseudonyms and anonymity. Old Section 4 topics on audit logging, records archival, key changeover, compromise and disaster recovery, and CA termination have moved to Section 5. The remaining Section 4 topics have been expanded and reorganized to cover a complete certificate lifecycle. New topics include items implicit in the RFC 2527 Section 4, but now

explicit, such as certificate application processing, certificate modification, and the end of subscription.

New Sections 5.1 through 5.3 are almost identical to their counterparts in RFC 2527. The remainder of the new Section 5 is the topics moved from RFC 2527's Section 4, in the order that they had appeared in Section 4. Section 6 of the new framework is almost the same as the old Section 6, with some exceptions, such as the consolidation of old Section 6.8 (cryptographic module engineering controls) into Section 6.2.1 (now called "cryptographic module standards and controls") and the addition of time-stamping in a new Section 6.8. Section 7 is almost identical to the old Section 7, the major change being the addition of a section covering OCSP profile. Section 8 is almost identical to RFC 2527's Section 2.7.

New Section 9 contains business and legal topics that had been covered in RFC 2527's Section 2, including fees, financial responsibility, confidentiality, and intellectual property. It adds a section on the privacy of personal information, which has become a significant policy issue. The "liability" Section 2.2 in RFC 2527 now appears in Sections 9.6 through 9.9, covering representations and warranties, disclaimers, limitations of liability, and indemnities. Section 9.10 adds a section concerning the duration of the effectiveness of documentation. Section 9.12 collects terms concerning the way in which a document (CP, CPS, agreement, or other document) may be amended, formerly appearing in Section 8.1. Section 9 includes "legal boilerplate" topics, some of which had been in the old Section 2. Finally, Section 9.17 is a catch-all "other provisions" section where drafters can place information that does not fit well into any other section of the framework.

The following matrix shows the sections in the old RFC 2527 framework and their successor sections in the new framework.

Current CP		***New CP***
1.	***Introduction***	1.
1.1	***Overview***	1.1
1.2	***Identification***	1.2
1.3	***Community and Applicability***	1.3
1.3.1	***Certification Authorities***	1.3.1
1.3.2	***Registration Authorities***	1.3.2
1.3.3	***End entities***	1.3.3, 1.3.4
1.3.4	***Applicability***	1.4, 4.5
1.4	***Contact Details***	1.5
1.4.1	***Specification Administration Organization***	1.5.1
1.4.2	***Contact Person***	1.5.2
1.4.3	***Person Determining CPS Suitability for the Policy***	1.5.3
2.	***General Provisions***	2, 8, 9
2.1	***Obligations***	2.6.4
2.1.1	***CA Obligations***	Integrated throughout entire framework
2.1.2	***RA Obligations***	Integrated throughout portions of the framework that apply to RAs
2.1.3	***Subscriber Obligations***	4.1.2, 4.4, 4.5, 4.5.1, 4.6.5, 4.7.5, 4.8.1, 4.8.5, 4.9.1, 4.9.2, 4.9.13, 4.9.15, 5., 6., 9.6.3, 9.9

	Current CP	New CP
2.1.4	***Relying Party Obligations***	4.5, 4.5.2, 4.9.6, 5., 6., 9.6.4, 9.9
2.1.5	***Repository Obligations***	2., 4.4.2, 4.4.3, 4.6.6, 4.6.7, 4.7.6, 4.7.7, 4.8.6, 4.8.7
2.2	***Liability***	9.6, 9.7, 9.8, 9.9
2.2.1	***CA Liability***	9.6.1, 9.7., 9.8, 9.9
2.2.2	***RA Liability***	9.6.2, 9.7, 9.8, 9.9
2.3	***Financial Responsibility***	9.2
2.3.1	***Indemnification by Relying Parties***	9.9
2.3.2	***Fiduciary Relationships***	9.7
2.4	***Interpretation and Enforcement***	9.16
2.4.1	***Governing Law***	9.14, 9.15
2.4.2	***Severability, Survival, Merger, Notice***	9.10.3, 9.11, 9.16.1, 9.16.3
2.4.3	***Dispute Resolution Procedures***	9.13, 9.16.4
2.5	***Fees***	9.1
2.5.1	***Certificate Issuance or Renewal Fees***	9.1.1
2.5.2	***Certificate Access Fees***	9.1.2
2.5.3	***Revocation or Status Information Access Fees***	9.1.3
2.5.4	***Fees for Other Services Such as Policy Information***	9.1.4
2.5.5	***Refund Policy***	9.1.5
2.6	***Publication and Repository***	2.
2.6.1	***Publication of CA Information***	2.2, 4.4.2, 4.4.3, 4.6.6, 4.6.7, 4.7.6, 4.7.7, 4.8.6, 4.8.7
2.6.2	***Frequency of Publication***	2.3
2.6.3	***Access Controls***	2.4
2.6.4	***Repositories***	2.1
2.7	***Compliance Audit***	8.
2.7.1	***Frequency of Entity Compliance Audit***	8.1
2.7.2	***Identity/Qualifications of Auditor***	8.2
2.7.3	***Auditor's Relationship to Audited Party***	8.3
2.7.4	***Topics Covered by Audit***	8.4
2.7.5	***Actions Taken as a Result of Deficiency***	8.5
2.7.6	***Communications of Results***	8.6
2.8	***Confidentiality***	9.3, 9.4
2.8.1	***Types of Information to be Kept Confidential***	9.3.1, 9.4.2
2.8.2	***Types of Information Not Considered Confidential***	9.3.2, 9.4.3
2.8.3	***Disclosure of Certificate Revocation/Suspension Information***	9.3.1, 9.3.2, 9.3.3, 9.4.2, 9.4.3, 9.4.4
2.8.4	***Release to Law Enforcement Officials***	9.3.3, 9.4.6
2.8.5	***Release as Part of Civil Discovery***	9.3.3, 9.4.6
2.8.6	***Disclosure Upon Owner's Request***	9.3.3, 9.4.7
2.8.7	***Other Information Release Circumstances***	9.3.3, 9.4.7
2.9	***Intellectual Property Rights***	9.5
3.	***Identification and Authentication***	3.
3.1	***Initial Registration***	3.1, 3.2
3.1.1	***Type of Names***	3.1.1
3.1.2	***Need for Names to be Meaningful***	3.1.2, 3.1.3
3.1.3	***Rules for Interpreting Various Name Forms***	3.1.4
3.1.4	***Uniqueness of Names***	3.1.5
3.1.5	***Name Claim Dispute Resolution Procedure***	3.1.6
3.1.6	***Recognition, Authentication, and Role of Trademarks***	3.1.6
3.1.7	***Method to Prove Possession of Private Key***	3.2.1
3.1.8	***Authentication of Organization Identity***	3.2.2
3.1.9	***Authentication of Individual Identity***	3.2.3
3.2	***Routine Rekey***	3.3.1, 4.6, 4.7

	Current CP	New CP
3.3	*Rekey After Revocation*	3.3.2
3.4	*Revocation Request*	3.4
4.	*Operational Requirements*	4., 5.
4.1	*Certificate Application*	4.1, 4.2, 4.6, 4.7
4.2	*Certificate Issuance*	4.2, 4.3, 4.4.3, 4.6, 4.7, 4.8.4, 4.8.6, 4.8.7
4.3	*Certificate Acceptance*	4.3.2, 4.4, 4.6, 4.7, 4.8.4-4.8.7
4.4	*Certificate Suspension and Revocation*	4.8, 4.9
4.4.1	*Circumstances for Revocation*	4.8.1, 4.9.1
4.4.2	*Who Can Request Revocation*	4.8.2, 4.9.2
4.4.3	*Procedure for Revocation Request*	4.8.3-4.8.7, 4.9.3
4.4.4	*Revocation Request Grace Period*	4.9.4
4.4.5	*Circumstances for Suspension*	4.9.13
4.4.6	*Who Can Request Suspension*	4.9.14
4.4.7	*Procedure for Suspension Request*	4.9.15
4.4.8	*Limits on Suspension Period*	4.9.16
4.4.9	*CRL Issuance Frequency (If Applicable)*	4.9.7, 4.9.8, 4.10
4.4.10	*CRL Checking Requirements*	4.9.6, 4.10
4.4.11	*On-Line Revocation/Status Checking Availability*	4.9.9, 4.10
4.4.12	*On-Line Revocation Checking Requirements*	4.9.6, 4.9.10, 4.10
4.4.13	*Other Forms of Revocation Advertisements*	4.9.11, 4.10
4.4.14	*Checking Requirements for Other Forms of Revocation Advertisements*	4.9.6, 4.9.11, 4.10
4.4.15	*Special Requirements re Key Compromise*	4.9.12
4.5	*Security Audit Procedures*	5.4
4.5.1	*Types of Event Recorded*	5.4.1
4.5.2	*Frequency of Processing Log*	5.4.2
4.5.3	*Retention Period for Audit Log*	5.4.3
4.5.4	*Protection of Audit Log*	5.4.4
4.5.5	*Audit Log Backup Procedures*	5.4.5
4.5.6	*Audit Collection System (Internal vs. External)*	5.4.6
4.5.7	*Notification to Event-Causing Subject*	5.4.7
4.5.8	*Vulnerability Assessments*	5.4.8
4.6	*Records Archival*	5.5
4.6.1	*Types of Records Archived*	5.5.1
4.6.2	*Retention Period for Archive*	5.5.2
4.6.3	*Protection of Archive*	5.5.3
4.6.4	*Archive Backup Procedures*	5.5.4
4.6.5	*Requirements for Time-Stamping of Records*	5.5.5
4.6.6	*Archive Collection System (Internal or External)*	5.5.6
4.6.6	*Procedures to Obtain and Verify Archive Information*	5.5.7
4.7	*Key Changeover*	5.6
4.8	*Compromise and Disaster Recovery*	5.7, 5.7.1
4.8.1	*Computing Resources, Software, and/or Data Are Corrupted*	5.7.2
4.8.2	*Entity Public Key is Revoked*	4.9.7, 4.9.9, 4.9.11
4.8.3	*Entity Key is Compromised*	5.7.3
4.8.4	*Secure Facility After a Natural or Other Type of Disaster*	5.7.4
4.9	*CA Termination*	5.8
5.	*Physical, Procedural, and Personnel Security Controls*	5.
5.1	*Physical Controls*	5.1
5.1.1	*Site Location and Construction*	5.1.1
5.1.2	*Physical Access*	5.1.2
5.1.3	*Power and Air Conditioning*	5.1.3
5.1.4	*Water Exposures*	5.1.4
5.1.5	*Fire Prevention and Protection*	5.1.5

	Current CP	New CP
5.1.6	*Media Storage*	5.1.6
5.1.7	*Waste Disposal*	5.1.7
5.1.8	*Off-Site Backup*	5.1.8
5.2	*Procedural Controls*	5.2
5.2.1	*Trusted Roles*	5.2.1, 5.2.4
5.2.2	*Number of Persons Required per Task*	5.2.2, 5.2.4
5.2.3	*Identification and Authentication for Each Role*	5.2.3
5.3	*Personnel Controls*	5.3
5.3.1	*Background, Qualifications, Experience, and Clearance Requirements*	5.3.1
5.3.2	*Background Check Procedures*	5.3.2
5.3.3	*Training Requirements*	5.3.3
5.3.4	*Retraining Frequency and Requirements*	5.3.4
5.3.5	*Job Rotation Frequency and Sequence*	5.3.5
5.3.6	*Sanctions for Unauthorized Actions*	5.3.6
5.3.7	*Contracting Personnel Requirements*	5.3.7
5.3.8	*Documentation Supplied to Personnel*	5.3.8
6.	*Technical Security Controls*	6.
6.1	*Key Pair Generation and Installation*	6.1
6.1.1	*Key Pair Generation*	6.1.1
6.1.2	*Private Key Delivery to Entity*	6.1.2
6.1.3	*Public Key Delivery to Certificate Issuer*	6.1.3
6.1.4	*CA Public Key Delivery to Users*	6.1.4
6.1.5	*Key Sizes*	6.1.5
6.1.6	*Public Key Parameters Generation*	6.1.6
6.1.7	*Parameter Quality Checking*	6.1.6
6.1.8	*Hardware/Software Key Generation*	6.1.1
6.1.9	*Key Usage Purposes (as per X.509 v3 Key Usage Field)*	6.1.9
6.2	*Private Key Protection*	6.2
6.2.1	*Standards for Cryptographic Module*	6.2.1
6.2.2	*Private Key (n out of m) Multi-Person Control*	6.2.2
6.2.3	*Private Key Escrow*	6.2.3
6.2.4	*Private Key Backup*	6.2.4
6.2.5	*Private Key Archival*	6.2.5
6.2.6	*Private Key Entry Into Cryptographic Module*	6.2.6, 6.2.7
6.2.7	*Method of Activating Private Key*	6.2.8
6.2.8	*Method of Deactivating Private Key*	6.2.9
6.2.9	*Method of Destroying Private Key*	6.2.10
6.3	*Other Aspects of Key Pair Management*	6.3
6.3.1	*Public Key Archival*	6.3.1
6.3.2	*Usage Periods for the Public and Private Keys*	6.3.2
6.4	*Activation Data*	6.4
6.4.1	*Activation Data Generation and Installation*	6.4.1
6.4.2	*Activation Data Protection*	6.4.2
6.4.3	*Other Aspects of Activation Data*	6.4.3
6.5	*Computer Security Controls*	6.5
6.5.1	*Specific Computer Security Technical Requirements*	6.5.1
6.5.2	*Computer Security Rating*	6.5.2
6.6	*Life Cycle Technical Controls*	6.6
6.6.1	*System Development Controls*	6.6.1
6.6.2	*Security Management Controls*	6.6.2
6.6.3	*Life Cycle Security Controls*	6.6.3
6.7	*Network Security Controls*	6.7
6.8	*Cryptographic Module Engineering Controls*	6.2.1, 6.2, 6.2.1, 6.2.11
7.	*Certificate and CRL Profiles*	7.

	Current CP	New CP
7.1	*Certificate Profile*	7.1
7.1.1	*Version Number(s)*	7.1.1
7.1.2	*Certificate Extensions*	7.1.2
7.1.3	*Algorithm Object Identifiers*	7.1.3
7.1.4	*Name Forms*	7.1.4
7.1.5	*Name Constraints*	7.1.5
7.1.6	*Certificate Policy Object Identifier*	7.1.6
7.1.7	*Usage of Policy Constraints Extension*	7.1.7
7.1.8	*Policy Qualifiers Syntax and Semantics*	7.1.8
7.1.9	*Processing Semantics for the Critical Certificate Policies Extension*	7.1.9
7.2	*CRL Profile*	7.2
7.2.1	*Version Number(s)*	7.2.1
7.2.2	*CRL and CRL Entry Extesions*	7.2.1
8.	*Specification Administration*	N/A
8.1	*Specification Change Procedures*	9.12
8.2	*Publication and Notification Policies*	2.2, 2.3
8.3	*CPS Approval Procedures*	1.5.4

The following matrix shows the sections in the new framework and the sections in RFC 2527 to which the headings in the new framework correspond.

	New RFC Section	RFC 2527 Section
1.	*Introduction*	1.
1.1	*Overview*	1.1
1.2	*Document Name and Identification*	1.2
1.3	*PKI Participants*	1.3
1.3.1	*Certification Authorities*	1.3.1
1.3.2	*Registration Authorities*	1.3.2
1.3.3	*Subscribers*	1.3.3
1.3.4	*Relying Parties*	1.3.3
1.3.5	*Other Participants*	N/A
1.4	*Certificate Usage*	1.3.4
1.4.1	*Appropriate Certificate Uses*	1.3.4
1.4.2	*Prohibited Certificate Uses*	1.3.4
1.5	*Policy Administration*	1.4
1.5.1	*Organization Administering the Document*	1.4.1
1.5.2	*Contact Person*	1.4.2
1.5.3	*Person Determining CPS Suitability for the Policy*	1.4.3
1.5.4	*CPS Approval Procedures*	8.3
1.6	*Definitions and Acronyms*	N/A
2.	*Publication and Repository Responsibilities*	2.1.5, 2.6
2.1	*Repositories*	2.6.4
2.2	*Publication of Certification Information*	2.6.1, 8.2
2.3	*Time or Frequency of Publication*	2.6.2, 8.2
2.4	*Access Controls on Repositories*	2.6.3
3.	*Identification and Authentication*	3.
3.1	*Naming*	3.1
3.1.1	*Type of Names*	3.1.1
3.1.2	*Need for Names to be Meaningful*	3.1.2
3.1.3.	*Anonymity or Pseudonymity of Subscribers*	3.1.2
3.1.4	*Rules for Interpreting Various Name Forms*	3.1.3
3.1.5	*Uniqueness of Names*	3.1.4
3.1.6	*Recognition, Authentication, and Role of Trademarks*	3.1.5, 3.1.6

New RFC Section		RFC 2527 Section
3.2	*Initial Identity Validation*	3.1
3.2.1	*Method to Prove Possession of Private Key*	3.1.7
3.2.2	*Authentication of Organization Identity*	3.1.8
3.2.3	*Authentication of Individual Identity*	3.1.9
3.2.4	*Non-Verified Subscriber Information*	N/A
3.2.5	*Validation of Authority*	3.1.9
3.2.6	*Criteria for Interoperation*	4.1
3.3	*Identification and Authentication for Re-Key Requests*	3.2, 3.3
3.3.1	*Identification and Authentication for Routine Re-Key*	3.2
3.3.2	*Identification and Authentication for Re-Key After Revocation*	3.3
3.4	*Identification and Authentication for Revocation Request*	3.4
4.	*Certificate Life-Cycle Operational Requirements*	4.
4.1	*Certificate Application*	4.1
4.1.1	*Who Can Submit a Certificate Application*	4.1
4.1.2	*Enrollment Process and Responsibilities*	2.1.3, 4.1
4.2	*Certificate Application Processing*	4.1, 4.2
4.2.1	*Performing Identification and Authentication Functions*	4.1, 4.2
4.2.2	*Approval or Rejection of Certificate Applications*	4.1, 4.2
4.2.3	*Time to Process Certificate Applications*	4.1, 4.2
4.3	*Certificate Issuance*	4.2
4.3.1	*CA Actions During Certificate Issuance*	4.2
4.3.2	*Notifications to Subscriber by the CA of Issuance of Certificate*	4.2, 4.3
4.4	*Certificate Acceptance*	2.1.3, 4.3
4.4.1	*Conduct Constituting Certificate Acceptance*	4.3
4.4.2	*Publication of the Certificate by the CA*	2.1.5, 2.6.1, 4.3
4.4.3	*Notification of Certificate Issuance by the CA to Other Entities*	2.1.5, 2.6.1, 4.2, 4.3
4.5	*Key Pair and Certificate Usage*	1.3.4, 2.1.3, 2.1.4
4.5.1	*Subscriber Private Key and Certificate Usage*	1.3.4, 2.1.3
4.5.2	*Relying Party Public Key and Certificate Usage*	1.3.4, 2.1.4
4.6	*Certificate Renewal*	3.2, 4.1, 4.2, 4.3
4.6.1	*Circumstances for Certificate Renewal*	3.2, 4.1
4.6.2	*Who May Request Renewal*	3.2, 4.1
4.6.3	*Processing Certificate Renewal Requests*	3.2, 4.1, 4.2
4.6.4	*Notification of New Certificate Issuance to Subscriber*	3.2, 4.2, 4.3
4.6.5	*Conduct Constituting Acceptance of a Renewal Certificate*	2.1.3, 3.2, 4.3
4.6.6	*Publication of the Renewal Certificate by the CA*	2.1.5, 2.6.1, 3.2, 4.3
4.6.7	*Notification of Certificate Issuance by the CA to Other Entities*	2.1.5, 2.6.1, 3.2, 4.2, 4.3
4.7	*Certificate Re-Key*	3.2, 4.1, 4.2, 4.3
4.7.1	*Circumstances for Certificate Re-Key*	3.2, 4.1
4.7.2	*Who May Request Certification of a New Public Key*	3.2, 4.1
4.7.3	*Processing Certificate Re-Keying Requests*	3.2, 4.1, 4.2
4.7.4	*Notification of New Certificate Issuance to Subscriber*	3.2, 4.2, 4.3
4.7.5	*Conduct Constituting Acceptance of a Re-Keyed Certificate*	2.1.3, 3.2, 4.3
4.7.6	*Publication of the Re-Keyed Certificate by the CA*	2.1.5, 2.6.1, 3.2, 4.3
4.7.7	*Notification of Certificate Issuance by the CA to Other Entities*	2.1.5, 2.6.1, 3.2, 4.2, 4.3
4.8	*Certificate Modification*	4.4
4.8.1	*Circumstances for Certificate Modification*	2.1.3, 4.4.1
4.8.2	*Who May Request Certificate Modification*	4.4.2
4.8.3	*Processing Certificate Modification Requests*	4.4.3
4.8.4	*Notification of New Certificate Issuance to Subscriber*	4.2, 4.3, 4.4.3
4.8.5	*Conduct Constituting Acceptance of Modified Certificate*	2.1.3, 4.3, 4.4.3
4.8.6	*Publication of the Modified Certificate by the CA*	2.1.5, 2.6.1, 4.2, 4.3, 4.4.3
4.8.7	*Notification of Certificate Issuance by the CA to Other Entities*	2.1.5, 2.6.1, 4.2, 4.3, 4.4.3
4.9	*Certificate Revocation and Suspension*	4.4
4.9.1	*Circumstances for Revocation*	2.1.3, 4.4.1

New RFC Section		RFC 2527 Section
4.9.2	*Who Can Request Revocation*	4.4.2
4.9.3	*Procedure for Revocation Request*	2.1.3, 4.4.3
4.9.4	*Revocation Request Grace Period*	4.4.4
4.9.5	*Time Within Which CA Must Process the Revocation Request*	N/A
4.9.6	*Revocation Checking Requirements for Relying Parties*	2.1.4, 4.4.10, 4.4.12, 4.4.14
4.9.7	*CRL Issuance Frequency*	4.4.9, 4.8.3
4.9.8	*Maximum Latency for CRLs*	4.4.9
4.9.9	*On-Line Revocation/Status Checking Availability*	4.4.11, 4.8.3
4.9.10	*On-Line Revocation Checking Requirements*	4.4.12
4.9.11	*Other Forms of Revocation Advertisements Available*	4.4.13, 4.4.14, 4.8.3
4.9.12	*Special Requirements re Key Compromise*	4.4.15
4.9.13	*Circumstances for Suspension*	2.1.3, 4.4.5
4.9.14	*Who Can Request Suspension*	4.4.6
4.9.15	*Procedure for Suspension Request*	2.1.3, 4.4.7
4.9.16	*Limits on Suspension Period*	4.4.8
4.10	*Certificate Status Services*	4.4.9-4.4.14
4.10.1	*Operational Characteristics*	4.4.9, 4.4.11, 4.4.13
4.10.2	*Service Availability*	4.4.9, 4.4.11, 4.4.13
4.10.3	*Operational Features*	4.4.9, 4.4.11, 4.4.13
4.11	*End of Subscription*	N/A
4.12	*Key Escrow and Recovery*	6.2.3
4.12.1	*Key Escrow and Recovery Policy and Practices*	6.2.3
4.12.2	*Session Key Encapsulation and Recovery Policy and Practices*	6.2.3
5.	*Facility, Management, and Operational Controls*	2.1.3, 2.1.4, 4., 5.
5.1	*Physical Controls*	5.1
5.1.1	*Site Location and Construction*	5.1.1
5.1.2	*Physical Access*	5.1.2
5.1.3	*Power and Air Conditioning*	5.1.3
5.1.4	*Water Exposures*	5.1.4
5.1.5	*Fire Prevention and Protection*	5.1.5
5.1.6	*Media Storage*	5.1.6
5.1.7	*Waste Disposal*	5.1.7
5.1.8	*Off-Site Backup*	5.1.8
5.2	*Procedural Controls*	5.2
5.2.1	*Trusted Roles*	5.2.1
5.2.2	*Number of Persons Required per Task*	5.2.2
5.2.3	*Identification and Authentication for Each Role*	5.2.3
5.2.4	*Roles Requiring Separation of Duties*	5.2.1, 5.2.2
5.3	*Personnel Controls*	5.3
5.3.1	*Qualifications, Experience, and Clearance Requirements*	5.3.1
5.3.2	*Background Check Procedures*	5.3.2
5.3.3	*Training Requirements*	5.3.3
5.3.4	*Retraining Frequency and Requirements*	5.3.4
5.3.5	*Job Rotation Frequency and Sequence*	5.3.5
5.3.6	*Sanctions for Unauthorized Actions*	5.3.6
5.3.7	*Independent Contractor Requirements*	5.3.7
5.3.8	*Documentation Supplied to Personnel*	5.3.8
5.4	*Audit Logging Procedures*	4.5
5.4.1	*Types of Events Recorded*	4.5.1
5.4.2	*Frequency of Processing Log*	4.5.2
5.4.3	*Retention Period for Audit Log*	4.5.3
5.4.4	*Protection of Audit Log*	4.5.4
5.4.5	*Audit Log Backup Procedures*	4.5.5
5.4.6	*Audit Collection System (Internal vs. External)*	4.5.6
5.4.7	*Notification to Event-Causing Subject*	4.5.7

New RFC Section		RFC 2527 Section
5.4.8	*Vulnerability Assessments*	4.5.8
5.5	*Records Archival*	4.6
5.5.1	*Types of Records Archived*	4.6.1
5.5.2	*Retention Period for Archive*	4.6.2
5.5.3	*Protection of Archive*	4.6.3
5.5.4	*Archive Backup Procedures*	4.6.4
5.5.5	*Requirements for Time-Stamping of Records*	4.6.5
5.5.6	*Archive Collection System (Internal or External)*	4.6.6
5.5.7	*Procedures to Obtain and Verify Archive Information*	4.6.7
5.6	*Key Changeover*	4.7
5.7	*Compromise and Disaster Recovery*	4.8
5.7.1	*Incident and Compromise Handling Procedures*	4.8
5.7.2	*Computing Resources, Software, and/or Data Are Corrupted*	4.8.1
5.7.3	*Entity Private Key Compromise Procedures*	4.8.3
5.7.4	*Business Continuity Capabilities After a Disaster*	4.8.4
5.8	*CA or RA Termination*	4.9
6.	*Technical Security Controls*	2.1.3, 2.1.4, 6.
6.1	*Key Pair Generation and Installation*	6.1
6.1.1	*Key Pair Generation*	6.1.1, 6.1.8
6.1.2	*Private Key Delivery to Subscriber*	6.1.2
6.1.3	*Public Key Delivery to Certificate Issuer*	6.1.3
6.1.4	*CA Public Key Delivery to Relying Parties*	6.1.4
6.1.5	*Key Sizes*	6.1.5
6.1.6	*Public Key Parameters Generation and Quality Checking*	6.1.6, 6.1.7
6.1.7	*Key Usage Purposes (as per X.509 v3 Key Usage Field)*	6.1.9
6.2	*Private Key Protection and Cryptographic Module Engineering Controls*	6.2, 6.8
6.2.1	*Cryptographic Module Standards and Controls*	6.2.1, 6.8
6.2.2	*Private Key (n out of m) Multi-Person Control*	6.2.2
6.2.3	*Private Key Escrow*	6.2.3
6.2.4	*Private Key Backup*	6.2.4
6.2.5	*Private Key Archival*	6.2.5
6.2.6	*Private Key Transfer Into or From a Cryptographic Module*	6.2.6
6.2.7	*Private Key Storage on Cryptographic Module*	6.2.6
6.2.8	*Method of Activating Private Key*	6.2.7
6.2.9	*Method of Deactivating Private Key*	6.2.8
6.2.10	*Method of Destroying Private Key*	6.2.9
6.2.11	*Cryptographic Module Rating*	6.2.1, 6.8
6.3	*Other Aspects of Key Pair Management*	6.3
6.3.1	*Public Key Archival*	6.3.1
6.3.2	*Certificate Operational Periods and Key Pair Usage Periods*	6.3.2
6.4	*Activation Data*	6.4
6.4.1	*Activation Data Generation and Installation*	6.4.1
6.4.2	*Activation Data Protection*	6.4.2
6.4.3	*Other Aspects of Activation Data*	6.4.3
6.5	*Computer Security Controls*	6.5
6.5.1	*Specific Computer Security Technical Requirements*	6.5.1
6.5.2	*Computer Security Rating*	6.5.2
6.6	*Life Cycle Technical Controls*	6.6
6.6.1	*System Development Controls*	6.6.1
6.6.2	*Security Management Controls*	6.6.2
6.6.3	*Life Cycle Security Controls*	6.6.3
6.7	*Network Security Controls*	6.7
6.8	*Time-Stamping*	N/A
7.	*Certificate, CRL, and OCSP Profiles*	7.

New RFC Section		RFC 2527 Section
7.1	*Certificate Profile*	7.1
7.1.1	*Version Number(s)*	7.1.1
7.1.2	*Certificate Extensions*	7.1.2
7.1.3	*Algorithm Object Identifiers*	7.1.3
7.1.4	*Name Forms*	7.1.4
7.1.5	*Name Constraints*	7.1.5
7.1.6	*Certificate Policy Object Identifier*	7.1.6
7.1.7	*Usage of Policy Constraints Extension*	7.1.7
7.1.8	*Policy Qualifiers Syntax and Semantics*	7.1.8
7.1.9	*Processing Semantics for the Critical Certificate Policies Extension*	7.1.9
7.2	*CRL Profile*	7.2
7.2.1	*Version Number(s)*	7.2.1
7.2.2	*CRL and CRL Entry Extesions*	7.2.1
7.3	*OCSP Profile*	N/A
7.3.1	*Version Number(s)*	N/A
7.3.2	*OCSP Extensions*	N/A
8.	*Compliance Audit and Other Assessments*	2.7
8.1	*Frequency and Circumstances of Assessment*	2.7.1
8.2	*Identity/Qualifications of Assessor*	2.7.2
8.3	*Assessor's Relationship to Assessed Entity*	2.7.3
8.4	*Topics Covered by Assessment*	2.7.4
8.5	*Actions Taken as a Result of Deficiency*	2.7.5
8.6	*Communications of Results*	2.7.6
9.	*Other Business and Legal Matters*	2.
9.1	*Fees*	2.5
9.1.1	*Certificate Issuance or Renewal Fees*	2.5.1
9.1.2	*Certificate Access Fees*	2.5.2
9.1.3	*Revocation or Status Information Access Fees*	2.5.3
9.1.4	*Fees for Other Services*	2.5.4
9.1.5	*Refund Policy*	2.5.5
9.2	*Financial Responsibility*	2.3
9.2.1	*Insurance Coverage*	2.3
9.2.2	*Other Assets*	2.3
9.2.3	*Insurance or Warranty Coverage for End-Entities*	2.3
9.3	*Confidentiality of Business Information*	2.8
9.3.1	*Scope of Confidential Information*	2.8.1, 2.8.3
9.3.2	*Information Not Within the Scope of Confidential Information*	2.8.2, 2.8.3
9.3.3	*Responsibility to Protect Confidential Information*	2.8, 2.8.3-2.8.7
9.4	*Privacy of Personal Information*	2.8
9.4.1	*Privacy Plan*	N/A
9.4.2	*Information Treated as Private*	2.8.1, 2.8.3
9.4.3	*Information Not Deemed Private*	2.8.2, 2.8.3
9.4.4	*Responsibility to Protect Private Information*	2.8, 2.8.1, 2.8.3
9.4.5	*Notice and Consent to Use Private Information*	N/A
9.4.6	*Disclosure Pursuant to Judicial or Administrative Process*	2.8.4-2.8.5
9.4.7	*Other Information Disclosure Circumstances*	2.8.6-2.8.7
9.5	*Intellectual Property rights*	2.9
9.6	*Representations and Warranties*	2.2
9.6.1	*CA Representations and Warranties*	2.2.1
9.6.2	*RA Representations and Warranties*	2.2.2
9.6.3	*Subscriber Representations and Warranties*	2.1.3
9.6.4	*Relying Party Representations and Warranties*	2.1.4
9.6.5	*Representations and Warranties of Other Participants*	N/A
9.7	*Disclaimers of Warranties*	2.2, 2.3.2
9.8	*Limitations of Liability*	2.2

New RFC Section		RFC 2527 Section
9.9	***Indemnities***	2.1.3, 2.1.4, 2.2, 2.3.1
9.10	***Term and Termination***	N/A
9.10.1	***Term***	N/A
9.10.2	***Termination***	N/A
9.10.3	***Effect of Termination and Survival***	N/A
9.11	***Individual Notices and Communications with Participants***	2.4.2
9.12	***Amendments***	8.1
9.12.1	***Procedure for Amendment***	8.1
9.12.2	***Notification Mechanism and Period***	8.1
9.12.3	***Circumstances Under Which OID Must be Changed***	8.1
9.13	***Dispute Resolution Provisions***	2.4.3
9.14	***Governing Law***	2.4.1
9.15	***Compliance with Applicable Law***	2.4.1
9.16	***Miscellaneous Provisions***	2.4
9.16.1	***Entire Agreement***	2.4.2
9.16.2	***Assignment***	N/A
9.16.3	***Severability***	2.4.2
9.16.4	***Enforcement (Attorney's Fees and Waiver of Rights)***	2.4.3
9.17	***Other Provisions***	N/A