Bechtel Externally Rooted PKI Certification Policy and Certificate Practice Statement

2PP-S310-00067, Rev 4.0

October 28, 2025

Electronic documents, once printed, are uncontrolled and may become outdated. Refer to the electronic documents for current revisions.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved

TABLE OF CONTENTS

DOCUMENT HISTORY 8

1. INTRODUCTION 9

1.1 Overview 9

1.2 Document Name and Identification 10

1.3 PKI Participants 11
1.3.1 Bechtel Policy Management Authority (BPMA) 11
1.3.2 Certification Authorities 12
1.3.2.1 Role of Certification Authorities 12
1.3.3 Registration Authorities 12
1.3.3.1 Role of Registration Authorities 12
1.3.4 Key Recovery Agent 13
1.3.5 Role of Key Recovery Agent 13
1.3.6 Subscribers (End Entities) 13
1.3.6.1 Role of Subscribers 13
1.3.6.2 PKI Sponsors 14
1.3.7 Relying Parties 14
1.3.8 Other Participants 14
1.3.8.1 Trusted Agents 14
1.3.8.2 Affiliated Organization 14

1.4 Certificate Usage 15
1.4.1 Appropriate Certificate Uses 15
1.4.1.1 Level of Assurance 15
1.4.1.2 General Usage 15
1.4.2 Prohibited Certificate Uses 17

1.5 Policy Administration 17
1.5.1 Organization Administering the Document 17
1.5.2 Contact Person 17
1.5.3 Person Determining CPS Suitability for the Policy 17
1.5.4 CPS approval procedures 18

1.6 Definitions and Acronyms 18

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 18

2.1 Repositories 18

2.2 Publication of Certification Information 18

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

2.3 Time or Frequency of Publication 19

2.4 Access Controls on Repositories 19

3. IDENTIFICATION AND AUTHENTICATION 19

3.1 Naming 19
3.1.1 Types of Names 19
3.1.2 Need for Names to be Meaningful 20
3.1.3 Anonymity or Pseudonymity of Subscribers 20
3.1.4 Rules for Interpreting Various Name Forms 20
3.1.5 Uniqueness of Names 20
3.1.6 Recognition, Authentication, and Role of Trademarks 20

3.2 Initial Identity Validation 21
3.2.1 Method to Prove Possession of Private Key 21
3.2.2 Authentication of Organization Identity 21
3.2.3 Authentication of Individual Identity 21
3.2.3.1 In-Person Authentication 21
3.2.4 Non-Verified Subscriber Information 22
3.2.5 Validation of Authority 22
3.2.6 Criteria for Interoperation 22

3.3 Identification and Authentication for Re-Key Requests 22
3.3.1 Identification and Authentication for Routine Re-Key 22
3.3.2 Identification and Authentication for Re-Key after Revocation 23

3.4 Identification and Authentication for Revocation Request 23

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 23

4.1 Certificate Application 23
4.1.1 Who can Submit a Certificate Application 24
4.1.2 Enrollment Process and Responsibilities 24

4.2 Certificate Application Processing 24
4.2.1 Performing Identification and Authentication Functions 24
4.2.2 Approval or Rejection of Certificate Applications 24
4.2.3 Time to Process Certificate Applications 25

4.3 Certificate Issuance 25
4.3.1 CA Actions during Certificate Issuance 25
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 25

4.4 Certificate Acceptance 25
4.4.1 Conduct Constituting Certificate Acceptance 25
4.4.2 Publication of the Certificate by the CA 26

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities 26

4.5 Key Pair and Certificate Usage 26
4.5.1 Subscriber Private Key and Certificate Usage 26
4.5.2 Relying Party Public Key and Certificate Usage 26

4.6 Certificate Renewal 27
4.6.1 Circumstance for Certificate Renewal 27
4.6.2 Who May Request Renewal 27
4.6.3 Processing Certificate Renewal Requests 27
4.6.4 Notification of New Certificate Issuance to Subscriber 27
4.6.5 Conduct constituting acceptance of a renewal certificate 27
4.6.6 Publication of the renewal certificate by the CA 27
4.6.7 Notification of certificate issuance by the CA to other entities 27

4.7 Certificate Re-Key 27
4.7.1 Circumstance for Certificate Re-Key 28
4.7.2 Who May Request Certification of a New Public Key 28
4.7.3 Processing Certificate Re-Keying Requests 28
4.7.4 Notification of New Certificate Issuance to Subscriber 28
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 28
4.7.6 Publication of the Re-Keyed Certificate by the CA 28
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 28

4.8 Certificate Modification 28

4.9 Certificate Revocation and Suspension 29
4.9.1 Circumstances for Revocation 29
4.9.2 Who can Request Revocation 29
4.9.3 Procedure for Revocation Request 29
4.9.4 Revocation Request Grace Period 30
4.9.5 Time Within Which CA Must Process the Revocation Request 30
4.9.6 Revocation Checking Requirement for Relying Parties 30
4.9.7 CRL Issuance Frequency 30
4.9.8 Maximum Latency for CRLs 31
4.9.9 On-Line Revocation/Status Checking Availability 31
4.9.10 On-Line Revocation Checking Requirements 31
4.9.11 Optional Features 31

4.10 End of Subscription 32
4.10.1 Operational Characteristics 32
4.10.2 Service Availability 32

4.11 Key Escrow and Recovery 32
4.11.1 Key Recovery Roles 32
4.11.1.1 Key Recovery Agent 32
4.11.1.2 Subscriber 32
4.11.1.3 Requestor 32
4.11.2 Escrowed Key Recovery Requests 33

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

4.11.2.1 Who Can Request Recovery of Escrowed Keys 33
4.11.2.2 Requirements for Requesting Escrowed Key Recovery 33
4.11.3 Delivery of Escrowed Key to Subscriber 33
4.11.4 Session Key Encapsulation and Recovery Policy and Practices 34

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 34

5.1 Physical Controls 34
5.1.1 Off-Site Backup 34

5.2 Procedural Controls 34
5.2.1 Trusted Roles 34
5.2.1.1 Certification Authority 35
5.2.1.2 Registration Authority 35
5.2.2 Number of Persons Required per Task 35
5.2.3 Identification and Authentication for Each Role 35

5.3 Personnel Controls 36
5.3.1 Qualifications, Experience, and Clearance Requirements 36
5.3.2 Training Requirements 36
5.3.3 Retraining Frequency and Requirements 36
5.3.4 Job Rotation Frequency and Sequence 36
5.3.5 Sanctions for Unauthorized Actions 36
5.3.6 Independent Contractor Requirements 37
5.3.7 Documentation Supplied to Personnel 37

5.4 Audit Logging Procedures 37
5.4.1 Types of Events Recorded 37
5.4.2 Frequency of Processing Log 37
5.4.3 Retention Period for Audit Log 38
5.4.4 Protection of Audit Log 38
5.4.5 Audit Log Backup Procedures 38
5.4.6 Notification to Event-Causing Subject 38
5.4.7 Vulnerability Assessments 38

5.5 Records Archival 38
5.5.1 Types of Records Archived 38
5.5.2 Retention Period for Archive 39
5.5.3 Protection of Archive 39
5.5.4 Archive Backup Procedures 39
5.5.5 Requirements for Time-Stamping of Records 39
5.5.6 Archive Collection System (Internal or External) 39
5.5.7 Procedures to Obtain and Verify Archive Information 39

5.6 Key Changeover 39

5.7 Compromise and Disaster Recovery 40
5.7.1 Incident and Compromise Handling Procedures 40

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

5.7.2 Computing Resources, Software, and/or Data are Corrupted 40

5.8 CA or RA Termination 40

6. TECHNICAL SECURITY CONTROLS 40

6.1 Key Pair Generation and Installation 40
6.1.1 Key Pair Generation 40
6.1.2 Private Key Delivery to Subscriber 41
6.1.3 Public Key Delivery to Certificate Issuer 41
6.1.4 Key Sizes 41
6.1.5 Public Key Parameters Generation and Quality Checking 41
6.1.6 Key Usage Purposes 41

6.2 Private Key Protection and Cryptographic Module Engineering Controls 42
6.2.1 Cryptographic Module Standards and Controls 42
6.2.2 Private Key (n out of m) Multi-Person Control 42
6.2.3 Private Key Escrow 42
6.2.4 Private Key Storage on Cryptographic Module 43
6.2.5 Method of Deactivating Private Key 43
6.2.6 Method of Destroying Private Key 43
6.2.7 Cryptographic Module Rating 43

6.3 Other Aspects of Key Pair Management 43
6.3.1 Public Key Archival 43
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 44

6.4 Activation Data 44

6.5 Computer Security Controls 44

6.6 Life Cycle Technical Controls 44

6.7 Network Security Controls 44

7. CERTIFICATE, CRL, AND OCSP PROFILES 45

7.1 Certificate Profile 45
7.1.1 Version Number(s) 45
7.1.2 Certificate Extensions 45
7.1.3 Name Forms 45
7.1.4 Name Constraints 45
7.1.5 Certificate Policy Object Identifier 45

7.2 CRL Profile 45

7.3 OCSP Profile 45

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 46

8.1 Frequency or Circumstances of Assessment 46

8.2 Identity/Qualifications of Assessor 46

8.3 Assessor's Relationship to Assessed Entity 46

8.4 Topics Covered by Assessment 46

8.5 Actions Taken as a Result of Deficiency 46

8.6 Communication of Results 46

9. OTHER BUSINESS AND LEGAL MATTERS 47

9.1 Fees 47

9.2 Financial Responsibility 47

9.3 Confidentiality of Business Information 47

9.4 Privacy of Personal and Corporate Information 47
9.4.1 Privacy Plan 47
9.4.2 Information Treated as Private 47
9.4.3 Information not Deemed Private 47

9.5 Intellectual Property Rights 48

9.6 Representations and Warranties 48
9.6.1 CA and RA Representations and Warranties 48
9.6.1.1 Limited Warranty 48
9.6.1.2 RA representations and warranties 48
9.6.2 Subscriber representations and warranties 48
9.6.3 Relying party representations and warranties 49

9.7 Disclaimers of Warranties 49

9.8 Limitations of Liability 50

9.9 Indemnities 50

9.10 Term and Termination 50

9.11 Individual Notices and Communications with Participants 50

9.12 Amendments 50

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

9.13 Dispute Resolution Provisions 51

9.14 Governing Law..... 51

9.15 Miscellaneous Provisions..... 51
9.15.1 Severability 51
9.15.2 Enforcement (attorney's fees and waiver of rights) 51
9.15.3 Force Majeure..... 51

10. LIST OF DEFINITIONS 51

11. LIST OF ACRONYMS 57

REFERENCES 57

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

DOCUMENT HISTORY

Document Change Control

Version	Release Date	Author	Status / Description
1.0	17-DEC-2009	Rick Ammenheuser John Bobrek	Initial CPS
2.0	9-JAN-2015	Steven Meier	General Update and reformatting to RFC 3647
3.0	6-APR-2022	Steven Meier John Bobrek	Update PKI Repository URL, Contact Information, CRL Publication Timeline
4.0	28-OCT-2025	Steven Meier	Updated Bechtel Logo, copyright, contact information, and RFC References

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

1. INTRODUCTION

Bechtel Global Corporation (“Bechtel”) issues for itself and on behalf any Bechtel Affiliate who participates in the activities described in this document, this Certification Policies and Practices Statement (CPS) of the Bechtel Certification Authority (hereinafter, Bechtel CA) applies to products and services of the Bechtel CA that provide and manage X.509 digital certificates. This CPS can be found on the Bechtel CA repository at: certauth.bechtel.com. This document will be reviewed and updated as described in Section 1.5.4.

The X.509 standard defines a certificate policy as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements". An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose. RFC 3647 issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and certificate management. While certain section titles are included in this policy according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the certificate management services of the Bechtel CA. Where applicable, these sections have been removed from this document. Where necessary additional information is presented as subsections added to the standard structure. Additional assertions on standards used in this CPS can be found under section “Acknowledgements”.

Inquiries pertaining to this CPS can be addressed to:

Bechtel Global Corporation
Attn: Chief Information Security Officer
12011 Sunset Hills Rd
Reston, VA 20190
USA
Email: SOC@BECHTEL.COM
URL: certauth.bechtel.com

For all PKI Participants, per Section 1.3, this CPS becomes effective and binding upon acceptance of a subscriber agreement, the submission of a certificate related request to the Bechtel CA for digital certificate issuance, and / or the reliance by any party on a certificate issued by the Bechtel CA.

1.1 Overview

Bechtel’s Public Key Infrastructure (PKI) solution is designed to accommodate both internally and externally trusted certificate authorities. One type of externally trusted relationship is an externally published trusted root authority. Externally trusted roots provide the capability for any user (using a popular browser) to authenticate the validity of any externally published certificates. This allows for the signing and encryption of internally produced electronic messages and the publishing of external certificate encrypted (e.g., https/TLS) protected websites.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

Bechtel has a Bechtel managed Certificate Authority (CA) which chains to an Externally Trusted Root CA for these services. This CA is known as a Bechtel CA, which issues and manages certificates on behalf of the Externally Trusted Root CA.

Herein, references to a Bechtel PKI, Bechtel CA, Issuing CA, and CA refer to this particular certificate authority unless specifically identified otherwise.

This CPS applies to the specific domain of the Bechtel CA. The purpose of this CPS is to describe the policies and practices for the operation of the Bechtel CA. This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of Bechtel certificates. The purpose is to demonstrate compliance with requirements pertaining to the issuance of digital certificates according to Bechtel's own and industry requirements pursuant to the standards set out above. The certificate types addressed in this CPS is the following:

- Bechtel sMIME Signature
- Bechtel sMIME Encryption
- Bechtel Key Recovery Agent
- Bechtel OCSP Signing
- Bechtel Public Webserver
- Bechtel External Issuing CA

Depending upon their type, these certificates:

- Can be used for electronic signatures and/or encryption of electronic mail
- Can be used for electronic signatures in order to replace handwritten signatures where transacting parties choose to accept them
- Can be used to authenticate infrastructure resources, such as web servers and other devices
- Can be used to authenticate and establish trust of other certification authorities

1.2 Document Name and Identification

This CPS is called The Bechtel Externally Rooted PKI Certification Policies and Practices Statement.

The Bechtel CA issues certificates for use in the verification of digital signatures and certificates for use in encryption.

This CPS is assigned an object identifier (OID), which is asserted in any certificate issued by the CA, where the CA complies with the certificate policy stipulations.

The OID registered by Bechtel for the Bechtel Externally Rooted PKI Certificate Policies and Practice Statement (this document) is:

{iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) Bechtel (16082) Public Key Infrastructure (2) Bechtel Externally Rooted PKI Certificate Policies and Practice Statement (2)} or in dotted notation: 1.3.6.1.4.1.16082.2.2

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

OID Branch	Dot Notation	ASN.1 Notation
Enterprise	1.3.6.1.4.1	OBJECT IDENTIFIER::= {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) }
Bechtel	1.3.6.1.4.1.16082	OBJECT IDENTIFIER::= {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Bechtel-Corporation(16802) }
PKI	1.3.6.1.4.1.16082.2	OBJECT IDENTIFIER::= {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Bechtel-Corporation(16802) Bechtel-Infrastructure-Definitions(1) PKI(2) }
Certificate Practice Statement	1.3.6.1.4.1.16082.2.2	OBJECT IDENTIFIER::= {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Bechtel-Corporation(16802) Bechtel-Infrastructure-Definitions(1) PKI(2) Certificate-Practice-Statement(2) }

Likewise, application certificates created under this CPS will originate for this branch of the Bechtel OID tree:

{iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) Bechtel (16082) Public Key Infrastructure (2) Application Policies(3)} or in dotted notation: 1.3.6.1.4.1.16082.2.3

Certificates created from this CPS will possess the following OIDs (as applicable) within their Enhanced Key Usage (EKU)

1.3 PKI Participants

The subcomponent describes the identity or types of entities that fill the roles and associated privileges of participants within Bechtel PKI.

Both CAs and Registration Authorities (RAs) are considered “Certificate Management Authorities” (CMAs). This policy will use the term CMA when a function may be assigned to either a CA or a RA, or when a requirement applies to both CAs and RAs.

Server-based Certificate Status Authorities (CSAs) such as Online Certificate Status Protocol (OCSP) Responders and Server-based Certificate Validation Protocol (SCVP) status providers operated by Bechtel are also considered CMAs.

1.3.1 Bechtel Policy Management Authority (BPMA)

The Bechtel Policy Management Authority (BPMA) is established to:

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- Oversee the creation and update of this CPS and plans for implementing any accepted changes.
- Review the results of compliance audits to determine if the CAs are meeting the stipulations of this CPS and make recommendations to the CAs regarding corrective actions, or other measures that might be appropriate, such as revocation of CA certificates or changes to this CPS.

1.3.2 Certification Authorities

A Certification Authority (CA), such as Bechtel CA, is an entity authorized by the BPMA to create, sign, and issue certificates to be used in public or private domains, within a business framework, a transaction context etc. A CA may also be referred to as the Issuing Authority to denote the purpose of issuing certificates at the request of an RA. Any CA requirement expressed in this Policy applies to all CA types unless expressly stated otherwise.

The Bechtel CA ensures the availability of the overall management of Bechtel certificate lifecycle, including control over the identification and authentication process, the certificate creation process, revocation of certificates, status verification of a certificate, as they become available or required in specific applications.

1.3.2.1 Role of Certification Authorities

Bechtel CA operates as a Trusted Service Provider to ensure Trust Services to all internal entities that have a relationship with Bechtel's CA, while adhering to the limitations and stipulations applied by the Externally Trusted Root CA.

1.3.3 Registration Authorities

A Registration Authority (RA) is an entity that enters into an agreement with a CA to interact with the Subscriber to perform the verification of the Subscribers' identity and information that is to be verified for certificate issuance, suspension and revocation. The RA will confirm and utilize the information pertaining to the Subscriber to enter the appropriate information for the generation and/or revocation of certificates as defined in this CPS and documented procedures.

1.3.3.1 Role of Registration Authorities

The Bechtel RA will interact with the Subscriber to carry out the provisioning of certificate by:

- Accepts, evaluates, approves or rejects the registration of certificate
- Registers subscribers to CA certification services
- Attends all stages of the identification of subscribers as assigned by the CA according to the type of certificates they issue
- Uses official or otherwise reliable documents to evaluate a subscriber request
- Following approval of a request, issue a certificate

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- Initiates the process to suspend, or unsuspend or revoke a certificate and request a certificate revocation from the Bechtel CA

1.3.4 Key Recovery Agent

A Key Recovery Agent (KRA) is an individual who is authorized to extract an escrowed key. The KRAs have high-level sensitive access to the escrowed keys. Because KRAs can recover large number of keys, the BPMA places a high level of trust in them. Therefore, the Bechtel CA shall closely control the number and location of KRAs.

1.3.5 Role of Key Recovery Agent

The Bechtel KRA will interact with the CMA and Bechtel CA to:

- Protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys
- Protect all information, including the KRA' s own private/public key that could be used to recover subscribers' escrowed keys
- Release subscribers' escrowed keys only for properly authenticated and authorized requests from requestors
- Protect all information regarding all occurrences of key recovery

The KRA cannot possess the responsibilities of the CMA role concurrently.

1.3.6 Subscribers (End Entities)

Subscriber of Bechtel CA services is the entity whose name appears as the subject in a certificate, and who asserts that it uses the certificate (private key and public key) for the purpose of electronic signature, authentication, and encryption services in accordance with this policy.

Subscribers typically hold a valid identification document, such as an identity card, passport or equivalent, which is used as credential in order to issue electronic certificates.

Subscribers are limited to the following categories of entities:

- Bechtel Employees
- Bechtel associates, contractors, business partners involved in the day-to-day activities within Bechtel that require access to Bechtel resources
- Bechtel operational or functional roles requiring the use of electronic signature and encryption services approved by the Bechtel CA
- Workstations, firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components

1.3.6.1 Role of Subscribers

The Subscriber will:

- Make true representation at all times to both the Bechtel CA regarding information to be included in certificates and other identification and authentication information;

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- Use certificates exclusively for legal and authorized company business
- Protect the private key for all certificates regardless of type
- Password protect or encrypt the private key when stored outside of the intended cryptographic module
- Protect their user password, by not writing it down or by storing a written copy in a locked file to which only that user has access
- Inform Bechtel IS&T within 72 hours of a change to any information included in the certificate
- Inform Bechtel IS&T within 1 hour of detecting a suspected compromise of the private key
- For Medium or High Assurance Certificates, read, sign and return the Subscriber Agreement Form upon receipt of the software and digital certificate

1.3.6.2 PKI Sponsors

A PKI Sponsor fills the role of a Subscriber for non-human system components and organizations that are named as public key certificate subjects. The PKI Sponsor works with the CMAs to register components (e.g., routers, firewalls) and is responsible for meeting the obligations of Subscribers as defined throughout this document.

1.3.7 Relying Parties

A Relying Party is any individual or entity that acts in reliance on a Bechtel Certificate to verify a digital signature and/or decrypt an encrypted document or message. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use and does so at its own risk.

1.3.8 Other Participants

1.3.8.1 Trusted Agents

Bechtel may choose to use the services of Trusted Agents to assist CMAs in performing identity verification tasks. A Trusted Agent is a person authorized to act as a representative of a CMA in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with CAs.

1.3.8.2 Affiliated Organization

An Affiliated Organization is an organization that has a relationship with Bechtel and which sponsors a subscriber the issuance of a certificate. Affiliated Organizations are responsible for verifying the subscriber identity and qualification prior to certificate issuance and will request revocation of the certificate if the qualification is no longer valid.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

1.4 Certificate Usage

Certain limitations apply to the use of Bechtel CA certificates.

1.4.1 Appropriate Certificate Uses

Certificates issued under the Bechtel CA are intended to support the following security services:

- Confidentiality
- Authentication
- Non-repudiation

Additional uses are specifically designated once they become available to subscribers. Unauthorized use of Certificates may result in the voiding of warranties offered by Bechtel CA to Subscribers and their Relying Parties.

1.4.1.1 Level of Assurance

The level of assurance associated with a public key certificate is an assertion by a CA of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate. Level of assurance depends on the proper registration of Subscribers and the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of this policy. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system.

1.4.1.2 General Usage

This section contains definitions for the three levels of assurance implied by the certificates implemented by Bechtel's CA. The certificates issued by the Bechtel CA (the subject of this CPS) will be identified accordingly.

Bechtel Low Assurance

To meet the Bechtel Low Assurance certificate class, the Subscriber of the certificate must be built from information provided by Active Directory and/or have knowledge of the associated account and password. A certificate that uses the Bechtel Low Assurance certificate class is not intended for purchases or other non-repudiation purposes but is mainly geared toward authenticating users and normal system processes. Low Assurance certificates may be used to prove that the original content is not modified, or that the user has access to any data encrypted with the private key or authenticate the source of the certificate subject.

Low Assurance Class certificates shall be built from the following minimum requirements. Additional criterion may be required by the specific certificate template being implemented.

- Validation of network access via authentication from network credentials
- Certificate Subject Name built from Active Directory attributes
- Certificate Application Policy "may" contain a Bechtel OID

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- Auto-Enrollment may be used

The Bechtel PKI certificate templates implement the Bechtel Low Assurance certificate class (Bechtel Application Policy OIDs are shown if applicable).

Bechtel Medium Assurance

To meet the Bechtel Medium Assurance certificate class, the Subscriber of the certificate must be identified in a face-to-face interview where he/she presents photo identification to the RA. The photo identification may be a Bechtel badge (for Bechtel employees), or one piece of government or state issued photo identification with signature (such as a driver's license, passport, etc.).

The registration authority (RA) will record the identification before issuing the certificate. The database of Medium Assurance identification records is protected as Bechtel Confidential data to ensure privacy and protection of the information. The RA is required to authenticate using his/her two-factor device before performing any activities.

Bechtel Medium Assurance certificates and related private keys may be stored within a two-factor device. If export is enabled for these private keys, it is the responsibility of the person performing the export to protect the private key material from theft.

Building upon the requirements for Low Assurance certificates, Medium Assurance Class certificates shall be created using the following minimum requirements. Additional criterion may be required by the Bechtel Policy Authority for the individual application template.

- Certificate Subject Name built from Active Directory attributes
- Certificate Application Policy will contain a Bechtel OID
- Enrollment is completed by a Registration Authority
- Subscriber needs to provide valid photo identification
- Certificate is contained to a two-factor device (e.g., smartcard)

The Bechtel PKI certificate templates implement the Bechtel Medium Assurance certificate class (Bechtel Application Policy OIDs are shown if applicable).

Bechtel High Assurance

High Assurance certificates require the Subscriber to use a two-factor authentication device (token, Smartcard or similar) and are generally required for administrative users of the PKI or secure systems. To meet the Bechtel High Assurance certificate policy, the Subscriber of the certificate must present photo identification and be identified in a face-to-face interview with the RA. The photo identification may be a Bechtel badge (for Bechtel employees) or one piece of government or state issued photo identification with signature (such as a driver's license, passport, etc.).

The local registration authority (RA) will record and maintain a scanned copy of the identification before issuing the certificate on the two-factor device. The database of High Assurance identification records is protected as Bechtel Confidential data to ensure privacy and protection of

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

the information. The RA is required to authenticate using his/her two-factor device and will require additional signature approvals before creating a High Assurance class certificate.

A Bechtel High Assurance certificate and related private key are stored on a two-factor hardware device, such as a smart card. A smart card prevents export of the associated private key, and requires both access to the smart card and knowledge of the smart card's PIN to access the private key.

The Bechtel PKI certificate templates implement the Bechtel High Assurance certificate class (Bechtel Application Policy OIDs are shown if applicable).

To allow the verification of the subject, each of these certificate requests is pended until the RA verifies the identity of the subject and satisfies the required number of authorized signatures.

1.4.2 Prohibited Certificate Uses

A Subscriber certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not authorized and will result in an annulment of warranties offered by the Bechtel CA.

1.5 Policy Administration

The BPMA of the Bechtel CA manages this CPS. The Bechtel CA registers, observes the maintenance, and interprets this CPS. The Bechtel CA makes available the operational conditions prevailing in the life-cycle management of Bechtel certificates.

1.5.1 Organization Administering the Document

The BPMA is responsible for the definition, revision, and promulgation of this policy. The BPMA is the Office of the Bechtel Chief Information Officer, and its designees.

1.5.2 Contact Person

Questions regarding this CPS should be directed to:

Bechtel Global Corporation
Attn: Chief Information Security Officer
12011 Sunset Hills Rd
Reston, VA 20190
USA
Email: SOC@BECHTEL.COM

1.5.3 Person Determining CPS Suitability for the Policy

The BPMA shall determine the suitability of any CPS to this policy.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

1.5.4 CPS approval procedures

The BPMA shall make the determination that a CPS complies with this policy for a given level of assurance. The CMA must have and meet all requirements of an approved CPS. The CMA will review this CPS annually and notify the BPMA of any recommended changes or revisions.

1.6 Definitions and Acronyms

A list of Acronyms and definitions can be found at the end of this CPS.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Bechtel CA publishes information about the digital certificates that it issues in an online repository, accessible to Subscribers and Relying Parties. Bechtel CA refrains from making publicly available certain elements of documents including security controls, procedures, internal security polices etc.

The repository for the Bechtel CA is provided by Bechtel's Active Directory. The protocol used to access the directory is the Lightweight Directory Access Protocol (LDAP) version 2, over TCP transport as specified in Section 3.1 of Internet RFC 1777.

When conveyed in LDAP requests and results, attributes defined in X.500 are encoded using string representations defined in RFC 1778, "The String Representation of Standard Attribute Syntaxes". These string encodings were based on the attribute definitions from X.500 (1988). Thus, the string representations of:

- UserCertificate (RFC 1778 section 2.25)
- CACertificate (RFC 1778 section 2.26)
- Certificate Revocation List, (RFC 1778 section 2.28)

Bechtel PKI uses X.509 version 3 certificates and revocation lists, as defined in X.509 (1997), the RFC 1778 string encoding of these attributes is inappropriate. For this reason, these attributes are encoded using syntax similar to the syntax Undefined from section 2.1 of RFC 1778: values of these attributes are encoded as if they were values of type OCTET STRING, with the string value of the encoding being the DER-encoding of the value itself.

2.2 Publication of Certification Information

Each CA shall provide an on-line repository (certauth.bechtel.com) that is available to Subscribers and Relying Parties and that contains:

- The most recently issued CRL
- The CA's certificate for its certificate and CRL signing key
- Certificates issued to the CA

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- A copy of this Policy

The procedures shall be designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimal down-time.

2.3 Time or Frequency of Publication

Certificates shall be published following Subscriber acceptance as specified in Section 4.4 and proof of possession of private key as specified in Section 3.2.1. The CRL is published as specified in Section 4.9.7. All information to be published in the repository shall be published promptly after such information becomes available to the CA.

2.4 Access Controls on Repositories

The Bechtel CA shall protect information not intended for public distribution or amendment.

With respect to the Bechtel CA information published in the Active directory, the Bechtel PKI CMA will have sufficient access permissions on entries to allow them to:

- For Bechtel CA entries:
    - Add, modify and delete all PKI attributes in its own directory entry;
    - Add, modify and delete all values of these attributes.
- For Bechtel CA CRL distribution point entries:
    - Create, modify and delete entries of structural object class CRL-Distribution-Point immediately subordinate to its own entry;
    - Add, modify and delete all attributes, and all values of the PKI attributes.
- For Bechtel CA user entries:
    - Add and delete user attributes of all entries representing prospective users;
    - Add, modify and delete the attribute “userCertificate” and all values of that attribute to/from these entries.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Bechtel CAs shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN).

Names for certificate issuers and certificate subjects will use the X.500 Distinguished Name form. Bechtel Corporation is a registered name in accordance with ANSI, the U.S. national registration

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

authority. A single naming hierarchy is established within Bechtel as outlined below. Certificates may contain other name forms, such as User Principal Names or RFC 822 Names, and these names must be included in the Subject Alternative Name (SAN) attribute of the certificate, rather than the Subject attribute.
Certificates issued to CAs and RAs shall use the X.500 DN form.

3.1.2 Need for Names to be Meaningful

Names used will identify the natural person, legal person, or object to which they are assigned in a meaningful way and in a manner permitting determination of the identity of the certificate Subscriber. The value of the commonName attribute used in naming Bechtel employees is not necessarily the name by which the associate is registered with the Bechtel Human Resources Department but is generally the name (e.g., nickname) by which they are commonly known within the organization. The value of the serialNumber attribute used in naming Bechtel employees is not the corporate employee number assigned to the employee at the time of hiring.

3.1.3 Anonymity or Pseudonymity of Subscribers

The Bechtel CA shall not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

DNs and their component RDNs (Relative Distinguished Names) are to be interpreted as defined in sections 3.1.1 and 3.1.2 of this CPS. Additional alternative name forms, if present, are to be interpreted in accordance with rules identified by the issuing name authority.

3.1.5 Uniqueness of Names

Names are unambiguously defined for each object in the naming hierarchy. The serialNumber attribute (i.e., the sequence number as part of a unique identifier) is used to ensure that no two individuals are assigned the same DN, and therefore the same electronic identity. Values of the serialNumber attribute are not reused.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Bechtel CA/RA authenticates names of employees and other entities within the Bechtel organization, to include Bechtel associates, contractors, business partners involved in the day-to-day activities within Bechtel that require access to Bechtel resources.

Bechtel shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the Subscriber generates keys, the Subscriber shall be required to prove to the certificate manager possession of the private key which corresponds to the public key in the certificate request. For signature keys, this may be done by signing the request.

In the case where key is generated directly on the Subscriber's token, or in a key generator that benignly transfers the key to the Subscriber's token, then the Subscriber is in possession of the private key at the time of generation or transfer. If the Subscriber is not in possession of the token when the key is generated, then the token shall be delivered to the Subscriber via a responsible method (see Section 6.1.2).

For all assurance levels, when keyed hardware tokens are delivered to Subscribers, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers. The certificate manager must maintain a record of validation for receipt of the token by the Subscriber. When any mechanism that includes a shared secret (e.g., a password or pin) is used, the mechanism shall ensure that the applicant and the certificate manager are the only recipients of this shared secret.

3.2.2 Authentication of Organization Identity

The Bechtel CA is issued a CA certificate from the externally rooted CA organization. As there are usually existing business agreements between Bechtel and the root authority's organization to be a qualified intermediate/subordinate, additional authentication of the identity of either organization is not generally required. If the CMA determines that there is a need for further authentication, this is handled either by searches of recognized databases of registered corporations, or by presentation of the organization's articles of incorporation to the CMA. In all cases, the authentication documentation is filed and archived by the CMA.

3.2.3 Authentication of Individual Identity

The responsibility for authentication of all subscribers' individual identities resides with the Bechtel RA. The Bechtel RA may rely on Trusted Agent, PKI Sponsor, and Affiliated Organization. The Human Resources database and/or Bechtel ID database must be used to validate all certificate users' identities. All certificates shall have a limited validity period.

Bechtel RA ensures that:

- Subscribers of certificates are properly identified and authenticated
- Subscriber certificate requests are complete, accurate and duly authorized.

3.2.3.1 In-Person Authentication

Bechtel Employees:

- Have already presented themselves in person and been verified as part of the existing hiring processes and/or background checks.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- No further documentation is required.

Bechtel associates, contractors, business partners:

- For pre-established business relationships a Trusted Agent, PKI Sponsor or Affiliated Organization validates the identity by proxy. The Bechtel RA uses this proxy validation to issue the subscriber's certificates.
- No further documentation is required.

3.2.4 Non-Verified Subscriber Information

Certificates shall not contain information that is not verified.

3.2.5 Validation of Authority

Certificates that contain explicit or implicit organization affiliations shall be issued only after determining the Subscriber has the authorizations to act on behalf of the organization in the implied and authorized capacity. Examples of these include CA, RA, and Operational/Functional Role certificates.

Operational/Functional Role certificates for each Operational/Functional Role may be issued to one or more individual members of the Operational/Functional Role provided the following requirements are met for each Operational/Functional Role:

- All certificates issued to the Operational/Functional Role shall have the same unique Subject DN that meaningfully conveys the Operational/Functional Role name
- Operational/Functional Role Manager is responsible ensuring control of private keys
- Encryption certificates issued to the Operational/Functional Role may share a single key pair
- Each individual member of the Operational/Functional Role shall be responsible for the decryption private keys
- Operational/Functional Role Manager is responsible for requesting the revocation of certificates if the key becomes compromised, lost, or Operational/Functional Role ceases to exist

3.2.6 Criteria for Interoperation

The Certificate and CRL Profile in this CPS shall form a basis for assessing interoperability with the Bechtel PKI. However, the decision to cross certify with an external PKI shall reside with the BPMA.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Bechtel employees and business partners are updated automatically by using Active Directory Autoenrollment mechanisms. Prior to expiration of the current key pairs, Group Policy invokes

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

Autoenrollment and the user's keys are updated transparently in the case of Bechtel Low Assurance certificates. Users are required to sign their renewal request with their previous certificate's private key in the case of a Bechtel High Assurance certificate. In these cases, authentication of the individual's identity as defined in section 3.2 of this CPS need not be repeated.

For Bechtel Medium Assurance certificates, the certificate requestor must apply for the new certificate by following the same certificate enrollment process used for the initial certificate request.

3.3.2 Identification and Authentication for Re-Key after Revocation

For subscribers whose certificates have been revoked, re-key will generally not be permitted until the identification and authentication requirements for initial registration described in section 3.2 of this CPS are repeated. RAs may allow exceptions in the following situations:

- Organizational change within Bechtel results in changes to the DNs of several employees
- Subscriber is temporarily unable to present him/herself in person (e.g., on extended travel) and the revocation was not due to a key compromise

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated and requires the Bechtel CA to service the revocation requests. Requests by the Subscriber to revoke his/her end-entity certificate require one of the following identification and authentication mechanisms prior to initiating an online request:

- Subscriber presents him/herself in person to the Bechtel RA or his delegate along with his/her Bechtel photo badge;
- Authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

This Policy identifies the minimal operational requirements and procedures that are necessary to support trust in the Bechtel PKI, and to minimize imposition of specific implementation requirements on CMAs, Subscribers, and Relying Parties applied to Certificate Lifecycle.

All entities, explicit or implicit within the Bechtel domain have a continuous obligation to inform the Bechtel CA of any changes in the attributes in a certificate until it has expired or is revoked.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

These steps may be performed in any order that is convenient for the CMA and Subscribers, and that do not defeat security; but all must be completed prior to certificate issuance. All communications among CMAs supporting the certificate application and issuance process shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued.

4.1.1 Who can Submit a Certificate Application

Certificate application may be submitted to the CA by the Subscriber, or an RA on behalf of the Subscriber

4.1.2 Enrollment Process and Responsibilities

The applicant and the Bechtel CA must perform the following steps when an applicant applies for a certificate:

- Establish and record the identity of Subscriber as defined in Section 3.2
- Obtain a public/private key pair for each certificate required
- Establish that the public key forms a functioning key pair with the private key held by the Subscriber
- Provide a point of contact for verification of any roles or authorizations requested

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Upon receiving the request, the CMA will:

- Verify the identity of the requestor
- Verify the authority of the requestor and the integrity of the information in the certificate request
- Create and sign a certificate, if all certificate requirements have been satisfied
- Make the certificate available to the Subscriber.

The certificate request may contain an already complied (“to-be-signed”) certificate. This certificate will not be signed until all verifications and modifications, if any, have been completed to the Bechtel CA's satisfaction.

4.2.2 Approval or Rejection of Certificate Applications

CMAs shall verify all authorization and other attribute information received from an applicant. Information regarding attributes shall be verified via those offices or roles that have authority to assign the information or attribute.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

If a certificate request is denied, then the Bechtel CA will not sign the requested certificate, and the Bechtel RA record the reason for rejection.

4.2.3 Time to Process Certificate Applications

The entire process from application authentication and certificate issuance shall take no more than 30 days. Any process that is not completed within the period is rejected.

4.3 Certificate Issuance

For Bechtel Low Assurance certificates, the issuance of the certificate will depend entirely on the Discretionary Access Control List (DACL) assigned to the requested certificate template. If the requestor has the correct permissions in the DACL, the certificate is issued

Upon receiving the request of a Bechtel Medium Assurance or Bechtel High Assurance certificate, the Bechtel RA will:

- Verify the identity of the requestor
- Verify the authority of the requestor and the integrity of the information in the certificate request
- Verify the certificate is stored using a two-factor device (e.g., smartcard)

4.3.1 CA Actions during Certificate Issuance

The CA shall authenticate a certificate request, ensure that the public key is bound to the correct Subscriber, obtain a proof of possession of the private key, then generate a certificate, [add the appropriate key usage extensions to the certificate], and provide the certificate to the Subscriber.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The Subscriber will be notified of certificate issuance.

4.4 Certificate Acceptance

An issued Bechtel CA certificate is deemed accepted by the subscriber when no objection is received by the Bechtel CA from the subscriber after receiving notification of certificate issuance. Any objection to accepting an issued certificate must explicitly be notified to the Bechtel CA. The reason for rejection including any fields in the certificate that contain erroneous information must also be submitted.

4.4.1 Conduct Constituting Certificate Acceptance

For Bechtel Low Assurance certificates, Subscriber certificate application and lack of objection to published certificates shall constitute certificate acceptance.

For Bechtel Medium Assurance or Bechtel High Assurance certificate, before a CA allows a Subscriber to make effective use of its private key, a member of the Bechtel CA shall

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- Explain to the Subscriber its responsibilities as defined in Section 1.3.4
- Inform the Subscriber of the issuance of a pending certificate when requesting a Bechtel Medium Assurance certificate
- Require the Subscriber to indicate acceptance of its obligations and its certificate, with either a digital or handwritten signature
- Document the Subscriber's acceptance of its responsibilities and its certificate.

The order of this process, and the mechanisms used, will depend on factors such as where the key is generated and how certificates are posted. In the case of non-human components (router, firewalls, etc.), the manager of the device shall perform the functions of the Subscriber.

4.4.2 Publication of the Certificate by the CA

CA certificates and Subscriber encryption certificates shall be published to the appropriate repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The obligations of the subscriber include:

- Accepting the policies and procedures set forth in this CPS
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorized use of their private key
- Using of the private key in accordance with the key usage extension in the certificate
- Observing any constraints, if the extended key usage extension is present and implies any limitation on the use of the private key
- Discontinuing use of private key after the associated certificate has been revoked or has expired
- Utilizing the decryption private key solely to decrypt previously encrypted information after the associated certificate has been revoked or has expired.

4.5.2 Relying Party Public Key and Certificate Usage

The Relying Parties shall ensure that a public key in a certificate is used only for the purposes indicated by the key usage and/or extended key usage extension, if the extension is present.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

4.6 Certificate Renewal

Renewing a certificate means generating a new certificate with the same subject, key, and authorizations as the current or previous one, but will obtain a new validity period and a new serial number. A certificate may be renewed if the public key has not reached the end of its validity, the associated private key has not been compromised, and the Subscriber name and attributes are correct.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if:

- The certificate has not reached the end of its validity period
- The certificate has not been revoked

4.6.2 Who May Request Renewal

The Subscriber or the Bechtel RA may request renewal of Subscriber certificates.

The Operational/Functional Role Manager may request renewal for Operational/Functional Role certificates.

4.6.3 Processing Certificate Renewal Requests

The renewal process shall be in accordance with the certificate issuance process described in Section 3.2.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.6.5 Conduct constituting acceptance of a renewal certificate

See Section 4.4.1

4.6.6 Publication of the renewal certificate by the CA

See Section 4.4.2

4.6.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3

4.7 Certificate Re-Key

Subscribers will periodically obtain new keys and re-establish their identities.

Re-keying a certificate means that a new certificate is created that has:

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- A new, different public key (corresponding to a new, different private key)
- A different serial number; and may be assigned a different validity period

4.7.1 Circumstance for Certificate Re-Key

A certificate shall be re-keyed when it can no longer be renewed

A revoked certificate shall not be re-keyed, except as defined in Section 3.3.2

4.7.2 Who May Request Certification of a New Public Key

The Subscriber or the Bechtel RA may request re-key of Subscriber certificates.

The Operational/Functional Role Manager may request re-key for Operational/Functional Role certificates.

4.7.3 Processing Certificate Re-Keying Requests

The re-key process shall be in accordance with the certificate issuance process described in Section 3.2.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.8 Certificate Modification

Certificate modification will be facilitated through the stipulations in Sections: 4.3, 4.5, and 4.6.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate shall be revoked prior to the expiration of the certificate validity period when the certificate is no longer considered valid for one of the following circumstances:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate's subject
- The certificate's subscriber has breached a material obligation under this CPS
- There has been a modification of the information contained in the certificate of the certificate's subject
- The Subscriber and/or other authorized entity (as stipulated in this CPS) request the certificate to be revoked
- The Bechtel CA ceases to exist or operate
- The External Root issuing the Bechtel CA Certificate ceases to exist or operate or otherwise revokes the Bechtel Certificate

In addition, if it is determined subsequent to issuance of new certificates that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key shall be revoked.

4.9.2 Who can Request Revocation

Within the Bechtel PKI, a CMA may summarily revoke certificates within its domain upon request of any of the following:

- Subscriber
- Authorized employee of the Subject of the Certificate (Role/Function)
- Anyone with access to the private Key that corresponds to the public key in the certificate
- The subject named in the certificate
- Any authorized members of Bechtel Information Security Team

4.9.3 Procedure for Revocation Request

Any request for a revocation shall identify the certificate to be revoked, explains the reason for revocation, and allows the request to be authenticated (e.g., digitally or manually signed). The request may be made by contacting the Bechtel IS&T Service Center. A CMA action is required for revocation (a Subscriber may not, via an automated process, revoke its own certificate). Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

Upon receipt of a revocation request from the Subscriber or another authorized party, the CMA shall authenticate the revocation request. The certificate manager may, at its discretion, take reasonable measures to verify the need for revocation. If the revocation request appears to be valid, the CMA shall revoke the certificate by placing its serial number and other identifying information on a CRL.

For Bechtel Medium Assurance or Bechtel High Assurance certificate issued by the Bechtel CA, Subscribers leaving organizations that sponsored their participation in the Bechtel PKI shall surrender to either the Bechtel CA, Bechtel RA, Trusted Agent, PKI Sponsor, or Affiliated Organization (through any accountable mechanism) all cryptographic hardware tokens that were issued under the sponsoring organization prior to leaving the organization.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy; Bechtel CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request

4.9.5 Time Within Which CA Must Process the Revocation Request

The CA shall process all revocation requests within three hour of receipt. CRL issuance frequency is addressed in Section 4.9.7.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties are required to check Certificate status using the applicable CRL before relying on a Bechtel CA certificate.

4.9.7 CRL Issuance Frequency

CRLs are periodically issued and posted to a repository according to the periods described below, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required.

The Externally Trusted Root that the Bechtel CA chains to is not cover or within scope of this CPS.

The following publication intervals are used for Bechtel PKI CRL publication:

- Offline CA:
    - Publish Base CRLs every twelve months
    - When an Issuing CA is created or revoked
    - In the event the Offline CAs certificate is renewed or re-keyed
- Issuing CA:
    - Publish Base CRLs weekly
    - Publish Delta CRLs daily

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- Publish Base and Delta CRLs within sixteen hours of notification of Subscriber certificate compromise.
- In the event the Issuing CAs certificate is renewed or re-keyed

4.9.8 Maximum Latency for CRLs

The CRL shall be posted upon generation, but no more than four hours after generation.

4.9.9 On-Line Revocation/Status Checking Availability

In addition to CRLs, Bechtel CAs shall also support on-line status checking via OCSP Responders.

On-line Certificate Status provides revocation status information only (e.g., OCSP Responder) shall ensure that:

- Accurate and up-to-date information from the authorized CA is used to provide the revocation status
- Latency of certificate status information shall meet or exceed the requirements for CRL issuance stated in Section 4.9.7
- OCSP Responder shall process requests and provide responses compliant with X.509 Internet Public Key Infrastructure Online Certificate Status Protocol [RFC 2560]
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked
- On-line CSAs used for verifying certificates asserting a policy OID from this CP shall ensure that:
  - Certificates indicated as being valid have a chain of valid certificates (valid as defined by [X.509])
  - Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation
  - Certificate status responses provide authentication and integrity services commensurate with the assurance level of the certificate being verified

4.9.10 On-Line Revocation Checking Requirements

Relying Parties must confirm revocation information.

Since some relying parties may not be able to accommodate on-line communications, all Bechtel CAs will support CRLs.

4.9.11 Optional Features

Certificate Status checking such as Server-based Certificate Validation Protocol (SCVP) shall comply with the requirements of this CPS and applicable Internet Standards.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

4.10 End of Subscription

Subscription is interchangeable with the certificate validity period. The subscription ends when the certificate is revoked or expired.

4.10.1 Operational Characteristics

The Bechtel CA maintains a CRL repository which can be used to validate revocation of a certificate.

4.10.2 Service Availability

Certificate Status Services are available 24x7 unless temporarily unavailable due to maintenance or service failure.

4.11 Key Escrow and Recovery

4.11.1 Key Recovery Roles

4.11.1.1 Key Recovery Agent

A KRA is an appointed and trusted individual who is authorized to interact with the Bechtel CA in order to extract an escrowed decryption private key.

4.11.1.2 Subscriber

A subscriber is an end-entity that holds a private key that corresponds to a public key listed in that certificate. For the purposes of Key Recovery, a subscriber is an end-entity that holds a decryption private key that is escrowed.

4.11.1.3 Requestor

A requestor is the person who requests the recovery of decryption private key(s). A requestor is generally the subscriber, a third party from the subscriber's organization (e.g., manager, corporate officer) or a law enforcement officer who is authorized with a legally valid, court-issued warrant or order to request recovery of a subscriber's escrowed key.

All other requestors require the approval of the BPMA and/or CMA.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

4.11.2 Escrowed Key Recovery Requests

4.11.2.1 Who Can Request Recovery of Escrowed Keys

Requests for recovery of escrowed key may be accepted from:

- Subscribers may request recovery of his/her own escrowed encryption keys
- Authorized law enforcement with a court order from a court of competent jurisdiction
- Third-Parties who have authorization for the BPMA and/or CMA

4.11.2.2 Requirements for Requesting Escrowed Key Recovery

The Bechtel KRA is ultimately responsible the authentication and verification of requests for escrowed key recovery. The primary method for requesting the recovery of a subscriber's escrowed key is the Bechtel IS&T Service Center.

- The Subscriber must use electronic means to request his/her own escrowed keys.
- The Bechtel KRA will validate the request for recovery, prior to carrying out the recovery
- The Bechtel KRA shall notify BPMA or CMA and legal counsel for any requests not specifically covered in this CPS

4.11.3 Delivery of Escrowed Key to Subscriber

Delivery of the escrowed key shall be protected at all times and will be securely delivered to the Subscriber. Recovered escrowed keys will be password protected, the KRA shall generate a random password at the time of recovery, and the password shall not be sent using the same method for delivery of the escrowed private key.

The Bechtel KRA shall:

- Authenticate the requestor through appropriate means
- Notify the Subscriber upon successful recovery and method for delivery
- Provide the recovery escrow key password using appropriate methods (method must be different than private key)
- Provide instructions to Subscriber

The Subscriber shall:

- Provide verification to the Bechtel KRA if applicable
- Protect and make use of the recovered escrowed key, in accordance with Section 1.3.6 and Section 4.5 of this CPS

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

4.11.4 Session Key Encapsulation and Recovery Policy and Practices

The Bechtel CA shall not support key escrow and recovery using key encapsulation techniques

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Bechtel CA has implemented commercially sound security controls to restrict access to the hardware and software used in providing CA services.

5.1 Physical Controls

Bechtel CA systems are located in physically secured facilities. Access to facilities (own, leased or rented), RA areas, and Computer Rooms housing the Bechtel CA requires a card key, which is given only to authorized personnel. Access is restricted based on job function. The facility also employs an intrusion detection system. Entry/exit is logged by the card reader system or through the use of a manual sign-in sheet. Opening and closing of areas are also logged. The alarm monitoring system for fire, water, and intrusion is wired into the building system.

5.1.1 Off-Site Backup

System backups, sufficient to recover from system failure, shall be made on a periodic schedule.

5.2 Procedural Controls

The BPMA will provide oversight of the Bechtel CA and will delegate the roles for managing the Bechtel CA to provide check/balance mechanism and to prevent collusion thus increasing the integrity of the solution.

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be careful and above reproach as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI.

Two approaches are taken to increase the likelihood that these roles can be successfully carried out:

- Design and configure the technology to avoid mistakes and prohibit inappropriate behavior.
- Distribute functions among several people, so that malicious activity requires collusion.

The primary trusted role defined by this Policy is that of the Bechtel CA and Bechtel RA. Other roles may be defined in other documents, which describe or impose requirements on the Bechtel CA's operation.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

5.2.1.1 Certification Authority

All Certificates asserting this policy must be issued by CA facilities under the direct control of the Bechtel CA. The responsible individual or body identified as operating the CA facilities must be named and made available during compliance audits. Any CA who asserts a policy identifier defined in this document is subject to the stipulations of this policy. Bechtel CA's role and the corresponding procedures a CA will follow shall be defined in detail in this CPS.

Primarily, a CA's responsibilities are to ensure that the following functions occur according to the stipulations of this policy:

- Certificate generation and revocation
- Posting Certificates, CRLs and delta CRLs
- Performing daily incremental database backups
- Administrative functions such as compromise reporting and maintaining the database

5.2.1.2 Registration Authority

Any RA that operates under this policy is subject to the stipulations of this policy, and of the BPMA approved CPS under which it operates.

Primarily, a RA's responsibilities are:

- Verifying identity, either through personal contact, or via Trusted Agents or employees, when allowed by this policy
- Entering Subscriber information, and verifying correctness
- Securely communicating requests to and responses from the CA
- Receiving and distributing Subscriber certificates

5.2.2 Number of Persons Required per Task

CA, KRA, and Bechtel High Assurance key generation, activation and backup shall be performed under a minimum of two-person control.

Where multi-party control for logical access is required, at least one of the participants shall be a Bechtel CA Administrator. A Bechtel CA Auditor shall not be considered as participant for multiparty control for logical access.

5.2.3 Identification and Authentication for Each Role

Individuals shall identify and authenticate themselves before being permitted to perform any actions set forth above for that role or identity.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

5.3 Personnel Controls

For individuals' assigned Bechtel CA management roles, there is to be no conflict between their responsibilities within the operation and management of the Bechtel CA and other duties assigned to them as part of other daily responsibilities within Bechtel.

5.3.1 Qualifications, Experience, and Clearance Requirements

The Bechtel CA shall perform checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job.

Background checks may include:

- Have demonstrated the ability to perform their duties
- Be trustworthy
- Have no other duties that would interfere or conflict with their duties as a CMA
- Have professional references confirmed
- Confirmation of previous employment
- Confirmation of the most relevant educational degree obtained
- Check of representations made by the candidate
- Any other as it might be deemed necessary

5.3.2 Training Requirements

The Bechtel CA makes available training for personnel to carry out CA and RA functions. The specific training required will depend on the equipment used, the tasks assigned, and the personnel selected.

5.3.3 Retraining Frequency and Requirements

Those involved in filling Bechtel PKI roles shall be aware of changes in the CMA operation. Any significant change to the CMA may result in additional training.

5.3.4 Job Rotation Frequency and Sequence

Not Applicable

5.3.5 Sanctions for Unauthorized Actions

Bechtel shall take appropriate administrative and disciplinary actions against personnel who violate this policy.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

5.3.6 Independent Contractor Requirements

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as Bechtel personnel.

5.3.7 Documentation Supplied to Personnel

The Bechtel CA and RAs make appropriate training and operating documentation available to personnel.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The Bechtel and its RA function will record system and CA application events and will create certificate management logs from the data collected in accordance with internal audit procedures.

The following events will be recorded:

- Applicant and Subscriber events
    - Request to create a certificate
    - Request to revoke a certificate
- Certificate lifecycle events.
    - Key generation
    - Key compromise notification
    - Creation of a certificate
    - Delivery of a certificate
    - Revocation of a certificate
    - Generation of a Certificate Revocation List
- Actions by Trusted Personnel
    - Login events and use of identification and authentication mechanisms
    - Changes to CA policies
    - Changes to CA keys

The Bechtel CA will collect event information and create Certificate management logs using automated and manual practices and procedures that are internal to the CMA.

5.4.2 Frequency of Processing Log

The Bechtel CA shall be reviewed at least 4 (quarterly) times per year, with at least 25 percent of the security audit data generated since the last review to be examined.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

The auditor shall implement procedures to ensure that the security audit data is transferred prior to overwriting or overflow of automated security audit log files.

5.4.3 Retention Period for Audit Log

The information generated on the Bechtel CA shall be kept on the Bechtel CA until the information is moved to an appropriate off-site facility. Deletion of the security audit data from the Bechtel CA shall be performed only by auditors. The audit log record retention period will follow corporate policies.

5.4.4 Protection of Audit Log

For the Bechtel CA, the security audit data shall not be open for reading or modification by any human, or by any automated process other than those that perform security audit processing. The entity performing security audit data archive shall not have modify access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the certificate manager equipment.

5.4.5 Audit Log Backup Procedures

The security audit data backup shall be protected in accordance with the requirements of Section 5.4.4.

5.4.6 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.7 Vulnerability Assessments

The certificate manager, system administrator, and other operating personnel shall be watchful for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel. The security audit data shall be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors shall check for continuity of the security audit data

5.5 Records Archival

5.5.1 Types of Records Archived

Certificate manager archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

5.5.2 Retention Period for Archive

Archive records shall be kept for a period of at least five years for the Bechtel CA without any loss of data. Applications necessary to read these archives must be maintained for at least the applicable retention period.

5.5.3 Protection of Archive

No unauthorized CA equipment operator shall be able to modify or delete the archive, but archived records may be moved to another medium. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. No transfer of medium shall invalidate certificate manager applied signatures. The certificate manager shall maintain a list of people authorized to modify or delete the archive, and make this list available during CPS compliance audits

5.5.4 Archive Backup Procedures

No stipulation

5.5.5 Requirements for Time-Stamping of Records

No stipulation

5.5.6 Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner approved by the CMA or BPMA.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, package, and send the archive information will be provided to personnel performing this activity. Only authorized CA equipment operators will be allowed to access the archive.

5.6 Key Changeover

The Bechtel CA uses a signing (private) key for creating certificates; however, Relying Parties employ the CA certificate for the life of the Subscriber certificate beyond that signing. Therefore, the Bechtel CA must not issue Subscriber certificates that extend beyond the expiration dates of their own certificates and public keys. To minimize risk to the Bechtel CA through compromise of a CA key, the private signing key will be changed more frequently, and only the new key will be used for certificate signing purposes from that time. The older, but still valid, certificate will be available to verify old signatures until all the Subscriber certificates signed under it have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

In case of a Bechtel CA key compromise, the parent CA shall revoke that CA certificate, and the revocation information shall be published immediately in the most expedient manner. Subsequently, the Bechtel CA installation shall be reestablished as described herein

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The Bechtel CA maintains a Disaster Recovery Plan. This plan is submitted to the Information Systems and Technology (IS&T) for approval. In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations shall be reestablished as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If the Bechtel CA cannot reestablish revocation capabilities within one week, then the Bechtel CA must report its keys as compromised. After capabilities are restored, The Bechtel CA will reestablish the Bechtel CA keys and certificates and then all Subscriber certificates. The IS&T department may grant extensions to the Bechtel CA on a case-by-case basis.

In the case of a disaster whereby the Bechtel CA installation is physically damaged, and all copies of the Bechtel CA signature key are destroyed as a result, the Bechtel CA shall request that its certificates be revoked. The Bechtel CA installation shall then be completely rebuilt, by reestablishing the CA equipment, generating new private and public keys and being recertified. Thereafter, all Subscriber certificates shall be re-issued.

5.8 CA or RA Termination

Bechtel CA termination will be handled in accordance with Section 5.7. If the termination is for convenience, contract expiration, re-organization, or other non-security related reason, and provisions have been made to continue compromise recovery (including destruction or continued protection of signing key), compliance and security audit, archive, and data recovery services, then neither the terminated Bechtel CA certificate, nor certificates signed by the Bechtel CA, need to be revoked.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The Bechtel CA signing key pair is created during the installation of the CA and is protected by a hardware security module (HSM). The Bechtel CA key generation process complies with FIPS 140-2 Level III.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

For all Bechtel CA issued user certificates, the PKI software generates the digital signature key pair and the encryption key pair. For an encryption certificate, the private key is securely transferred to the Bechtel CA database by using the Bechtel CA's encryption certificate.

6.1.2 Private Key Delivery to Subscriber

In most cases, a private key will be generated and remain within the cryptographic boundary of a cryptographic module. If the owner of the module generates the key locally, then there is no need to deliver the Subscriber's private key. If the key is generated on a hardware cryptographic module elsewhere, then the hardware cryptographic module must be delivered to the Subscriber. Accountability for the location and state of the hardware cryptographic module must be maintained until the Subscriber is in possession of it. The Subscriber shall acknowledge receipt of the hardware cryptographic module.

6.1.3 Public Key Delivery to Certificate Issuer

The Bechtel CA verification public key is delivered in a CA certificate to internal users using Active Directory or external users accessing the Authority Information Access (AIA) URLs residing on the Internet.

6.1.4 Key Sizes

Bechtel PKI shall make reasonable effort to utilize RSA algorithm with a key length that is consistent with industry standards, in accordance with business agreements with the External Rooted CA and supported by Bechtel systems and applications.

6.1.5 Public Key Parameters Generation and Quality Checking

The Bechtel CA securely generates and protects its own private keys, using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorized usage of them. The Bechtel CA implements and documents key generation procedures, in line with this CPS.

6.1.6 Key Usage Purposes

Public keys that are bound into certificates shall be certified for use in signing or encrypting. The use of a specific key is determined by the key usage extension in the X.509 certificate.

Certificates issued by Bechtel's CA contain the key Usage certificate extension restricting the purpose to which the certificate can be applied. Certificates are further restricted by both the Enhanced Key Usage (EKU) and Application Policies extensions to define what applications a certificate may be used for.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The cryptographic module used in the Bechtel CA is designed to generate keys to comply with FIPS 140-2 Level III. For user certificates, the cryptographic modules used to generate keys must be compliant with FIPS 140-2 Level I.

6.2.2 Private Key (n out of m) Multi-Person Control

Actions which require verification by more than one administrative person include:

These actions must be authorized by a quorum of the operator card set holders.

- Issuing new subordinate CA certificates
- Renewing CA certificates
- Backing up CA private key material

In addition, a quorum of administrative card holders is required to authorize the following actions:

- Replacing a failed HSM in the security world
- Recovering a lost operator card set PIN
- Replacing the existing administrator card set with a new set

6.2.3 Private Key Escrow

Bechtel CA private keys are backed up using the Hardware Security Module's backup methods. User encryption private keys are backed up in the PKI database. A user's private signing key is never backed up at the database, in order to provide support for non-repudiation services. Private keys stored in the Bechtel CA database are encrypted and its integrity is protected by the Parent's Root PKI master keys. Only a certificate manager can extract the encrypted private key from the CA database. Once extracted, only a designated Key Recovery Agent can decrypt the private key and distribute the private key to the user.

The Bechtel CA signing key is protected by the integrated Hardware Security Module (HSM).

The encryption key pair history for all Bechtel CA subscribers, including a complete history of all decryption private keys is stored encrypted in the Bechtel CA database. The CA signing key pair is also stored in the database.

The Bechtel CA database is designed to be backed up daily. The replication data is contained within an IPSec tunnel during transport to further protect integrity of the database.

All key material used by the HSM stored on the local file system must be protected using AES encryption.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

6.2.4 Private Key Storage on Cryptographic Module

Bechtel CA signing private keys are generated in software, within the cryptographic HSM and not entered by other entities into that module. In all cases, private keys are stored encrypted in the cryptographic module and are decrypted only at the time at which they are actually being used.

Subscriber signing private keys are generated in software at the client computer. The private keys are stored encrypted in the user's profile and are protected by a reliable Data Protection API (DPAPI).

Private keys are activated at the time of subject login to the relevant PKI component occurs.

6.2.5 Method of Deactivating Private Key

The private keys remain active for the period of login. The login period is ended either by the subject logging out from the PKI application or automatically as determined by a preset timer. Each PKI user as a general default option using the PKI/Client software sets the timer.

Crypto modules, which have been activated, must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, e.g. via a manual logout procedure, or by a passive timeout. Hardware crypto modules must be deactivated, removed, and stored when not in use.

6.2.6 Method of Destroying Private Key

All sensitive keys in memory are overwritten with zeros when no longer used. Permanent destruction of private keys is achieved with secure delete operations.

Private keys should be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software crypto modules, this can be overwriting the data. For hardware tokens, this will likely be executing a "zeroize" command. Physical destruction of hardware should not be required.

6.2.7 Cryptographic Module Rating

The Bechtel CA uses appropriate cryptographic devices to perform CA key management tasks. Those cryptographic devices are known as Hardware Security Modules (HSMs).

Such devices meet formal requirements (FIPS 140-1 level 3 as minimum), which guarantee, amongst other things, that device tampering is immediately detected; and private keys cannot leave devices unencrypted.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The Bechtel CA signing key pair, user encryption public key certificates and verification public key certificates are backed up in the Certificate services database. The complete encryption key pair history and verification public key history for all end entities, including history of status changes

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

such as revocation date and reason, are stored in Active Directory in the “userCertificate” attribute of each subscriber.

The PKI database is archived according to the procedures described in section 5.5 of this CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The following lifetimes are defined for the CA hierarchy:

- Bechtel CAs: CA signing key lifetime is set to seven (7) years or as defined in the business agreement with External Root CA.
- Certificates issued to computers, users, and networks devices are defined by the individual template used with a maximum lifetime set up to three (3) years.

6.4 Activation Data

All access to Bechtel PKI components shall require a password, PIN, or other mechanism of equivalent authentication robustness shall be used to protect access to use of a private key. The activation data may be Subscriber selected. Any password or PIN shall be generated in conformance with Bechtel policy.

6.5 Computer Security Controls

The Bechtel CA system is physically secured as described in section 5.1 and the network is secured as described in section 6.7 of this CPS. The operating system enforces identification and authentication of all users.

6.6 Life Cycle Technical Controls

Quality assurance processes are employed during the system development of Certificate Services to make applications PKI-ready. A complete, separate test environment is configured to provide rigorous testing for each PKI enabled application.

Security management processes are industry standard.

6.7 Network Security Controls

Bechtel PKI shall be located on internal networks behind boundary/perimeter network defenses and afforded protections consistent with commercial electronic commerce practices for network security.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number(s)

This policy requires the Bechtel CA to issue X.509 Version 3 certificates.

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in certificate templates. Any valid X.509 version 3 certificate extensions may be included in the issued certificates.

7.1.3 Name Forms

In general, the DN will match the DN of the related Active Directory object. Some applications may require one or more alternative name formats. In this case, an alternate name form may be included in the subjectAltName (SAN) extension. If there is no DN, then the subject field of the base certificate shall be an empty sequence, and that extension shall be marked critical.

7.1.4 Name Constraints

Bechtel PKI will use names within the Bechtel domain and as permitted in any business agreements.

7.1.5 Certificate Policy Object Identifier

Certificates issued under this policy shall assert the OID appropriate to the level of assurance with which it was issued, as defined in Section 1.2.

7.2 CRL Profile

CRLs issued under this Policy shall assert a version number as described in the RFC 5280 X.509 standard.

7.3 OCSP Profile

This will be made available at the discretion of the Bechtel CA, on request from parties explaining their interest.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

An audit of the Bechtel CA operations is performed at least once annually and performed as part of the recurring ISO 27001 auditing procedures.

Additional auditing may be performed by a third-party or as established within the business agreement with the External Root.

8.2 Identity/Qualifications of Assessor

The auditor must demonstrate competence in the field of security compliance audits of Information Technology (IT) systems.

The auditor(s) for the ISO 27001 auditing team either possesses or acts under the direction of an individual with appropriate credentials.

8.3 Assessor's Relationship to Assessed Entity

The compliance audit shall be performed by an appropriately certified or recognized entity that is independent of the Bechtel CA.

8.4 Topics Covered by Assessment

The annual audit investigates the operations of the CA and RA functions of the Bechtel CA to ensure their compliance with this CPS and with other applicable PKI procedures.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the Bechtel CA and this CPS, the following actions will be taken:

- The compliance auditor shall note the discrepancy and provided recommendations if applicable
- The compliance auditor will notify those identified in Section 8.6
- The CMA shall recommend a remedy, including time for completion, to the BPMA

The BPMA will determine the appropriate remedy, up to and including revocation or non-recognition of the Bechtel CA's certificate. Upon correction of the deficiency, the BPMA may reinstate the Bechtel CA's certificate.

8.6 Communication of Results

The compliance auditor shall report the results of a compliance audit to the BPMA. The results shall be reported to the Bechtel CA and its External Root, if required. The implementation of

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

remedies shall be communicated to the appropriate authority. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The Bechtel CA provides certificates for Bechtel; as such does not sell or re-sell PKI Services.

9.2 Financial Responsibility

Issuance of certificates by the Bechtel CA and assistance in that issuance by Bechtel RA does not make Bechtel or its CA or RA an agent, fiduciary, trustee, or other representative of Subscribers, Relying Parties, or any other party.

9.3 Confidentiality of Business Information

All information that is not considered by the BPMA to be public domain information is to be kept confidential and store securely. Additional specifics are addressed in the subsections below

9.4 Privacy of Personal and Corporate Information

9.4.1 Privacy Plan

The Bechtel CA shall protect all Subscribers identifying information from unauthorized disclosure and that information shall be maintained in accordance with applicable laws.

9.4.2 Information Treated as Private

Each Subscriber's private signing key is confidential to that Subscriber. The CA and RA are not provided any access to those keys, unless otherwise stated in this CPS.

Information held in audit trails is considered confidential to Bechtel and shall not be released outside the corporation, unless required by law.

Personal and corporate information held by the Bechtel CA and RA, other than that which is explicitly published as part of a certificate, CRL, or this CPS is considered confidential and shall not be released unless required by law.

9.4.3 Information not Deemed Private

A certificate should only contain information that is relevant and necessary to effect secure transactions with the certificate.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

Information included in certificates and CRLs issued by the Bechtel CA are not considered confidential.

Confidentiality of information in the Bechtel directory is dependent on the particular data items and applications. Confidentiality of relevant information in the directory is achieved through the use of security access controls.

9.5 Intellectual Property Rights

Certificates and CRLs issued by the Bechtel CA are the property of Bechtel.

The Distinguished Names (DNs) used to represent entities within the Bechtel Active directory and in certificates issued by the Bechtel CA to end-entities within that domain, all include a Relative Distinguished Name (RDN) for Bechtel and as such are the property of Bechtel.

9.6 Representations and Warranties

9.6.1 CA and RA Representations and Warranties

As the CA and RA functions are both provided by Bechtel, the liability issues related to both functions are combined in this CPS. The phrase “the Bechtel CMA” includes all functions performed by Bechtel described in section 1.3.

9.6.1.1 Limited Warranty

THE BECHTEL CMA PROVIDES THE FOLLOWING LIMITED WARRANTY TO THE CERTIFICATE BENEFICIARIES AT THE TIME OF CERTIFICATE ISSUANCE: (A) IT ISSUED THE CERTIFICATE SUBSTANTIALLY IN COMPLIANCE WITH THIS CPS; B) THE INFORMATION CONTAINED WITHIN THE CERTIFICATE ACCURATELY REFLECTS THE INFORMATION PROVIDED TO OR AVAILABLE TO THE BECHTEL CMA IN ALL MATERIAL RESPECTS; AND (C) IT HAS TAKEN REASONABLE STEPS TO VERIFY THAT THE INFORMATION WITHIN THE CERTIFICATE IS ACCURATE. THE STEPS THE BECHTEL CMA TAKES TO VERIFY THE INFORMATION CONTAINED IN A CERTIFICATE ARE SET FORTH IN THIS CPS.

9.6.1.2 RA representations and warranties

The Bechtel RAs warrant that: (a) there are no material misrepresentations of fact in the Certificate known or originating from the entities approving the Certificate application or issuing the Certificate; (b) there are no errors in the information in the Certificate that were introduced by entities approving the Certificate application as a result of a failure to provide reasonable care in managing the Certificate application; (c) their Certificates meet all material requirements of this CPS; and (d) revocation services (when applicable) and use of a Repository comply with this CPS in all material aspects.

9.6.2 Subscriber representations and warranties

No stipulation.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

9.6.3 Relying party representations and warranties

Relying Parties represent and warrant that: (a) they have read, understand and agree to this CPS; (b) they have verified both the Bechtel CA Certificate and any other certificates in the certificate chain using the relevant CRL or OCSP; (c) they will not use a Certificate if the Certificate has expired or been revoked; (d) they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate; (c) they have studied the applicable limitations on the usage of Certificates and agree to the Bechtel CA's limitations on liability related to the use of Certificates; (d) they are solely responsible for deciding whether or not to rely on information in a Certificate; and (e) they are solely responsible for the legal and other consequences of their failure to perform the Relying Party obligations in this CPS.

Relying Parties also represent and warrant that they will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a Certificate after considering:

1. Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;

2. The intended use of the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension) or as stated in this CPS;

3. The data listed in the Certificate;

4. The economic value of the transaction or communication;

5. The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication;

6. The Relying Party's previous course of dealing with the Subscriber;

7. The Relying Party's understanding of trade, including experience with computer-based methods of trade; and

8. Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

9.7 Disclaimers of Warranties

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1. OF THIS CPS, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE BECHTEL CA DISCLAIMS ALL OTHER WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF ACCURACY OF INFORMATION PROVIDED WITH RESPECT TO CERTIFICATES ISSUED BY THE BECHTEL CMA, THE CRL, AND ANY PARTICIPANT'S OR THIRD PARTY'S PARTICIPATION IN THE BECHTEL PKI, INCLUDING USE OF KEY PAIRS, CERTIFICATES, THE CRL OR ANY OTHER GOODS OR SERVICES PROVIDED BY THE BECHTEL CMA TO THE PARTICIPANT.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1 OF THIS CPS, THE BECHTEL CMA DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE.

9.8 Limitations of Liability

Subscribers, relying parties, RAs, and owners of the CAs trusted by the qualified subordinate CA are not eligible for Compensation claims or for losses resulting from inappropriate or fraudulent use of this PKI.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BECHTEL SHALL NOT BE LIABILE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOST DATA, LOST PROFITS, LOST REVENUE OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY, INCLUDING BUT NOT LIMITED TO CONTRACT OR TORT (INCLUDING PRODUCTS LIABILITY, STRICT LIABILITY AND NEGLIGENCE), AND WHETHER OR NOT IT WAS, OR SHOULD HAVE BEEN, AWARE OR ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY STATED HEREIN. BECHTEL'S AGGREGATE LIABILITY UNDER THIS CPS IS LIMITED TO $5000.

9.9 Indemnities

The Bechtel CMA (e.g., CA, RA, Trusted Agents) assume no financial responsibility for improperly used certificates.

9.10 Term and Termination

This CPS shall remain in effect until either a new Bechtel CPS is approved by the BPMA or the Bechtel PKI is terminated.

The requirements of this CPS remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants

All parties shall use commercially reasonable methods to communicate with each other.

9.12 Amendments

The Bechtel CMA may change this CP / CPS at any time in its sole discretion and without prior notice to Subscribers or Relying Parties. The CP/ CPS and any amendments thereto are available in the Repository. Amendments to this CP / CPS will be evidenced by a new version number and date except where amendments are merely clerical.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

9.13 Dispute Resolution Provisions

Any dispute arising under this CP / CPS where a Relying Party is seeking relief of any form shall be heard exclusively in the federal or state courts of the State of Virginia.

All matters relating to the issuance, renewal, revocation, suspension of certificates for a Bechtel employee shall be decided solely by Bechtel IS&T.

Any dispute in which a Subscriber who is a Bechtel employee is seeking relief of any form from Bechtel shall be handled according to the applicable employee dispute resolution process.

9.14 Governing Law

This CPS is governed by the laws of the State of Virginia excluding (1) its choice of law principles, and (ii) the United Nations Convention on Contracts for the International Sale of Goods.

All Participants hereby submit to the exclusive jurisdiction and venue of the federal and state courts in the State of Virginia.

9.15 Miscellaneous Provisions

9.15.1 Severability

If it is determined that one section of this policy is invalid, illegal, or unenforceable, the validity, legality, and enforceability of the remainder of this CP / CPS shall not in any way be affected or impaired.

9.15.2 Enforcement (attorney's fees and waiver of rights)

Bechtel may seek indemnification and attorney's fees from a party for damages, losses, and expenses related to that party's conduct. Bechtel's failure to enforce a provision of this CP / CPS does not waive Bechtel's right to enforce the same provision later or right to enforce other provisions of this CP / CPS. To be effective, any waiver must be in writing and signed by Bechtel.

9.15.3 Force Majeure

Bechtel shall not be liable for any default or delay in the performance of its obligations under the CP / CPS to the extent and while such default or delay is caused, directly or indirectly, by fire; flood; earthquake; elements of nature or acts of God; acts or war; acts of terrorism; acts of cyber terrorism or cyber-security events; riots; civil disorders; rebellions or revolutions in the United States; strikes, lockouts, labor difficulties, or any similar cause beyond the control of Bechtel.

10. LIST OF DEFINITIONS

ACCEPT (A CERTIFICATE)
To approve of a digital certificate by a certificate applicant within a transactional framework
ACCREDITATION

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

A formal declaration by an approving authority that a certain function/entity meets specific formal requirements

AFFILIATED ORGANIZATION
An organization that has a relationship with a subscriber and sponsors that subscriber for obtaining a certificate

APPLICATION FOR A CERTIFICATE
A request sent by a certificate applicant to a CA to issue a digital certificate

APPLICATION SOFTWARE VENDOR:
A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc

ARCHIVE
To store records for period of time for purposes such as security, backup, or audit.

ASSURANCES
A set of statements or conduct aiming at conveying a general intention

AUDIT
Procedure used to validate compliance with formal criteria or controls

AUTHENTICATION
A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship

AUTHORISATION
Granting of rights

AVAILABILITY
The rate of accessibility of information or resources

BECHTEL AFFILIATE
Any entity under the common ownership or control as Bechtel Global Corporation or any legal or contractual joint venture, project, or arrangement in which Bechtel has at least a 20 percent interest and for which Bechtel provides information technology services including Certificate Authority functions.

BECHTEL CA PUBLIC CERTIFICATION SERVICES
A digital certification system made available by Bechtel CA as well as the entities that belong to the Bechtel CA domain as described in this CPS

BECHTEL CA PROCEDURESA document describing the Bechtel CA's internal procedures with regard to registration of end users, security. etc.

BECHTEL POLICY MANAGEMENT AUTHORITY (BPMA)
The Bechtel Policy Management Authority (BPMA) is defined in Section 1.3.1.

CERTIFICATE
The public key of a subject and the associated information, digitally signed with the private key of the issuer of the certificate. Unless explicitly specified, the certificates described here are the subscriber's certificates

CERTIFICATE REVOCATION LIST OR CRL
A list maintained by the CA of certificates that are revoked before their expiration time

CERTIFICATION AUTHORITY OR CA
An entity that is trusted to associate a public key to the information on the subject, contained in the certificate. Unless explicitly specified, the CA described herein is the Bechtel CA

CERTIFICATION PRACTICE STATEMENT OR CPS
A statement of the practices in the management of certificates during all life phases

CERTIFICATE CHAIN
A hierarchical list certificates containing a subscriber certificate and CA certificates

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

CERTIFICATE EXPIRATION
The end of the validity period of a digital certificate
CERTIFICATE EXTENSION
A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subscriber, the certificate issuer, and/or the certification process
CERTIFICATE HIERARCHY
A level-based sequence of certificates of one (root) CA and subordinate entities that include, CAs and subscribers
CERTIFICATE MANAGEMENT
Actions associated with certificate management include storage, dissemination, publication, revocation, and suspension of certificates.
CERTIFICATE MANAGEMENT AUTHORITY (CMA)
Certificate Authorities (CAs), Registration Authorities (RAs), Server-based Certificate Status Authorities (CSAs) such as Online Certificate Status Protocol (OCSP) Responders and Server-based Certificate Validation Protocol (SCVP) status providers operated by Bechtel. Each is separately or some combination of the functions collectively is a Certificate Management Authority (CMA).
CERTIFICATE REVOCATION LIST (CRL)
A list issued and digitally signed by a CA that includes revoked and suspended certificates. Such list is to be consulted by relying parties at all times prior to relying on information featured in a certificate
CERTIFICATE SERIAL NUMBER
A sequential number that uniquely identifies a certificate within the domain of a CA
CERTIFICATE SIGNING REQUEST (CSR)
A machine-readable application form to request a digital certificate
CERTIFICATION
The process to issue a digital certificate
CERTIFICATION AUTHORITY (CA)
An authority, such as Bechtel CA that issues, suspends, or revokes a digital certificate
CERTIFICATE POLICY (CP)
A statement of the practices of a CA and the conditions of issuance, suspension, revocation etc. of a CA certificate
CERTIFICATE ISSUANCE
Delivery of X.509 v3 digital certificates
CERTIFICATE SUSPENSION
Online service used to temporarily disable a digital certificate and to automatically revoke it if no request for re-activating it is submitted within a certain time period
CERTIFICATE REVOCATION
Online service used to permanently disable a digital certificate before its expiration date
CERTIFICATE REVOCATION LISTS
Online publication of complete and incremental digital certificates revocation lists compliant with
COMMERCIAL REASONABLENESS
A legal term from Common Law, in electronic commerce it means the usage of technology that provide reasonable assurance of trustworthiness
COMPROMISE
A violation of a security policy that results in loss of control over sensitive information
CONFIDENTIALITY
The condition to disclose data to selected and authorized parties only
CONFIRM A CERTIFICATE CHAIN

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

To validate a certificate chain in order to validate an end-user subscriber certificate

CRYPTOGRAPHIC MODULE

The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module [FIPS140-]

DIGITAL CERTIFICATE

A formatted piece of data that relates an identified subject with a public key the subject uses

DIGITAL SIGNATURE

To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made

DISTINGUISHED NAME

A set of data that identifies a real-world entity, such as a person in a computer-based context

DIRECTORY SERVICE

Online publication of certificates allowing the retrieval of a certificate based on its certificate identifier

END-ENTITY

A person or device

END-USER SUBSCRIBER

A subscriber other than another CA

EXTENSIONS

Extension fields in X.509 v.3.0 certificates

GENERATE A KEY PAIR

A trustworthy process to create private keys during certificate application whose corresponding public key are submitted to the applicable CA during certificate application in a manner that demonstrates the applicant's capacity to use the private key

GOVERNMENT ENTITY

A government-operated legal entity, agency, department, ministry, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.)

HASH

An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

IDENTIFICATION

The process to confirm the identity of an entity. Identification is facilitated in public key cryptography by means of certificates

INCORPORATE BY REFERENCE

To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message

KEY GENERATION PROCESS

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

The trustworthy process of creating a private/public key pair. The public key is supplied to a CA during the certificate application process

KEY PAIR

A private key and its corresponding public key in asymmetric encryption

NOTICE

The result of notification to parties involved in receiving CA services in accordance with this CPS

NOTIFY

To communicate specific information to another person as required by this CPS and applicable law

OBJECT IDENTIFIER

A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain

OPERATIONAL/FUNCTIONAL ROLE MANAGER

A person who is responsible for managing the Operational/Functional Role, including assigning individuals to the Operational/Functional Role membership and maintaining the list of Operational/Functional Role members and public key certificates issued to them

OCSP RESPONDER

A trusted entity that provides on-line revocation status of certificates to Relying Parties. The OCSP Responder is either explicitly trusted by the Relying Party, or through the CA that issued the certificate whose revocation status is being sought.

PKI HIERARCHY

A set of CAs whose functions are organized according to the principle of delegation of authority and related to each other as subordinate and superior CA

PKI SPONSOR

Fills the role of a Subscriber for non-human system components or organizations that are named as public key certificate subjects and is responsible for meeting the obligations of Subscribers as defined throughout this document.

PRIVATE KEY

A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key

PUBLIC KEY

A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.

PUBLIC KEY CRYPTOGRAPHY

Cryptography that uses a key pair of mathematically related cryptographic keys

PUBLIC KEY INFRASTRUCTURE (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system

REGISTERED AGENT

An individual or entity that is both authorized by the Applicant to receive service of process and business communications on behalf of the Applicant

REGISTERED OFFICE

The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and legal notices received

REGISTRATION NUMBER

The unique number assigned to the Private organization Applicant or Subject entity by the Incorporating Agency in such entity's Jurisdiction of Incorporation

REGISTRATION AUTHORITY OR RA

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.

RELIANCE
To accept a digital signature and act in a way that shows trust in it

RELYING PARTY
Any entity that relies on a certificate for carrying out any action

REPOSITORY
A database and/or directory listing digital certificates and other relevant information accessible on-line

REVOKE A CERTIFICATE
To permanently end the operational period of a certificate from a specified time forward

ROOT CA
In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain

SIGNATURE
A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances

SIGNER
A person who creates a digital signature for a message, or a signature for a document

SMART CARD
A hardware token that contains a chip to implement among others cryptographic functions

STATUS VERIFICATION
Online service based on the Online Certificate Status Protocol (RFC 2560) used to determine the current status of a digital certificate without requiring CRLs

SUBJECT OF A DIGITAL CERTIFICATE
The named party to which the public key in a certificate is attributable, as user of the private key corresponding to the public key

SUBSCRIBER
The subject of a digital certificate, or a party designated by the subject to apply for the certificate

SUBSCRIBER AGREEMENT
The agreement between a subscriber and a CA for the provision of public certification services

TRUSTED AGENT
Entity authorized to act as a representative of a Certificate Management Authority in providing Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

TRUSTED POSITION
A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, suspension, or revocation of certificates, including operations that restrict access to a repository

TRUSTWORTHY SYSTEM
Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy

WEB -- WORLD WIDE WEB (WWW)
A graphics based medium for the document publication and retrieval of information on

WRITING
Information accessible and usable for reference

X.509

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

The standard of the ITU-T (International Telecommunications Union-T) for digital certificates

ZEROIZE

A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS140]

11. LIST OF ACRONYMS

AES: Advanced Encryption Standard
BPMA: Bechtel Policy Management Authority
CA: Certification Authority
CMA: Certificate Management Authority
CP: Certificate Policy
CPS: Certification Practice Statement
CRL: Certificate Revocation List
CSA: Certificate Status Authority
DACL: Discretionary Access Control List
DES: Data Encryption Standard
DN: Distinguished Name
FIPS: Federal Information Processing Standard
FTP: File Transfer Protocol
IETF: Internet Engineering Task Force
ISO: International Standards organization
IT: Information Technology
ITU: International Telecommunications Union
IS&T Information Systems & Technology
KRA: Key Recovery Agent
OCSP: Online Certificate Status Protocol
PKI: Public Key Infrastructure
RA: Registration Authority
RDN: Relative Distinguished Name
RFC: Request for Comments
RSA: Rivest, Shamir, Adleman (encryption and digital signature algorithm)
SCVP: Server-based Certificate Validation Protocol
SHA: Secure Hash Algorithm
SSL: Secure Sockets Layer
TA: Trusted Agent
USD: United States Dollar

REFERENCES

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile. (obsoletes RFC 3280)
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.

- ISO/IEC 27001 Information Security Management System
- RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile. (obsoletes RFC 3039)
- RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP(obsoletes RFC 2560)

Electronic documents, once printed, are uncontrolled and may become outdated. Refer to the electronic documents for current revisions.

Bechtel Level 3 – General. Non-confidential business information.
© 2009 - 2025 Bechtel Global Corporation (Bechtel). All rights reserved.