BR v. 1.2.5 Mapped to BR v. 1.3.0 (RFC 3647

BR v.1.2	Title	BR v.1.3	Title
Page ii	Preface Page	1.1	Overview
Page ii	Notice to Readers	1.5	Policy administration
Page ii	CA/B Forum Members	1.3	PKI Participants
Page iii	Document History	1.2	Document Name and identification
Page iii	Implementers' Note	8	Compliance Audit
Page iv	Relevant Compliance Dates	1.2.2	Relevant Dates
1, 2	Scope, Purpose	1.1	Overview
3	References	1.6.3	References
4	Definitions	1.6.1	Definitions
5	Abbreviations and Acronyms	1.6.2	Abbreviations and Acronyms
6	Conventions	1.6.4	Conventions
7	Certificate Warranties and Representations	9.6	Representations and Warranties
8.1	Compliance	8, 9.16.3	Compliance Audit, Severability
8.2	Certificate Policies	2	Publication of Information
8.3	Commitment to Comply	2.1	Repositories
8.4	Trust Model	3.2.6	Criteria for Interoperation or Certification
9.1	Issuer Information	7.1.4.1	Name Forms: Issuer
9.2	Subject Information	7.1.4.2	Name Forms: Subject
9.3.1	Certificate Policy Identification	1.2	Document Name and identification
9.3.2-9.3.4	Root, Subordinate, and Subscriber Certificates	7.1.6	Certificate Policy Object Identifier
9.4	Validity Period	6.3.2	Certificate Operational Periods and Key Pair Usage Periods
9.4.2	SHA-1 Validity Period	7.1.3	Algorithm Object Identifiers
9.5	Public Key	6.1.3, 6.1.1.3	Public Key Delivery to Certificate Issuer, Subscriber Key Pair Generation
9.6	Certificate Serial Number	7.1	Certificate Profile
9.7	Technical Constraints in Sub CA Certificates via Name Constraints and EKU	7.1.5	Name Constraints
9.8	Additional Technical Requirements	6, 7.1	Technical Security Controls or Certificate Profile, as appropriate
10	Certificate Application	4	Certificate Life-Cycle Requirements
10.1	Documentation Requirements	4.1.2	Enrollment Process and Responsibilities
10.2	Certificate Request	4.1 - 4.2	Certificate Applications
10.2.4	Subscriber Private Key	6.1.2	Private Key Delivery to Subscriber
10.2.5	Subordinate CA Private Key	6.2.4 - 6.2.6	Private Key Backup, Private Key Transfer into or from a Cryptographic Module
10.3	Agreements/Terms of Use	9.6.3	Subscriber Representations and Warranties
11.1	Authorization by Domain Name Registrant	3.2.2	Authentication of Organization and Domain Identity
11.2.3	Authenticity of Certificate Request	3.2.5	Validation of Authority
11.2.4	Verification of Individual Applicant	3.2.3	Authentication of Individual Identity
11.2.5	Verification of Country	3.2.2.3	Verification of Country
11.3	Age of Certificate Data	3.3.1	Identification and Authentication For Routine Re-Key
11.4	Denied List	4.1.1	Who Can Submit a Certificate Application
11.5	High Risk Requests	4.2.1	Performing Identification and Authentication Functions
11.6	Data Source Accuracy	3.2.2.7	Data Source Accuracy
12	Certificate Issuance by a Root CA	4.3.1	CA Actions During Certificate Issuance
13.1.1	Revocation Request	3.4, 4.9.2	Identification and authentication for revocation request, Who Can Request Revocation
13.1.2	Certificate Problem Reporting	4.9.3	Procedure for Revocation Request
13.1.3	Investigation	4.9.5, 2.3	Time Within Which CA Must Process the Revocation Request, Time or frequency of publication
13.1.4	Response	4.10.2	Service Availability
13.1.5	Reasons for Revoking a Subscriber Certificate	4.9.1.1	Reasons for Revoking a Subscriber Certificate
13.1.6	Reasons for Revoking a Subordinate CA Certificate	4.9.1.1, 5.7.3.2	Reasons for Revoking a Subordinate CA Certificate, Intermediate or Subordinate CA Compromise Procedures
13.2	Certificate Status Checking	2	Repositories, Publication of certification information
13.2.1	Mechanisms	4.9, 4.9.11	Other Forms of Revocation Advertisements Available, Certificate Revocation and Suspension
13.2.2	Repository	1.3, 4.9.7, 4.1	Service Availability, Certificate Status Servers
13.2.3	Response Time	4.9.8	Maximum Latency for CRLs
13.2.4	Deletion of Entries	4.10.1	Operational Characteristics
13.2.5	OCSP Signing	4.9.9	On-line Revocation/Status Checking Available
13.2.6	Response for Non-Issued Certificates	4.9.10	On-line Revocation Checking Requirements
13.2.7	Certificate Suspension	4.9.13	Circumstances for Suspension
14.1	Trustworthiness and Competence	5.2	Procedural Controls
14.1.1	Identity and Background Verification	5.3.1	Qualifications, Experience, and Clearance Requirements
14.1.1	Identity and Background Verification	5.3.2	Background Check Procedures
14.1.2	Training and Skill Level	5.3.3, 5.3.4	Training Requirements and Retraining Frequency and Requirements
14.2	Delegation of Functions	1.3.2, 5.3.7	Registration Authorities, Independent Contractor Requirements
15	Data Records	2	Repositories, Publication of certification information
15.1	Documentation and Event Logging	5.4.1	Types of Events Recorded

BR v. 1.2.5 Mapped to BR v. 1.3.0 (RFC 3647

BR v.1.2	Title	BR v.1.3	Title
15.2	Events and Actions	5.4.1	Types of Events Recorded (and Certificate renewal, re-key, modification, as appropriate)
15.3.1	Audit Log Retention	5.4.3, 5.5	Retention period for Audit Log, Records Archival
15.3.2	Documentation Retention	5.5.1, 5.5.2	Retention Period for Archive
16.1	Objectives, Security Plan, Business Continuity, System Security, Private Key Protection	5	Facility, Management, and Operational Controls,
16.2	Risk Assessment	5, 5.4.8	Facility, Management, and Operational Controls, and Vulnerability Assessments
16.3	Security Plan	5	Facility, Management, and Operational Controls,
16.4	Business Continuity	5.7.4	Business Continuity
16.5	System Security	5	Facility, Management, and Operational Controls,
16.6	Private Key Protection	6.2	Private Key Protection and Cryptographic Module Engineering
17	Audit	8.2	Frequency or Circumstances of Assessment
17.1	Eligible Audit Schemes	8.4	Topics Covered By Assessment
17.2	Audit Period	8.1	Frequency or Circumstances of Assessment
17.3	Audit Report	8.6	Communication of Results
17.4	Pre-Issuance Readiness Audit	8.1	Frequency or Circumstances of Assessment
17.5	Audit of Delegated Functions	8.4	Topics Covered By Assessment
17.6	Auditor Qualifications	8.2	Identity/Qualifications of Assessor
17.7	Key Generation Ceremony	6.1.1	Key Pair Generation
17.8	Regular Quality Assessment Self Audits	8.7	Self-Audits
17.9	Regular Quality Assessment of Technically Constrained Subordinate CAs	8.7	Self-Audits
18.1	Liability to Subscribers and Relying Parties	9.8	Limitations of Liability
18.2	Indemnification of Application Software Suppliers	9.9.1	Indemnities
18.3	Root CA Obligations	9.6.1	CA Representations and Warranties
App. A	Cryptographic Algorithm and Key Requirements (Normative)	6.1.5	Key Sizes
App. A (1)	Root CA Certificates	6.1.5	Key Sizes
App. A (2)	Subordinate CA Certificates	6.1.5	Key Sizes
App. A (3)	Subscriber Certificates	6.1.5	Key Sizes
App. A (4)	General Requirements for Public CAs	6.1.6	Public Key Parameters Generation and Quality Checking
App. B	Certificate Extensions (Normative)	6.1.7, 7.1.2	Key Usage Purposes, Certificate Extensions
App. B (1)	Root CA Certificate	7.1.2.1	Key Usage Purposes, Certificate Extensions
App. B (2)	Subordinate CA Certificate	7.1.2.2	Key Usage Purposes, Certificate Extensions
App. B (3)	Subscriber Certificate	7.1.2.3	Key Usage Purposes, Certificate Extensions
App. B (4)	All Certificates	7.7.2.4	Key Usage Purposes, Certificate Extensions
App. C	User Agent Verification (Normative)	2.2	Publication of Information

BR v. 1.3.0 (RFC 3647) Mapped to BR v. 1.2.5

BR v.1.3	Title	BR v.1.2	Title
1	Introduction	Page ii	Intro
1.1.	Overview	1	Scope
1.2.	Document name and Identification	9.3.1	Reserved Certificate Policy Identifiers
1.2.1.	Revisions	Page ii	Document History
1.2.2.	Relevant Dates		Relevant Compliance Dates
1.3.	PKI Participants		
1.3.1.	Certification Authorities	Page ii	Intro
1.3.2.	Registration Authorities	14.2.1, 14.2.4	
1.3.3.	Subscribers		
1.3.4.	Relying Parties	Page ii	Intro
1.3.5.	Other Participants	Page ii	Intro
1.4.	Certificate Usage	2	Purpose
1.4.1.	Appropriate Certificate Uses		
1.4.2.	Prohibited Certificate Uses		
1.5.	Policy administration	Page ii	Notice to Readers
1.6.	Definitions and acronyms		
1.6.1.	Definitions	4	Definitions
1.6.2.	Acronyms	5	Abbreviations and Acronyms
1.6.3.	References	3	References
1.6.4.	Conventions	6	Conventions
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	8.2.1	Implementation
2.1.	Repositories	13.2.1	Mechanisms
2.2.	Publication of information	8.2.2, 8.3, App. C	Disclosure, Commitment to Comply
2.3.	Time or frequency of publication		
2.4.	Access controls on repositories		
3	IDENTIFICATION AND AUTHENTICATION		
3.1.	Naming		
3.2.	Initial identity validation		
3.2.1.	Method to Prove Possession of Private Key		
3.2.2.	Authentication of Organization and Domain Identity	11.2	Verification of Subject Identity Information
3.2.2.1	Identity	11.2.1	Identity
3.2.2.2	DBA/Tradename	11.2.2	DBA/Tradename
3.2.2.3	Verification of Country	11.2.5	Verification of Country
3.2.2.4	Authorization by Domain Name Registrant	11.1.1	Authorization by Domain Name Registrant
3.2.2.5	Authentication for an IP Address	11.1.2	Authentication for an IP Address
3.2.2.6	Wildcard Domain Validation	11.1.3	Wildcard Domain Validation
3.2.2.7	Data Source Accuracy	11.6	Data Source Accuracy
3.2.3.	Authentication of Individual Identity	11.2.4	Verification of Individual Applicant
3.2.4.	Non-verified Subscriber Information		
3.2.5.	Validation of Authority	11.2.3	Authenticity of Certificate Request
3.2.6.	Criteria for Interoperation or Certification	8.4	Trust Model
3.3.	Identification and authentication for re-key requests		
3.3.1.	Identification and Authentication for Routine Re-key	11.3	Age of Certificate Data
3.3.2.	Identification and Authentication for Re-key After Revocation		
3.4.	Identification and authentication for revocation request		
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS		
4.1.	Certificate Application		
4.1.1.	Who Can Submit a Certificate Application	11.4	Denied List
4.1.2.	Enrollment Process and Responsibilities	10.1, 10.2.1, 10.2.2	Documentation Requirements, Certificate Request
4.2.	Certificate application processing		
4.2.1.	Performing Identification and Authentication Functions	10.2.3, 11.5, 14.2.1	Information Requirements, High Risk Requests,
4.2.2.	Approval or Rejection of Certificate Applications	11.1.4	New gTLD Domains
4.2.3.	Time to Process Certificate Applications		
4.3.	Certificate issuance		
4.3.1.	CA Actions during Certificate Issuance	12	Certificate Issuance by a Root CA
4.3.2.	Notification of Certificate Issuance		
4.4.	Certificate acceptance		
4.5.	Key pair and certificate usage		
4.6.	Certificate renewal		
4.7.	Certificate re-key		
4.8.	Certificate modification		
4.9.	Certificate revocation and suspension		
4.9.1.	Circumstances for Revocation		
4.9.1.1	Reasons for Revoking a Subscriber Certificate	13.1.5	Reasons for Revoking a Subscriber Certificate
4.9.1.2	Reasons for Revoking a Subordinate CA Certificate	13.1.6	Reasons for Revoking a Subordinate CA Certificate
4.9.2.	Who Can Request Revocation		
4.9.3.	Procedure for Revocation Request	13.1.1, 13.1.2,	revocation Request, Certificate Problem Reporting
4.9.4.	Revocation Request Grace Period		
4.9.5.	Time within which CA Must Process the Revocation Request	13.1.3	Investigation
4.9.6.	Revocation Checking Requirement for Relying Parties		
4.9.7.	CRL Issuance Frequency	13.2.2	Repository
4.9.8.	Maximum Latency for CRLs		

BR v. 1.3.0 (RFC 3647) Mapped to BR v. 1.2.5

BR v.1.3	Title	BR v.1.2	Title
4.9.9.	On-line Revocation/Status Checking Availability	13.2.5	OCSP Signing
4.9.10.	On-line Revocation Checking Requirements	13.2.2, 13.2.6	Repository, Response for non-issued certificates
4.9.11.	Other Forms of Revocation Advertisements Available		
4.9.12.	Special Requirements Related to Key Compromise		
4.9.13.	Circumstances for Suspension	13.2.7	Certificate Suspension
4.9.14.	Who Can Request Suspension		
4.9.15.	Procedure for Suspension Request		
4.9.16.	Limits on Suspension Period		
4.10.	Certificate status services		
4.10.1.	Operational Characteristics	13.2.4	Deletion of Entries
4.10.2.	Service Availability	13.2.3, 13.2.2, 13.1.4	Repository, Response, Response Time
4.10.3.	Optional Features		
4.11.	End of subscription		
4.12.	Key escrow and recovery		
5	MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS	16.1, 16.2, 16.3, 16.5	Data Security, Objectives, Risk Assessment, Security Plan, System Security
5.1.	Physical security Controls		
5.2.	Procedural controls		
5.2.1.	Trusted Roles		
5.2.2.	Number of Individuals Required per Task	16.6	Private Key Protection
5.2.3.	Identification and Authentication for Trusted Roles		
5.2.4.	Roles Requiring Separation of Duties		
5.3.	Personnel controls		
5.3.1.	Qualifications, Experience, and Clearance Requirements	14.1.1.	Identity and Background Verification
5.3.2.	Background Check Procedures		
5.3.3.	Training Requirements and Procedures	14.1.2	Training and Skill Level
5.3.4.	Retraining Frequency and Requirements	14.1.2	Training and Skill Level
5.3.5.	Job Rotation Frequency and Sequence		
5.3.6.	Sanctions for Unauthorized Actions		
5.3.7.	Independent Contractor Controls	14.2.1	Delegation of Functions, General
5.3.8.	Documentation Supplied to Personnel		
5.4.	Audit logging procedures		
5.4.1.	Types of Events Recorded	15.1, 15.2	Documentation, Event Logging, Events, Actions
5.4.2.	Frequency for Processing and Archiving Audit Logs		
5.4.3.	Retention Period for Audit Logs	15.2	Events and Actions
5.4.4.	Protection of Audit Log		
5.4.5.	Audit Log Backup Procedures		
5.4.6.	Audit Log Accumulation System (internal vs. external)		
5.4.7.	Notification to Event-Causing Subject		
5.4.8.	Vulnerability Assessments	16.2	Risk Assessment
5.5.	Records archival		
5.5.1.	Types of Records Archived		
5.5.2.	Retention Period for Archive	15.3.2	Documentation Retention
5.5.3.	Protection of Archive		
5.5.4.	Archive Backup Procedures		
5.5.5.	Requirements for Time-stamping of Records		
5.5.6.	Archive Collection System (internal or external)		
5.5.7.	Procedures to Obtain and Verify Archive Information		
5.6.	Key changeover		
5.7.	Compromise and disaster recovery		
5.7.1.	Incident and Compromise Handling Procedures	16.4	Business Continuity
5.7.2.	Recovery Procedures if Computing Resources, ... Are Corrupted		
5.7.3.	Recovery Procedures After Key Compromise		
5.7.4.	Business Continuity Capabilities after a Disaster		
5.8.	CA or RA termination		
6	TECHNICAL SECURITY CONTROLS		
6.1.	Key pair generation and installation		
6.1.1.	Key Pair Generation		
6.1.1.1	CA Key Pair Generation	17.7	Key Generation Ceremony
6.1.1.2	RA Key Pair Generation		
6.1.1.3	Subscriber Key Pair Generation	9.5	Public Key
6.1.2.	Private Key Delivery to Subscriber	10.2.4	Subscriber Privvate Key
6.1.3.	Public Key Delivery to Certificate Issuer		
6.1.4.	CA Public Key Delivery to Relying Parties		
6.1.5.	Key Sizes	App. A	Cryptographic Algorithm and Key Requirements
6.1.6.	Public Key Parameters Generation and Quality Checking	App. A	Cryptographic Algorithm and Key Requirements
6.1.7.	Key Usage Purposes	12	Certificate Issuance by a Root CA
6.2.	Private Key Protection and Cryptographic Module Engineering Controls	16.6	Prrivate Key Protection
6.2.1.	Cryptographic Module Standards and Controls		
6.2.2.	Private Key (n out of m) Multi-person Control		
6.2.3.	Private Key Escrow		
6.2.4.	Private Key Backup		
6.2.5.	See Section 5.2.2.Private Key Archival	10.2.5	Subordinate CA Private Key
6.2.6.	Private Key Transfer into or from a Cryptographic Module	10.2.5	Subordinate CA Private Key

BR v. 1.3.0 (RFC 3647) Mapped to BR v. 1.2.5

BR v.1.3	Title	BR v.1.2	Title
6.2.7.	Private Key Storage on Cryptographic Module	16.6	Prrivate Key Protection
6.2.8.	Activating Private Keys		
6.2.9.	Deactivating Private Keys		
6.2.10.	Destroying Private Keys		
6.2.11.	Cryptographic Module Capabilities		
6.3.	Other aspects of key pair management		
6.3.1.	Public Key Archival		
6.3.2.	Certificate Operational Periods and Key Pair Usage Periods	9.4.1	Subscriber Certificates, Validity Period
6.4.	Activation data		
6.5.	Computer security controls		
6.5.1.	Specific Computer Security Technical Requirements	16.5	System Security
6.5.2.	Computer Security Rating		
6.6.	Life cycle technical controls		
6.7.	Network security controls		
6.8.	Time-stamping		
7	CERTIFICATE, CRL, AND OCSP PROFILES		
7.1.	Certificate profile	9.8, 9.6	Additional Technical Requirements, Certificte Serial Number
7.1.1.	Version Number(s)		
7.1.2.	Certificate Content and Extensions; Application of RFC 5280	App. B	Certificate Content and Extensions; Application of RFC 5280
7.1.3.	Algorithm Object Identifiers	9.4.2	SHA-1 Validity Period
7.1.4.	Name Forms	9.1.4, 9.2, 9.2.1, 9.2.4, 9	Issuer Information, Subject Information
7.1.5.	Name Constraints	9.7	Technical Constraints in Sub CA Certificates via Name Constraints and EKU
7.1.6.	Certificate Policy Object Identifier	9.3	Certificate Policy Identification
7.1.7.	Usage of Policy Constraints Extension		
7.1.8.	Policy Qualifiers Syntax and Semantics		
7.1.9.	Processing Semantics for the Critical Certificate Policies Extension		
7.2.	CRL profile		
7.3.	OCSP profile		
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	8.1, page ii	Compliance
8.1.	Frequency or circumstances of assessment	17, 17.2, 17.4	Audit Period, Pre-Issuance Readiness Audit
8.2.	Identity/qualifications of assessor	17.6	Auditor Qualifications
8.3.	Assessor's relationship to assessed entity		
8.4.	Topics covered by assessment	17.1, 17.5,	Eligible Audit Schemes, Audit of Delegated Functions
8.5.	Actions taken as a result of deficiency		
8.6.	Communication of results	17.3	Audit Report
8.7.	Self-Audits	17.8, 14.2.2, 17.9	Regular Quality Assessment Self Audits, Compliance Obligation
9	OTHER BUSINESS AND LEGAL MATTERS		
9.1.	Fees		
9.2.	Financial responsibility		
9.3.	Confidentiality of business information		
9.4.	Privacy of personal information		
9.5.	Intellectual property rights		
9.6.	Representations and warranties		
9.6.1.	CA Representations and Warranties	17.1, 18.3	Eligible Audit Schemes, Audit of Delegated Functions, Root CA Obligations
9.6.2.	RA Representations and Warranties		
9.6.3.	Subscriber Representations and Warranties	7.2, 10.3	Certificate Warranties and Representations by the Applicant, Subscriber and Terms of Use Agreement
9.6.4.	Relying Party Representations and Warranties		
9.6.5.	Representations and Warranties of Other Participants		
9.7.	Disclaimers of warranties		
9.8.	Limitations of liability	14.2.3, 18.1	Allocation of Liability, Liability to Subscribers and Relying Parties
9.9.	Indemnities		
9.9.1.	Indemnification by CAs	18.2	Indemnification of Application Software Suppliers
9.9.2.	Indemnification by Subscribers		
9.9.3.	Indemnification by Relying Parties		
9.10.	Term and termination		
9.11.	Individual notices and communications with participants		
9.12.	Amendments		
9.13.	Dispute resolution provisions		
9.14.	Governing law		
9.15.	Compliance with applicable law		
9.16.	Miscellaneous provisions		
9.16.1.	Entire Agreement		
9.16.2.	Assignment		
9.16.3.	Severability	8.1	Compliance
9.16.4.	Enforcement		
9.16.5.	Force Majeure		
9.17.	Other provisions		