

Contents

1. Introduction	1-1
1.1 Purpose and Scope	1-1
1.2 Target Audience	1-2
1.3 Reasons for Issue 1	1-2
1.4 Structure of This Document	1-2
1.5 Requirements Terminology	1-3
1.6 Requirement Labeling Conventions	1-3
1.6.1 Numbering of Requirement and Related Objects	1-3
1.6.2 Requirement and Objective Object Identification	1-4
2. General Information	2-1
2.1 Problem/Opportunity	2-1
2.2 General Description	2-2
2.2.1 Certification Authority (CA)	2-4
2.2.2 Digital Certificates	2-5
2.2.3 Registration Authority (RA)	2-5
2.2.4 PKI Directory	2-6
2.2.5 Certificate Subjects	2-7
2.2.6 Key Recovery	2-7
2.3 Assumptions, Dependencies, and Constraints	2-8
3. PKI Security	3-1
3.1 Theft of the CA's Private Key	3-3
3.1.1 Cryptanalysis Defense	3-3
3.1.2 Break-In Defense	3-6
3.1.3 Spoofing Defense	3-7
3.1.4 Detection of CA Key Compromise	3-8
3.1.5 Recovery From Compromised CA Key	3-9
3.2 Theft of an RA's Private Key	3-10
3.2.1 Protected RA Operations	3-10
3.2.2 Detection of RA Key Compromise	3-11
3.2.3 Recovery From Compromised RA Key	3-12
3.3 Theft of a TMN Entity Private Key	3-12
3.3.1 User's Private Key Protection	3-12
3.3.2 Detection of Theft of a User's Private Key	3-13
3.3.3 User's Private Key Recovery	3-14
3.4 Spoofing of the CA's Public Key	3-15
3.4.1 CA Key Spoofing Protection	3-15
3.5 Spoofing of an RA's Public Key	3-17
3.6 Spoofing of a User's Public Key	3-17
3.7 Corruption of the PKI Directory	3-18
3.7.1 Protection of the PKI Directory	3-18
3.8 Loss of the CA's Private Key	3-19
3.9 Loss of an RA's Private Key	3-20
3.10 Loss of a User's Private Key	3-20

4. Functional Requirements	4-1
4.1 Certificate Requirements	4-1
4.1.1 Certificate Extensions	4-1
4.1.1.1 Authority Key Identifier	4-2
4.1.1.2 Subject Key Identifier	4-3
4.1.1.3 Key Usage	4-3
4.1.1.4 Private Key Usage Period	4-4
4.1.1.5 Certificate Policies	4-4
4.1.1.6 Policy Mapping	4-4
4.1.1.7 Subject Alternative Name	4-5
4.1.1.8 Issuer Alternative Name	4-5
4.1.1.9 Subject Directory Attributes	4-5
4.1.1.10 Basic Constraints	4-5
4.1.1.11 Name Constraints	4-6
4.1.1.12 Policy Constraints	4-6
4.1.1.13 Extended Key Usage	4-6
4.1.1.14 CRL Distribution Points	4-7
4.1.1.15 Authority Information Access	4-7
4.1.1.16 Key Recovery	4-7
4.1.2 Certificate Revocation List (CRL) Extensions	4-7
4.1.2.1 Authority Key Identifier	4-7
4.1.2.2 Issuer Alternative Name	4-8
4.1.2.3 CRL Number	4-8
4.1.2.4 Delta CRL Indicator	4-8
4.1.2.5 Issuing Distribution Point	4-8
4.1.3 Extensions for Individual Entries in CRLs	4-9
4.1.3.1 Reason Code	4-9
4.1.3.2 Hold Instruction Code	4-9
4.1.3.3 Invalidity Date	4-9
4.1.3.4 Certificate Issuer	4-9
4.2 Certificate Validation	4-10
4.3 Registration Authority (RA)	4-11
4.4 Audit	4-14
4.5 Protocol Requirements	4-15
4.6 CA Configuration, Backup, and Recovery	4-17
4.7 CA Operations	4-18
5. Global Product Requirements	5-1
5.1 Availability/Reliability	5-1
5.2 Performance	5-1
5.3 Security	5-1
Appendix A: References	A-1
Appendix B: Acronyms	B-1
Requirement-Object Index	ROI-1

List of Figures

Figure 2-1	Interactions Among TMN PKI Components	2-3
------------	---	-----