CHEVRON U.S.A. INC.  
PUBLIC KEY INFRASTRUCTURE  
Root Certificate Authority Set of Provisions  
Version 2  

Approved by the Chevron Policy Management Authority on December 20, 2012
LEGAL DISCLAIMER

No portion of this document is intended or shall be considered to be legal advice. All materials are provided for informational purposes only. The reader shall not act or abstain from acting based on such information without first consulting a qualified attorney.
# TABLE OF CONTENTS

1. **INTRODUCTION** .................................................................................................................. 1
   1.1 OVERVIEW ......................................................................................................................... 1
   1.2 DOCUMENT NAME AND IDENTIFICATION .................................................................... 4
   1.3 PKI PARTICIPANTS ............................................................................................................ 4
      1.3.1 Certification Authorities ............................................................................................... 4
      1.3.2 Registration Authorities ............................................................................................... 5
      1.3.3 Subscribers .................................................................................................................. 5
      1.3.4 Relying Parties ............................................................................................................ 6
      1.3.5 Other Participants ........................................................................................................ 6
   1.4 CERTIFICATE USAGE ........................................................................................................ 6
      1.4.1 Appropriate Certificate Uses ....................................................................................... 6
      1.4.2 Prohibited Certificate Uses ......................................................................................... 6
   1.5 POLICY ADMINISTRATION ............................................................................................... 6
      1.5.1 Organization Administering the Document ................................................................. 6
      1.5.2 Contact Person ............................................................................................................ 6
      1.5.3 Person Determining CPS Suitability for the Policy .................................................... 6
      1.5.4 CPS Approval Procedure ............................................................................................ 7
   1.6 DEFINITIONS AND ACRONYMS ...................................................................................... 7

2. **PUBLICATION AND REPOSITORY RESPONSIBILITIES** ............................................. 13
   2.1 REPOSITORIES ................................................................................................................. 13
   2.2 PUBLICATION OF CERTIFICATION INFORMATION .................................................. 13
   2.3 TIME OR FREQUENCY OF PUBLICATION .................................................................... 13
   2.4 ACCESS CONTROLS ON REPOSITORIES .................................................................... 13

3. **IDENTIFICATION AND AUTHENTICATION** ................................................................. 14
   3.1 NAMING ............................................................................................................................. 14
      3.1.1 Types of Names .......................................................................................................... 14
      3.1.2 Need For Names To Be Meaningful .......................................................................... 14
3.1.3 Anonymity or Pseudonymity of Subscribers ............................................. 14
3.1.4 Rules for Interpreting Various Name Forms ............................................. 14
3.1.5 Uniqueness of Names .............................................................................. 14
3.1.6 Recognition, Authentication, and Role of Trademarks ............................... 14

3.2 INITIAL IDENTITY VALIDATION ..................................................................... 15
3.2.1 Method to Prove Possession of Private Key ............................................... 15
3.2.2 Authentication of Organization Identity ....................................................... 15
3.2.3 Authentication of Individual Identity .......................................................... 15
3.2.4 Non-Verified Subscriber Information ......................................................... 15
3.2.5 Validation of Authority .............................................................................. 15
3.2.6 Criteria for Interoperation ........................................................................ 15

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS .......... 15
3.3.1 Identification and Authentication for Routine Re-key ................................. 15
3.3.2 Identification and Authentication for Re-key After Revocation ................. 16

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST .... 16

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .......................... 17
4.1 CERTIFICATE APPLICATION ........................................................................ 17
4.1.1 Who Can Submit a Certificate Application ............................................... 17
4.1.2 Enrollment Process and Responsibilities ...................................................... 17
4.2 CERTIFICATE APPLICATION PROCESSING ................................................ 17
4.2.1 Performing Identification and Authentication Functions .......................... 17
4.2.2 Approval or Rejection of Certificate Applications ....................................... 17
4.2.3 Time to Process Certificate Applications .................................................. 17
4.3 CERTIFICATE ISSUANCE ............................................................................ 17
4.3.1 CA Actions During Certificate Issuance ..................................................... 17
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate ............... 18
4.4 CERTIFICATE ACCEPTANCE ....................................................................... 18
4.4.1 Conduct Constituting Certificate Acceptance .............................................. 18
4.4.2 Publication of the Certificate by the CA ....................................................... 18
4.4.3 Notification of Certificate Issuance by the CA to Other Entities ............... 18
4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

4.5.2 Relying Party Public Key and Certificate Usage

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

4.6.2 Who May Request Renewal

4.6.3 Processing Certificate Renewal Requests

4.6.4 Notification of New Certificate Issuance to Subscriber

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

4.6.6 Publication of the Renewal Certificate by the CA

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-Key

4.7.2 Who May Request Certification of a New Public Key

4.7.3 Processing Certificate Re-Keying Requests

4.7.4 Notification of New Certificate Issuance to Subscriber

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

4.7.6 Publication of the Re-Keyed Certificate by the CA

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

4.8 CERTIFICATE MODIFICATION

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

4.9.2 Who Can Request Revocation

4.9.3 Procedure for Revocation Request

4.9.4 Revocation Request Grace Period

4.9.5 Time Within Which CA Must Process the Revocation Request

4.9.6 Revocation Checking Requirement for Relying Parties

4.9.7 CRL Issuance Frequency

4.9.8 Maximum Latency for CRLs

4.9.9 On-Line Revocation/Status Checking Availability
4.9.10 On-Line Revocation Checking Requirements ........................................... 23
4.9.11 Other Forms of Revocation Advertisements Available ................................... 23
4.9.12 Special Requirements re Key Compromise ................................................. 23
4.9.13 Circumstances for Suspension ..................................................................... 23
4.9.14 Who Can Request Suspension .................................................................... 24
4.9.15 Procedure for Suspension Request ............................................................. 24
4.9.16 Limits on Suspension Period ........................................................................ 24

4.10 CERTIFICATE STATUS SERVICES .................................................................. 24
4.10.1 Operational Characteristics ........................................................................ 24
4.10.2 Service Availability ................................................................................... 24
4.10.3 Operational Features .................................................................................. 24

4.11 END OF SUBSCRIPTION ................................................................................ 24

4.12 KEY ESCROW AND RECOVERY .................................................................... 24
4.12.1 Key Escrow and Recovery Policy and Practices .......................................... 24
4.12.2 Session Key Encapsulation and Recovery Policy and Practices .................. 24

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS ...................... 25

5.1 PHYSICAL CONTROLS ................................................................................... 25
5.1.1 Site Location and Construction .................................................................... 25
5.1.2 Physical Access ............................................................................................ 25
5.1.3 Power and Air Conditioning ......................................................................... 26
5.1.4 Water Exposures ......................................................................................... 26
5.1.5 Fire Prevention and Protection ..................................................................... 26
5.1.6 Media Storage .............................................................................................. 26
5.1.7 Waste Disposal ............................................................................................ 27
5.1.8 Off-Site Backup ........................................................................................... 27

5.2 PROCEDURAL CONTROLS .......................................................................... 27
5.2.1 Trusted Roles ............................................................................................... 27
5.2.2 Number of Persons Required Per Task ....................................................... 28
5.2.3 Identification and Authentication for Each Role ......................................... 29
5.2.4 Roles Requiring Separation of Duties ......................................................... 29
5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

5.3.2 Background Check Procedures

5.3.3 Training Requirements

5.3.4 Retraining Frequency and Requirements

5.3.5 Job Rotation Frequency and Sequence

5.3.6 Sanctions for Unauthorized Actions

5.3.7 Independent Contractor Requirements

5.3.8 Documentation Supplied to Personnel

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

5.4.2 Frequency of Processing Log

5.4.3 Retention Period for Audit Log

5.4.4 Protection of Audit Log

5.4.5 Audit Log Backup Procedures

5.4.6 Audit Collection System (Internal vs. External)

5.4.7 Notification to Event-Causing Subject

5.4.8 Vulnerability Assessments

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

5.5.2 Retention Period for Archive

5.5.3 Protection of Archive

5.5.4 Archive Backup Procedures

5.5.5 Requirements for Time-Stamping of Records

5.5.6 Archive Collection System (Internal or External)

5.5.7 Procedures to Obtain and Verify Archive Information

5.6 KEY CHANGEOVER

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

5.7.2 Computing Resources, Software, and/or Data Are Corrupted
5.7.3 Entity Private Key Compromise Procedure ...........................................34
5.7.4 Business Continuity Capabilities After a Disaster ...............................34
5.8 CA OR RA TERMINATION ........................................................................34

6. TECHNICAL SECURITY CONTROLS .........................................................35

6.1 KEY PAIR GENERATION AND INSTALLATION ......................................35
   6.1.1 Key Pair Generation ...........................................................................35
   6.1.2 Private Key Delivery to Subscriber ....................................................35
   6.1.3 Public Key Delivery to Certificate Issuer ...........................................35
   6.1.4 CA Public Key Delivery to Relying Parties .......................................35
   6.1.5 Key Sizes .........................................................................................35
   6.1.6 Public Key Parameters Generation and Quality Checking ..................36
   6.1.7 Key Usage Purposes .........................................................................36

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS ...............................................................36
   6.2.1 Cryptographic Module Standards and Controls .................................36
   6.2.2 Private Key (N out of M) Multi-Person Control ..................................36
   6.2.3 Private Key Escrow ..........................................................................36
   6.2.4 Private Key Backup ..........................................................................37
   6.2.5 Private Key Archival .........................................................................37
   6.2.6 Private Key Transfer Into or From a Cryptographic Module .............37
   6.2.7 Private Key Storage on Cryptographic Module .................................37
   6.2.8 Method of Activating Private Key .....................................................37
   6.2.9 Method of Deactivating Private Key ................................................37
   6.2.10 Method of Destroying Private Key ..................................................38
   6.2.11 Cryptographic Module Rating .......................................................38

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT ..................................38
   6.3.1 Public Key Archival .........................................................................38
   6.3.2 Certificate Operational Periods and Key Pair Usage Periods .............38

6.4 ACTIVATION DATA ..................................................................................38
   6.4.1 Activation Data Generation and Installation ......................................38
6.4.2 Activation Data Protection ................................................................. 38
6.4.3 Other Aspects of Activation Data ...................................................... 39

6.5 COMPUTER SECURITY CONTROLS .......................................................... 39
6.5.1 Specific Computer Security Technical Requirements ............................ 39
6.5.2 Computer Security Rating ................................................................. 39

6.6 LIFE CYCLE TECHNICAL CONTROLS ...................................................... 39
6.6.1 System Development Controls .......................................................... 39
6.6.2 Security Management Controls ......................................................... 39
6.6.3 Life Cycle Security Controls .............................................................. 39

6.7 NETWORK SECURITY CONTROLS .......................................................... 40
6.8 TIME-STAMPING ................................................................................. 40

7. CERTIFICATE, CRL, AND OCSP PROFILES ............................................ 41
7.1 CERTIFICATE PROFILE ......................................................................... 41
7.2 CRL PROFILE ....................................................................................... 45
7.3 OCSP PROFILE ..................................................................................... 46

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS .................................. 47
8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT ......................... 47
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR ........................................ 47
8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY .............................. 47
8.4 TOPICS COVERED BY ASSESSMENT ................................................... 48
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY .................................. 48
8.6 COMMUNICATION OF RESULTS ............................................................ 48

9. OTHER BUSINESS AND LEGAL MATTERS ............................................. 49
9.1 FEES ..................................................................................................... 49
9.2 FINANCIAL RESPONSIBILITY ................................................................ 49
9.2.1 Insurance Coverage ......................................................................... 49
9.2.2 Other Assets .................................................................................... 49
9.2.3 Insurance or Warranty Coverage for End-Entities ............................... 49
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION ............................... 49
9.3.1 Scope of Confidential Information ................................................... 49
9.3.2 Information Not Within the Scope of Confidential Information ........................................50
9.3.3 Responsibility to Protect Confidential Information .........................................................50
9.4 PRIVACY OF PERSONAL INFORMATION .....................................................................50
9.5 INTELLECTUAL PROPERTY RIGHTS .........................................................................50
9.6 REPRESENTATIONS AND WARRANTIES ...........................................................................50
  9.6.1 CA Representations and Warranties ...........................................................................50
  9.6.2 RA Representations and Warranties ..........................................................................50
  9.6.3 Subscriber Representations and Warranties .................................................................50
  9.6.4 Relying Party Representations and Warranties ...............................................................51
  9.6.5 Representations and Warranties of Other Participants ...................................................52
9.7 DISCLAIMER OF WARRANTIES .......................................................................................52
9.8 LIMITATIONS OF LIABILITY .........................................................................................52
9.9 INDEMNITIES ..................................................................................................................52
9.10 TERM AND TERMINATION ............................................................................................52
  9.10.1 Term .........................................................................................................................52
  9.10.2 Termination ...............................................................................................................52
  9.10.3 Effect of Termination and Survival .............................................................................53
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS ..................53
9.12 AMENDMENTS ..............................................................................................................53
  9.12.1 Procedure for Amendment .......................................................................................53
  9.12.2 Notification Mechanism and Period ..........................................................................53
  9.12.3 Circumstances Under Which OID Must Be Changed .................................................53
9.13 DISPUTE RESOLUTION PROVISIONS .........................................................................53
9.14 GOVERNING LAW .........................................................................................................54
9.15 COMPLIANCE WITH APPLICABLE LAW ....................................................................54
9.16 MISCELLANEOUS PROVISIONS ..................................................................................54
  9.16.1 Entire Agreement .......................................................................................................54
  9.16.2 Assignment ...............................................................................................................54
  9.16.3 Severability ...............................................................................................................55
  9.16.4 Enforcement (Attorneys’ Fees and Waiver of Rights) ...................................................55
9.16.5 Force Majeure........................................................................................................55
9.17 OTHER PROVISIONS..................................................................................................55
  9.17.1 Conflict of Provisions ..........................................................................................55
  9.17.2 Limitation Period on Actions ............................................................................55
1. INTRODUCTION

1.1 OVERVIEW

This combined Certificate Policy (CP) and Certification Practices Statement (CPS) or Set of Provisions (SoP), written in accordance with the RFC 3647 framework, defines the requirements applicable to and certification practices of the Root Certification Authority (CA) within the Public Key Infrastructure (PKI) operated by Chevron U.S.A. Inc. (Chevron) and its affiliates. This SoP defines an internal Chevron PKI for use solely by Chevron and its employees; persons or entities outside Chevron are not authorized to receive or rely upon certificates issued within the Chevron PKI except as provided by separate written agreement, that is a Relying Party Agreement, with Chevron. The Chevron PKI is hierarchical in form with a single Root, and multiple Intermediate and Issuing Certification Authorities that are subordinate to that Root. These CAs are collectively known as the “Chevron PKI Domain.” The relationships among the CAs are illustrated in Figure 1, below. The Intermediate CAs also have their own SoP, while the Issuing CAs have their own SoPs.
The governing bodies of this PKI are the Chevron Policy Management Authority (PMA), the Chevron Policy Authority (PA), the Chevron Identity Management and Architecture Authority (IMAA), and the Chevron General Manager of Information Risk Strategy and Management (GM-IRSM). The PMA, PA, IMAA and GM-IRSM will be staffed from within Chevron. The PMA will consist of one or more members from the Chevron Council of Chief Information Officers (CIOs), the PA, IMAA and GM-IRSM. The relationships are illustrated in Figure 2.
The PMA is the broad policymaker with enterprise-wide oversight authority for the overall operation of the Chevron PKI. Its responsibilities include, but are not limited to, approving the SoPs for the Root, Intermediate, and Issuing CAs, approving Cross-Certification Agreements; approving trust relationships with Bridge Certification Authorities (BCAs); exercising oversight authority for the PKI as a whole; appointing the PA and IMAA; and reviewing the reports of the auditors regarding the PKI.

The PA is responsible for reviewing the legal and contractual aspects of the SoP, CP and CPS documents for Chevron; reviewing the legal and contractual aspects of any Cross-Certification Agreements with external CAs; reviewing any agreements with BCAs; and, reviewing the SoP, CP, and CPS documents to ensure consistency.

The IMAA operates the PKI in accordance with the approved documents, ensures that certificates are issued in accordance with the respective documents, and provides technical guidance regarding those documents. In addition, the IMAA creates facilities and a management structure consistent with the SoP, oversees the operations of the PKI, and develops a business continuity plan for the PKI.

The GM-GIRM advises the PMA on information security and PKI related issues. The GM-GIRM ensures that PKI operations conform to Chevron’s security policy and standards.

The relationships among the Chevron Root, Intermediate, and Issuing CAs, End-Entities and Relying Parties are governed by the terms and conditions in the following documents, where applicable: the Chevron Root CA’s Set of Provisions, the Intermediate CAs’ Set of Provisions, the Issuing CAs’ Set of Provisions, any other SoP for which a Chevron Intermediate CA or Issuing CA has issued a certificate or cross-certification certificate, Cross-Certification Agreements, Bridge Certification Agreements, Relying Party Agreements and Subscriber Agreements.

This Set of Provisions defines two (2) types of certificates issued by the Chevron Root CA:
• **Root CA Certificate:** The Root CA certificate is a self-signed certificate issued to the Chevron Root CA by the Chevron Root CA.

• **Intermediate CA Certificate:** An Intermediate CA certificate is issued and signed by the Root CA for each Intermediate CA participating in the Chevron PKI.

### 1.2 DOCUMENT NAME AND IDENTIFICATION

This SoP is called the “Chevron Root CA Set of Provisions”. The OID for this document is 1.3.6.1.4.1.6646.114176.37.1.1.1.2.

This SoP is represented by an “object identifier” (OID), which is a numeric string contained in each certificate issued by this Intranet Issuing CA. In addition, pursuant to RFC 5280, the policyQualifierInfo field may contain the URI of this SoP. To ensure interoperability and uniqueness of that OID for customers, Chevron has registered the OIDs following the procedures specified in ISO/IEC and ITU standards. Chevron U.S.A. Inc. is registered as 1.3.6.1.4.1.6646.

This SoP level has been assigned a unique OID subordinate to the Chevron OID, having a root of 1.3.6.1.4.1.6646.114176.37.1.1.1.x where x is equal to 1 and is henceforth incremented by 1 for each revision of the SoP.

### 1.3 PKI PARTICIPANTS

This SoP describes the Chevron PKI, which accommodates a worldwide, public and widely distributed community of wired and wireless users with diverse needs for communications and information security. The Root CA is the portion of that PKI that is regulated by this document.

This document discusses a PKI consisting of one (1) Root CA, two (2) Intermediate CAs and three (3) Issuing CAs as illustrated in Figure 1. Additional Intermediate CAs and Issuing CAs may be added at a later date. The entities participating in the Chevron PKI are the Root CA as described in Section 1.3.1.1; the Intermediate CAs as described in Section 1.3.1.2; the Issuing CAs as described in Section 1.3.1.3; the Subscribers of the Root, Intermediate, and Issuing CAs; and, Relying Parties. Except as expressly authorized by separate agreement with Chevron, no person or entity outside Chevron shall have any rights or obligations under this SoP.

### 1.3.1 Certification Authorities

Where necessary, this document distinguishes the different users and roles accessing the CA functions. Where this distinction is not required, the term “Certification Authority” is used to refer to the total Certification Authority entity, including the software and its operations.

#### 1.3.1.1 Chevron Root CA

The Certification Authority that:

- Creates, signs, distributes and revokes certificates binding the X.500 Distinguished Name of Intermediate CAs with its respective signature verification key
- Promulgates certificate status through Certificate Revocation Lists (CRL)
Has designed and implemented, and operates its certification practices to reasonably achieve the requirements of this document.

The Chevron Root CA IMAA is responsible for ensuring that the practices the Chevron Root CA employs in issuing certificates and certificate revocation lists are in accordance with this SoP.

1.3.1.2 Chevron Intermediate Certification Authorities

Within the Chevron PKI there are two Intermediate CAs: an Extranet Intermediate CA and an Intranet Intermediate CA. Each Intermediate CA:

- Creates, signs, distributes and revokes certificates binding the X.500 Distinguished Name of Issuing CAs with its respective signature verification key
- Promulgates certificate status through CRLs

Each Chevron Intermediate CA may have its own IMAA as opposed to a single IMAA for the entire Chevron PKI. The respective Intermediate CA IMAA is responsible for ensuring that the practices employed by each Chevron Intermediate CA when issuing certificates and certification lists are in accordance with its SoP.

1.3.1.3 Chevron Issuing Certification Authorities

Within the Chevron PKI there are multiple Issuing CAs, each subordinate to a specific Intermediate CA. Each Issuing CA:

- Creates, signs, distributes and revokes certificates binding the X.500 Distinguished Name of Subscribers with its respective signature verification key
- Promulgates certificate status through CRLs and delta CRLs

Each Chevron Issuing CA may have its own IMAA as opposed to a single IMAA for the entire Chevron PKI. The respective Issuing CA IMAA is responsible for ensuring that the practices employed by each Chevron Issuing CA when issuing certificates, as may be more comprehensively described in the respective Chevron Issuing CA CPS, are consistent with its respective CP.

The Chevron Issuing CAs’ IMAAs are responsible for the operation of the Chevron Issuing CAs in accordance with their corresponding CP.

1.3.2 Registration Authorities

While not an independent RA, the Chevron Root CA registration process is responsible for providing identification and authentication of the Chevron Intermediate CAs. The Chevron Root CA will not serve as an RA for any other CA in the PKI.

1.3.3 Subscribers
The Chevron Intermediate CAs are the sole Subscribers to this CA. In this PKI the Chevron Root CA will not issue certificates to End-Entities. Only the Issuing CAs can issue certificates to End-Entities.

1.3.4 **Relying Parties**

A Relying Party is an individual or software agent that relies on the data within a certificate in making decisions. Except as expressly authorized by separate agreement with Chevron, no person or entity outside Chevron shall be considered a Relying Party.

1.3.5 **Other Participants**

No stipulation - this section intentionally left blank.

1.4 **CERTIFICATE USAGE**

This Set of Provisions defines two (2) types of certificates issued by the Chevron Root CA:

- **Root CA Certificate:** The Root CA certificate is a self-signed certificate issued to the Chevron Root CA by the Chevron Root CA.

- **Intermediate CA Certificates:** The Intermediate CA certificates are issued and signed by the Root CA for each Intermediate CA participating in the Chevron PKI. This certificate is used to verify the signature of the certificates issued by the Intermediate CAs.

1.4.1 **Appropriate Certificate Uses**

The Root CA Certificate is the Trust Anchor of this PKI. Both the Root CA Certificate and the respective Intermediate CA Certificate are used when performing certificate path validation as described in RFC 3280.

1.4.2 **Prohibited Certificate Uses**

No stipulation - this section intentionally left blank.

1.5 **POLICY ADMINISTRATION**

1.5.1 **Organization Administering the Document**

The Chevron PA administers this SoP as part of a larger set of provisions adopted by the Chevron PMA.

1.5.2 **Contact Person**

Contact your Chevron Sponsor for questions regarding this policy. Your Chevron Sponsor will be able to submit your question on your behalf to the Chevron IT Service Desk. A ticket will be open with the appropriate IT team in order to address the question.
1.5.3 **Person Determining CPS Suitability for the Policy**

No stipulation - this section intentionally left blank.

1.5.4 **CPS Approval Procedure**

The Chevron PMA shall approve this SoP and any subsequent changes; see Section 9.12 Amendments, for additional information.

1.6 **DEFINITIONS AND ACRONYMS**

The terms and acronyms used in this PKI, but not necessarily in this SoP, are defined below; the source of a definition is cited when known. Note that certain technical terms are case-sensitive and may begin with a lower case letter, for example commonName.

**ACS** – Administrative Card Share is part of an administrator card set authorized to participate in N of M administration of an nCipher Security World.

**Activation data** – Data values, other than keys, that are required to operate cryptographic modules and that need to be protected, for example, a PIN, a pass-phrase, or a manually held key share. (RFC 3647)

**AICPA** – American Institute of Certified Public Accountants.

**Arc** – A unique path from the root of the global OID registration tree to a particular node within that tree. Comprised of one or more sub-arcs.

**ARL** – Authority Revocation List, a CRL that lists revoked CA certificates.

**ASN.1** – Abstract Symbolic Notation 1. A formal mathematical way of defining and relating objects. Used in many RFCs and technical specifications.

**Badging Officer** – A person, acting in a LRA role, who verifies the identity of an individual.

**Blocking** – Violation of smart card security policies can result in the "blocking" of the smart card, rendering it inactive.

**CA** – Certification Authority

**CA-certificate** – A certificate for one CA’s public key issued by another CA. (RFC 3647)

**CCTV** – Closed Circuit TV

**CDP** – Certificate Distribution Point

**Certificate Manager** – A trusted role in Microsoft CA Server that is authorized to approve, deny, and revoke certificates.

**Certification path** – An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path. (RFC 3647)

**Certificate Policy (CP)** – 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. For example, a particular CP might indicate applicability of a type of certificate to the
authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. (RFC 3647)

**Certification Practices Statement (CPS)** – A statement of the practices that a CA employs in issuing, managing, revoking and renewing or re-keying certificates. (RFC 3647)

**CIS** – Schlumberger’s Card Issuance System

**CMC** – Certificate Management Messages over Cryptographic Message Syntax, a message format used to convey a request for one or more certificates to a registration manager or certificate manager. See RFC 2797. Incorporates PKCS #7 and PKCS #10.

**CMS** – Schlumberger’s Card Management System

**commonName (CN)** – The Common Name attribute type specifies an identifier of an object. A Common Name is not a directory name; it is a (possibly ambiguous) name by which the object is commonly known in some limited scope (such as an organization) and conforms to the naming conventions of the country or culture with which it is associated. (Recommendation X.520)

**CPA** – Certified Public Accountant

**CRL** – Certificate Revocation List

**Cross-certificate** – A certificate issued to a CA by another CA.

**CSP** – Cryptographic Service Provider, a Microsoft term for an object that provides cryptographic services. It can be either the Windows operating system, a smart card, or an HSM.

**CSR** – Certificate Signing Request

**DES** – Data Encryption Standard, a symmetric encryption algorithm.

**DRP** – Disaster Recovery Plan

**DMZ** – Demilitarized Zone, a portion of an organization’s network outside of the Intranet but still under that organization’s management and control.

**DN** – Distinguished Name

**End-Entity (EE)** – A subject of a certificate, who is not a CA in the PKI. (PKIX Road Map)

**FBCA** – Federal Bridge Certification Authority

**FIPS** – Federal Information Processing Standards, developed by the United States Federal Government.

**FIPS 140-1 and FIPS 140-2** – Standards for HSMs. FIPS 140-2 has recently superseded FIPS 140-1.

**Hardware Security Module (HSM)** – A device designed to provide cryptographic functions, especially the safekeeping of a private key.

**HTTP** – Hyper Text Transfer Protocol

**HVAC** – Heating, Ventilating, and Air Conditioning
IEC – International Electrotechnical Commission
IKE – Internet Key Exchange, see RFC 2409.
IMAA – Identity Management and Architectural Authority
IPSEC – Internet Protocol Security
ISO – International Standards Organization
issuer – The name of the CA that signs the certificate; a certificate attribute field.

Issuing Certification Authority (Issuing CA) – In the context of a particular certificate, the Issuing CA is the CA that issued the certificate (see also Subject Certification Authority).

KGC – Key Generation Ceremony, the complex procedure for the generation of a CA’s private key.

LDAP – Lightweight Directory Access Protocol

Local Registration Authority (LRA) – Persons or systems that have been delegated authority to perform a portion of the registration process by the RA. For the Chevron PKI there will be two clearly defined LRA roles:

- Badging Officers, who issue smart cards to individuals
- Administrators, who will approve a device’s application for a certificate

MIP – Manager of Information Protection

Modification – (Certificate Modification) The issuance of a certificate to replace an existing certificate due to change in a Subscriber’s information other than his public key. For example, a change in an individual’s DN due to a change in name.

N of M – see Secret Shares

nCipher – A manufacturer of Hardware Security Modules.

NIST – National Institute of Standards and Technology (USA).

notAfter – The date and time after which a certificate expires; an attribute field.

Object – A program or data element, as in object oriented programming.

Object Identifier (OID) – A value (distinguishable from all other such values) that is associated with an object. (ITU-T X680) Referenced in many RFCs and used in the ASN.1 encoding of certificates.

OCS – Operator Card Set, authorized to participate in N of M activation of a CA’s private keys within an nCipher Security World.

PA – Policy Authority

Passphrase – An alphanumerical character string frequently used to control access to a smart card, similar to a PIN but offering greater protection for the same length.
PIN – A Personal Identification Number, or numeric password, used to protect the private keys on a smart card or ATM card.


PKCS #7 – Cryptographic Message Syntax Standard, used for distributing certificates.

PKCS #10 – A standard for certificate requests, published by RSA Security.


PKE – Public Key Encryption

PKI – Public Key Infrastructure

PMA – Policy Management Authority

Policy qualifier – Policy-dependent information that may accompany a CP identifier in an X.509 certificate. (RFC 3647)

Registration Authority (RA) – An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing Subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by Subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is sometimes used in other documents for the same concept.] (RFC 3647) Also see LRA.

Re-key – (Certificate Re-key) Ceasing use of a key pair and then generating a new key pair to replace it. The CA must certify the new public key. Re-key differs from renewal where a previously generated key pair remains in use and only a new certificate is requested.

Relying Party – A recipient of a certificate, who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms "certificate user" and "Relying Party" are used interchangeably. (RFC 3647)

Relying Party Agreement (RPA) – An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates. (RFC 3647)

Renewal – (Certificate Renewal) Issuance of a new certificate to the Subscriber without changing the Subscriber’s or any other participant’s public key or any other information in the certificate. (RFC 3647)

Repository – A trustworthy system for storing and retrieving certificates or other information relevant to certificates. (ABA PAG draft)

RSA – The acronym for the inventors of the RSA algorithm - Ron Rivest, Adi Shamir, and Leonard Adleman.

RSA Security – A publicly held corporation listed on the New York Stock Exchange.

Secret Shares – A set of smart cards, PINs, etc. used for N out of M control of a CA’s private key. These smart cards differ from the smart cards that are issued to individuals.
Shareholder  –  An individual authorized to hold a secret share.

Security World  –  An nCipher framework that maps security policies onto a flexible hardware-based security infrastructure. It provides for the total lifecycle management of security-critical encryption keys.

Set of Provisions (SoP)  –  A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in RFC 3647.

S/MIME  –  Secure Multipurpose Internet Mail Extensions

SID  –  Security Identifier, a logical security feature of the Microsoft Windows architecture.

SSL/TLS  –  Secure Sockets Layer/Transport Layer Security

Sponsor  –  An individual, authorized by his management to enroll devices.

SoP  –  Set of Provisions; a CP, CPS, or similar document that follows the RFC 3647 “Framework”.

subjectAltName  –  A certificate attribute field that typically contains the subject’s e-mail address.

Subscriber  –  A subject of a certificate, who is issued a certificate. (RFC 3647)

Subject Certification Authority (Subject CA)  –  In the context of a particular CA-certificate, the Subject CA is the CA whose public key is certified in the certificate (see also Issuing Certification Authority). (RFC 3647)

Truncation  –  The policy of not issuing certificates with expiration dates later than that of the expiration date of the signing CA.

Trust Anchor  –  Valid paths begin with certificates issued by a Trust Anchor. Typically the root in a PKI is the Trust Anchor.

Trusted Time Source  –  An extremely accurate clock, typically at NIST.

Trusted Role  –  Those individuals, who perform a role such as N out of M, that is critical to the operation or integrity of this PKI.

Trustworthy Systems  –  An operating system or certificate authority that complies with a designated design standard. This may refer to an internal Chevron standard or a published external standard such as the Common Criteria.

UPS  –  Uninterruptible Power Supply

URI  –  Universal Resource Identifier, a URL, FTP address, e-mail address, etc.

White Card  –  A temporary smart card issued solely for emergency network logon. The card does not have the employee’s picture nor can it be used for physical access control. Used at those locations, such as oil platforms, where a replacement SmartBadge cannot be issued or delivered in a timely manner.

X.500  –  A recommendation promulgated by ITU/T for specifying directory service and its protocols. It is a common standard for repositories.
X.509 — A public key certificate specification originally developed as part of the X.500 directory specification, often used in public key systems. Now effectively governed by IETF standards.

Yellow Card — A smart card issued to a temporary employee. The card does not have a picture of the employee or contractor. It is not used for physical access.

3DES — Triple DES; a symmetric encryption algorithm similar to DES, but much stronger.
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This PKI shall operate a Repository in which the SoP, CP and CPS documents, certificates issued to Subordinate CAs and End-Entities, and their respective CRLs and delta-CRLs are stored.

2.1 REPOSITORIES

Chevron operates the Repository for this PKI. The Repository is a logical construction, and it may be composed of several discrete servers providing their services through different Internet protocols such as HTTP or LDAP or proprietary protocols such as Active Directory.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The Root CA will publish Root CA Certificates, Intermediate CA Certificates and its CRLs to the Repository. The Root CA will include within any certificate it issues the URI of its CRL.

2.3 TIME OR FREQUENCY OF PUBLICATION

Root CA certificates and Intermediate CA certificates will be signed as scheduled. The Root CA will publish a CRL once every twelve (12) months. In exceptional situations, the Root may be required to sign and publish a CRL prior to the next scheduled time. As the Root CA is off-line and at a different physical location from the Repository, up to seven (7) days may elapse between the signing of such certificates or CRLs and their being available from the Repository.

2.4 ACCESS CONTROLS ON REPOSITORIES

The Root SoP, certificates and CRLs published to the Repository will be publicly accessible from the Repository. Chevron IT will establish access controls to prevent anyone other than an authorized individual, authorized system proxy or authorized system agent from deleting, altering or updating the contents of the Repository.
3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The certificates issued by the Root CA shall have the legal name of the organization, Chevron, in the Organization field of the Issuing Authority, and the authenticated commonName value of the Issuing Authority shall be “Chevron Root CA” in accordance with RFC 3280.

In the Root CA’s self-signed certificate, the Subject DNs shall have the legal name of the organization in the Organization field, and the authenticated commonName value of the subject shall be “Chevron Root CA” in accordance with RFC 3280.

The certificates issued to the Intermediate CAs by the Root CA shall have the legal name of the organization in the Organization field, and the authenticated commonName value of the subject shall be “Chevron Intranet Intermediate 10” for the Intranet and “Chevron Extranet Intermediate 50” for the Extranet in accordance with RFC 3280. Additional Intranet Intermediate CAs may be established; their numeric suffixes would range from 11 to 49. Also, additional Extranet Intermediate CAs may be established; their numeric suffixes would range from 51 to 99. The PMA must approve the addition of any Intermediate CA.

3.1.2 Need For Names To Be Meaningful

All certificates issued by the Root CA shall include an identifier that represents the Subscriber to which the certificate was issued. This identifier may not necessarily directly correspond to the subject’s legal name.

3.1.3 Anonymity or Pseudonymity of Subscribers

This policy does allow for the use of pseudonymous names in certificates. However, this policy does not permit anonymous Subscribers.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation - this section intentionally left blank.

3.1.5 Uniqueness of Names

All certificates issued by the Root CA shall include a DN that uniquely represents the self-signed Root CA or subordinate CA to which the certificate was issued.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation - this section intentionally left blank.
3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

Prior to the issuance of an Intermediate CA certificate, the Root CA requires proof of possession of a private key before creating and signing a certificate containing the associated public key. The Intermediate CAs will generate their own key pairs within a FIPS 140-1 Level 3 device. Each Intermediate CA will generate a PKCS #10 request. Such a request consists of three parts: certification request information, a signature algorithm identifier and the digital signature of the requestor on the certification request information. The Intermediate CA will forward the PKCS #10 request to the Root CA. The Root CA fulfills the request by authenticating the requestor entity and verifying the entity’s signature, and if the request is valid, constructing an X.509 certificate.

3.2.2 Authentication of Organization Identity

The PA endorses the application for an Intermediate CA certificate, and obtains the necessary signatures, which may include the signature of an officer of the corporation, and the appropriate corporate seal. The PA will then forward the application to the PMA for approval. Once the application is approved, the PMA will direct the IMAA to operate the CA, so as to issue the requested certificate.

3.2.3 Authentication of Individual Identity

Not applicable as the Root CA does not, as a matter of policy, issue certificates to End-Entities.

3.2.4 Non-Verified Subscriber Information

All Subscriber information contained within the certificate will be verified.

3.2.5 Validation of Authority

No stipulation - this section intentionally left blank.

3.2.6 Criteria for Interoperation

It is the intention of this PKI to participate in the Federal Bridge Certification Authority (BCA). Criteria for interoperation with this PKI will be determined by the PA and IMAA and approved by the PMA.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

The PKI maintains a schedule for renewing and re-keying each CA within its domain. Even though it is a scheduled event, the self-signed Root CA certificate may not be re-keyed or renewed until after IMAA approval has been obtained. The policies described in Section 3.2.1 and Section 3.2.2 must be followed when re-keying or renewing the Intermediate CAs.
3.3.2 Identification and Authentication for Re-key After Revocation

The self-signed Root CA certificate may not be re-keyed until after the PMA has determined that the cause for revocation has been remedied. The policies described in Section 3.2.1 and Section 3.2.2 must be followed when re-keying the Intermediate CAs after revocation.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

A request to revoke the certificates issued by the Root CA shall be sent to the PMA for reasons such as:

- Suspected or actual knowledge of the private key being compromised
- Corporate reorganization or merger
- Request of the Subscriber

If approved by the PMA, the IMAA will perform the revocation.
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

To issue certificates to Intermediate CAs, a PKI Administrator prepares the application for an Intermediate CA certificate, and forwards it to the PA for endorsement.

4.1.2 Enrollment Process and Responsibilities

The request must include sufficient documentation to demonstrate that the Subject DN is either a legal entity of Chevron, a registered service mark owned by Chevron, a registered trademark owned by Chevron or some other name that Chevron has rights to use. The PA reviews the application and if she approves it, endorses it and sends it to PKI Administrator, who will forward the request to Symantec and schedule the key signing.

4.2 CERTIFICATE APPLICATION PROCESSING

The PMA will process applications from the Intermediate CAs for certificates.

4.2.1 Performing Identification and Authentication Functions

The request must include sufficient documentation to demonstrate that the Subject DN is either a pseudonym for a device operated for Chevron, a legal entity of Chevron, a registered service mark owned by Chevron, or a registered trademark owned by Chevron.

4.2.2 Approval or Rejection of Certificate Applications

The PMA must review and approve the request before authorizing certificate issuance. The decision to approve or reject an Intermediate CA application shall be solely at the discretion of the PMA. The issuance of a certificate to a subordinate CA must be formally approved by the PMA.

4.2.3 Time to Process Certificate Applications

Such action should be taken within one (1) month of the application and the requesting PA notified of the action.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

Once the application has been approved by the PMA, an administrator of the Intermediate CA will initiate a cross-certificate request containing its CA verification key. The Intermediate CA’s key pair will be generated as described in Section 6.1 of the respective Intermediate CA’s SoP. The cross-certification request, which will be recorded in PKCS #10 format, will forward it to the Root CA’s IMAA. Due to the need to schedule the
operation of the off-line Root CA, up to several weeks may elapse between approval and issuance. The Root IMAA will operate the Root CA so as to issue the authorized certificates.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Using that PKCS #10 request, the Root CA will generate a signed certificate and package it in a PKCS #7 format that will be returned to one of the Root CA’s Shareholders.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

The Intermediate CA’s PKI Administrator will open the PKCS #7 message and install the certificate on the respective CA. Successful installation constitutes acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

Self-signed certificates and Intermediate CA certificates are published in the Repository within seven (7) days of issuance.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Chevron will publish them to the repository, Active Directory, within seven (7) days of issuance. When the certificates in the workstation’s cache expire, the workstation will obtain the certificate from the repository. Subsequently, Chevron will distribute the self-signed certificates and Intermediate CA certificates to the next generation of its desktop image.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The Intermediate CAs are the only Subscribers of the Root CA. The human administrator(s) for such Subscribers are obligated to:

- Protect private keys by storing them on a FIPS 140-1 Level 3 cryptographic device
- Use the private keys for signing certificates issued to subordinate CAs, CRLs, delta CRLs, ARLs, delta ARLs, or for signing cross-certificates
- Maintain cryptographic material in a secure manner according to established Chevron procedures for handling such material

4.5.2 Relying Party Public Key and Certificate Usage

The self-signed Root certificate and Intermediate CA certificates are to be used for performing certificate path validation as described in RFC 3280.
4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

This PKI will not issue certificates with expiration dates later than that of the expiration date of the signing CA. In other words, if the signer’s key expires in one year, an End-Entity’s certificate cannot expire in two years even though policy would otherwise allow such certificates. The life of the End-Entity certificate would be truncated from two years to one.

Within this PKI, to preclude Truncation, a signer’s certificate up to and including the Root may be renewed.

Within its current lifetime, the Root CA’s self-signed certificate may be renewed provided its 2048-bit key length is still considered to be cryptographically secure by the PMA. The current renewal schedule is given in Table 1 below.

Within its current lifetime, an Intermediate CA’s certificate may be renewed provided its 2048-bit key length is still considered to be cryptographically secure by the IMAA. At this time Chevron plans to re-key the intermediate CAs rather than renew their certificates. The current re-keying schedule is given in the table below.

Table 1 - Root and Intermediate Renewal and Re-Key Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Root</th>
<th>Intermediate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2004</td>
<td></td>
<td>Renew until 2009</td>
</tr>
<tr>
<td>1/2006</td>
<td>Re-key until 2026</td>
<td>Re-key until 2016</td>
</tr>
<tr>
<td>1/2012 (est.)</td>
<td></td>
<td>Re-key until 2022</td>
</tr>
</tbody>
</table>

4.6.2 Who May Request Renewal

The respective IMAA may request renewal of the Root CA’s self-signed certificate or an Intermediate CA’s certificate.

4.6.3 Processing Certificate Renewal Requests

The request must include sufficient documentation to demonstrate that the Subject DN is still either pseudonym for a device operated for Chevron a legal entity of Chevron, still a registered service mark owned by Chevron, or still a registered trademark owned by Chevron. A Root CA Shareholder will present the request and PKCS #10 message to Symantec.

4.6.4 Notification of New Certificate Issuance to Subscriber

The Root CA will generate a signed certificate and package it in a PKCS #7 format that will be returned to the Root CA Shareholder.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
The Intermediate CA’s PKI Administrator will open the PKCS #7 message and install the certificate on the respective CA. Successful installation constitutes acceptance of the renewal certificate.

4.6.6 Publication of the Renewal Certificate by the CA

Self-signed Root CA renewal certificates and Intermediate CA renewal certificates are published in the Repository within seven (7) days.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Chevron will add self-signed renewal certificates and Intermediate CA renewal certificates to its repository, portions of which are available via HTTP and LDAP services.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-Key

Within this PKI, to preclude Truncation as discussed in Section 4.6.1, the signer’s certificate up to and including the Root may be re-keyed.

Within its current lifetime, the Root CA’s self-signed certificate may be re-keyed with a 2048-bit key length, provided such a length is still considered to be cryptographically secure by the PMA. However, re-keying is not currently scheduled.

Within its current lifetime, an Intermediate CA’s certificate may be re-keyed with a 2048-bit key length, provided such a length is still considered to be cryptographically secure by the PMA. The current certificate re-key schedule is given in Section 4.6.1.

4.7.2 Who May Request Certification of a New Public Key

The respective IMAA may request re-keying of the Root CA’s self-signed certificate or the re-keying of an Intermediate CA’s certificate from the PMA.

4.7.3 Processing Certificate Re-Keying Requests

The request must include sufficient documentation to demonstrate that the Subject DN is still a pseudonym for a device operated for Chevron, still either a legal entity of Chevron, still a registered service mark owned by Chevron, or still a registered trademark owned by Chevron. The IMAA must review and approve the request before authorizing certificate issuance. The decision to approve or reject an Intermediate CA application shall be solely at the discretion of the IMAA. Such action should be taken within one (1) week of the application and the IMAA must notify the Root Shareholders.

4.7.4 Notification of New Certificate Issuance to Subscriber

The Root CA will generate a signed certificate and package it in a PKCS #7 format that will be returned to the Root Shareholder.
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The Intermediate CA’s PKI Administrator will open the PKCS #7 message and install the re-keyed certificate on the respective CA. Successful installation constitutes acceptance of the re-keyed certificate.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Self-signed Root CA re-keyed certificates and Intermediate CA re-keyed certificates are published in the Repository prior to its signing any subordinate certificate.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Chevron will add self-signed re-keyed certificates and Intermediate CA re-keyed certificates to its repository, portions of which are available via HTTP and LDAP services.

4.8 CERTIFICATE MODIFICATION

Certificate modification is not permitted within this PKI.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

The IMAA of any CA within the Chevron PKI may request the revocation of a CA’s certificate(s). Superior CAs may unilaterally revoke any certificate(s) issued to a subordinate CA. Revocation will be approved and processed in accordance with its respective policy. Certificate suspension is not permitted.

4.9.1 Circumstances for Revocation

4.9.1.1 Permissive Revocation

An Intermediate CA may request revocation at any time and for any reason.

4.9.1.2 Required Revocation

The Intermediate CA is required to request a revocation of certificates issued to itself if:

- The Intermediate CA discovers or has reason to believe that there has been a compromise of its private signing key
- The information on the certificate is no longer accurate
- The Intermediate CA no longer qualifies as an Intermediate CA

The Root CA shall revoke the certificate upon:

- The request of an Intermediate CA
- Knowing that the information on the certificate is no longer accurate
• Discovery or suspicion that there has been a compromise of the Intermediate CA’s private signing key

• Discovery that the certificate was issued in a manner not materially in accordance with this SoP, the certificate was issued to an entity other than the one named as the subject of the certificate, or the certificate was issued without the authorization of the entity named as the subject of such certificate

The Root CA shall revoke its own signing certificate if:

• The information in the certificate is no longer accurate

• It discovers that there has been a compromise of the Root CA’s private signing key

• The Root CA is terminated as specified in Section 5.8 of this SoP

4.9.2 Who Can Request Revocation

Any Relying Party possessing evidence of compromise, the Root CA, any Intermediate CA, or any Issuing CA may request revocation.

Revocation of certificates issued to CAs will be approved by the IMAA. Any request for revocation that is declined must be denied in writing.

Before revoking the certificate issued to a CA, all certificates previously issued by that CA must also be revoked. As a prerequisite, all certificates issued by an Issuing CA, whose certificate was signed by an Intermediate CA, must first be revoked.

4.9.3 Procedure for Revocation Request

A revocation request may be generated electronically. The request shall be approved by the appropriate CA’s IMAA.

4.9.4 Revocation Request Grace Period

The Intermediate CA’s IMAA must request revocation within twenty-four (24) hours if the Intermediate CA’s IMAA discovers or has reason to believe that there has been a compromise of its private signing key, the information on the certificate is no longer accurate, or the Intermediate CA no longer qualifies as an Intermediate CA, for example, the end of a joint venture that led to the creation of such an Intermediate CA.

4.9.5 Time Within Which CA Must Process the Revocation Request

The Root CA shall process revocation requests within two (2) business days from time of receipt. Two (2) business days are required to schedule access to the off-site facility, to bring the N of M Shareholders together, and to bring the Root CA online.

4.9.6 Revocation Checking Requirement for Relying Parties

Certificates may be stored locally in the Relying Party’s public key application, but the Relying Party must check the status of the certificate before use.
The Intranet Intermediate certificate issued by the Root CA includes the names of the primary (LDAP) cRLDistributionPoints and secondary (HTTP) extension fields. The Extranet Intermediate certificate issued by the Root CA includes the name of the primary DistributionPoint (HTTP) extension field. The Relying Party is obligated to examine the Root’s base CRL, along with any other CRL/ARLs required in certificate chain processing prior to trusting the certificate in accordance with RFC 3280. Delta CRLs are not issued by the Root CA.

In addition, when a Relying Party downloads a CRL/ARL from a public Repository, the Relying Party shall verify it by validating its digital signature.

4.9.7 **CRL Issuance Frequency**

The Root CA shall issue a CRL every twelve (12) months or within one (1) hour of the revocation of an Intermediate CA certificate. The lifetime of the CRL, the interval between the thisUpdate and nextUpdate attribute fields within the CRL, may be up to sixteen (16) months.

4.9.8 **Maximum Latency for CRLs**

The issued CRL must be published within four (4) days of its issuance.

4.9.9 **On-Line Revocation/Status Checking Availability**

This PKI does not support:

- Online Certificate Status Protocol (OCSP)
- XML Key Management Specification (XKMS)
- Simple Certificate Validation Protocol (SCVP)

4.9.10 **On-Line Revocation Checking Requirements**

No stipulation - this section intentionally left blank.

4.9.11 **Other Forms of Revocation Advertisements Available**

No stipulation - this section intentionally left blank.

4.9.12 **Special Requirements re Key Compromise**

Chevron shall use commercially reasonable efforts to notify Relying Parties if it discovers, or has reason to believe, that there has been a compromise of the private key of one of its own CAs. All Relying Parties shall be notified concerning such compromise through the use of a CRL/ARL. In addition, external parties, who have signed Relying Party Agreements, will be notified via email, regular mail, facsimile, or telephone using commercially reasonable efforts.

4.9.13 **Circumstances for Suspension**
4.9.14 **Who Can Request Suspension**

No stipulation - this section intentionally left blank.

4.9.15 **Procedure for Suspension Request**

No stipulation - this section intentionally left blank.

4.9.16 **Limits on Suspension Period**

No stipulation - this section intentionally left blank.

4.10 **CERTIFICATE STATUS SERVICES**

4.10.1 **Operational Characteristics**

The Root CA will issue version 2 CRLs as specified in RFC 3280.

4.10.2 **Service Availability**

The Repository, including the latest CRL, will be available for at least 99.9 percent of the time.

4.10.3 **Operational Features**

No stipulation - this section intentionally left blank.

4.11 **END OF SUBSCRIPTION**

No stipulation - this section intentionally left blank.

4.12 **KEY ESCROW AND RECOVERY**

4.12.1 **Key Escrow and Recovery Policy and Practices**

Chevron does not escrow its Root CA keys.

4.12.2 **Session Key Encapsulation and Recovery Policy and Practices**

No stipulation - this section intentionally left blank.
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

Chevron Root CA operations are conducted within Symantec’s primary facilities in Mountain View, California. These facilities provide the Chevron Root CA with a physically protected environment that deters, prevents and detects unauthorized use of, access to or disclosure of sensitive information and systems. These facilities have seven (7) physical security tiers as described in Section 5.1.2.

Symantec also maintains disaster recovery facilities in Herndon, Virginia for the Chevron Root CA operations. Their disaster recovery facilities are protected by multiple tiers of physical security comparable to those of their primary facility.

5.1.2 Physical Access

Symantec provides seven (7) concentric tiers of physical security to protect the Chevron Root CA, with access to the lower tier required before gaining access to the higher tier. While the Root KGC will occur within Tier 4, the key material will be stored at Tier 7.

Table 2 - Physical Security Tiers

<table>
<thead>
<tr>
<th>Tier</th>
<th>Description</th>
<th>Access Control Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Security</td>
<td>Physical Security Tier 1 refers to the outermost physical security barrier</td>
<td>Access to this tier requires the use of a proximity card employee badge. Physical access</td>
</tr>
<tr>
<td>Tier 1</td>
<td>for the facility.</td>
<td>to Tier 1 is automatically logged and video recorded.</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Tier 2 includes common areas, including restrooms and common hallways.</td>
<td>Tier 2 enforces individual access control for all persons entering the common areas of the</td>
</tr>
<tr>
<td>Tier 2</td>
<td></td>
<td>CA facility through the use of a proximity card employee badge. Physical access to Tier 2 is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>automatically logged.</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Tier 3 is the first tier at which sensitive CA operational activity takes</td>
<td>Tier 3 enforces individual access control through the use of two-factor authentication,</td>
</tr>
<tr>
<td>Tier 3</td>
<td>place. Sensitive CA operational activity is any activity related to the</td>
<td>including biometrics. Unescorted personnel, including untrusted employees or visitors, are</td>
</tr>
<tr>
<td></td>
<td>lifecycle of the certification process, such as authentication, verification</td>
<td>not allowed into a Tier 3 secured area. Physical access to Tier 3 is automatically logged.</td>
</tr>
<tr>
<td>Tier</td>
<td>Description</td>
<td>Access Control Mechanisms</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Tier 4 is the tier at which especially sensitive CA operations occur, the ceremony room.</td>
<td>The Tier 4 ceremony room enforces dual control, each through the use of two-factor authentication including biometrics. Individuals approved for unescorted Tier 4 access must satisfy the Trusted Employee Policy. Physical access to Tier 4 is automatically logged.</td>
</tr>
<tr>
<td>Tier 4</td>
<td>Key Management Tiers 5 through 7 serve to protect off-line storage of Cryptographic Storage Units (CSUs) and keying material.</td>
<td>Off-line CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with Symantec’s segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes. Progressively restrictive physical access privileges control access to each tier.</td>
</tr>
</tbody>
</table>

5.1.3 **Power and Air Conditioning**

Symantec’s secure facilities are equipped with primary and backup

- Power systems to ensure continuous, uninterrupted access to electric power
- Heating/ventilation/air conditioning systems to control temperature and relative humidity

5.1.4 **Water Exposures**

Symantec has taken reasonable precautions to prevent floods or other damaging water exposure to the Root CA hardware.

5.1.5 **Fire Prevention and Protection**

Symantec has taken reasonable precautions to prevent, detect and extinguish fires. Additional measures have been taken to prevent damaging exposure to flame or smoke. Symantec’s fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 **Media Storage**

All media containing production software and data, audit, archive or backup information is stored within Symantec facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and to protect such media from accidental damage due to environmental hazards (e.g., water, fire and electromagnetism).
5.1.7 **Waste Disposal**

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed, or “zeroized,” in accordance with the manufacturer’s guidance prior to disposal. Other non-sensitive waste is disposed of in accordance with Symantec’s normal waste disposal practices.

5.1.8 **Off-Site Backup**

Symantec’s management personnel perform backups of critical system data, audit log data and other sensitive information. Off-site backup media are stored in a physically secure manner using a bonded third party storage facility and Symantec’s East Coast disaster recovery facility.

5.2 **PROCEDURAL CONTROLS**

5.2.1 **Trusted Roles**

Employees of both Chevron and Symantec are assigned to the Trusted Roles listed below, and are authorized to perform the specified administrative and technical functions.
Table 3 - Trusted Roles

<table>
<thead>
<tr>
<th>Trusted Role</th>
<th>Symantec/Chevron</th>
<th>Authorized To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrysalis Green PED Key Holders for the primary token.</td>
<td>From both entities, Symantec must have less than M keys.</td>
<td>Participate in N of M activation of primary Chrysalis token.</td>
</tr>
<tr>
<td>Chrysalis Green PED Key Holders for the backup token.</td>
<td>From both entities, Symantec must have less than M keys.</td>
<td>Participate in N of M activation of backup Chrysalis token.</td>
</tr>
</tbody>
</table>

Only the following may be assigned to a Trusted Role:

- Symantec’s customer service personnel
- Chevron’s and Symantec’s cryptographic operations personnel
- Chevron’s and Symantec’s security personnel
- Chevron’s and Symantec’s system administration personnel
- Symantec’s designated engineering personnel
- Symantec’s executives that are designated to manage infrastructural trustworthiness

Symantec considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Employees of Symantec seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements established by Symantec. Employees of Chevron will be appointed by the PMA.

5.2.2 Number of Persons Required Per Task

Chevron adheres to Symantec’s established policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware [the Chrysalis token, also called a Cryptographic Signing Unit (CSU) by Symantec] and associated key material require that several individuals be present concurrently.

These internal control procedures are designed to ensure:

- Access to Root CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction
- That two (2) specific individuals are always present when a token containing private keys is removed from the safe deposit box in which it is stored, and that they remain with the token until it is returned to the safe deposit box
• Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device

• Persons with physical access to modules do not hold the Chrysalis PED keys, and vice versa

• That three (3) of the five (5) Chrysalis Green PED Key holders (N of M control) be present to activate the primary and/or backup tokens

• At least one (1) of those Green PED Key holders present must be from Chevron, which limits Symantec to no more than two (2) keys for each token. Chevron will retain three (3) keys for each token

• As the Green PED keys are not interchangeable between tokens, a Green PED Key holder may hold a Green PED Key from both the primary token and its clone

5.2.3 Identification and Authentication for Each Role

Chevron and Symantec employees assigned to a Trusted Role must be designated as such by their respective organization. For Chevron, the PMA will provide such designation. Symantec will follow its established procedures.

Chevron will provide Symantec with sufficient information, so that Symantec can confirm that the individual, who appears at Symantec’s premises, is indeed the person he claims to be; and, that he has been appropriately authorized. Chevron will have confirmed the identity further by following background-checking procedures described in Section 5.3.1.

Symantec assures that its personnel have achieved Trusted Status, and that the Chevron IMAA has granted written approval for such persons to serve in a Chevron Trusted Role.

Before Chevron’s Trusted Persons are issued access devices and granted access to the required facilities, or issued electronic credentials to access and perform specific functions on Chevron’s Root CA, they will have to present a well-recognized form of identification (e.g., passport or driver’s license) upon their arrival at Symantec’s premises.

Immediately before Symantec’s Trusted Persons perform a Chevron Trusted Role, they will have to present suitable identification to those Chevron Trusted Persons, who are present.

5.2.4 Roles Requiring Separation of Duties

For the Root CA, no individual may serve in more than one Trusted Role; for example, persons authorized for HSM N out of M control, the Chrysalis Green PED keys, must not also control physical access to safe a HSM is stored.
5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

Individuals selected for a Trusted Role have demonstrated their loyalty, trustworthiness and integrity, and must present proof of the requisite background, qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.2 Background Check Procedures

Prior to assigning an employee to a Trusted Role, both Chevron and Symantec have completed background checks on their respective personnel. To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, Chevron will utilize a substitute investigative technique permitted by law that provides substantially similar information including, but not limited to, obtaining a background check performed by the applicable governmental agency.

5.3.3 Training Requirements

Individuals assigned to Trusted Roles shall be given the training to perform their job responsibilities competently and satisfactorily.

5.3.4 Retraining Frequency and Requirements

Both Symantec and Chevron provide refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. Security awareness training is provided on an ongoing basis.

5.3.5 Job Rotation Frequency and Sequence

No stipulation - this section intentionally left blank.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of Chevron policies and procedures. Disciplinary actions may include measures up to and including termination, and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

No stipulation - this section intentionally left blank.

5.3.8 Documentation Supplied to Personnel

Individuals assigned to Permanent Trusted Roles must annually acknowledge, in writing that they understand the responsibilities of their trusted role as documented in this SoP and its entry/exit requirements.
5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded
All significant events shall be recorded in the Root CA audit logs including, but not limited to:

- System start-up and shutdown
- CA application start-up and shutdown
- Attempts to create, remove, set passwords or change the system privileges of the privileged users (Trusted Roles)
- Changes to CA details and/or keys
- Changes to certificate creation policies (e.g., validity period)
- Login and log-off attempts, both successes and failures
- Unauthorized attempts to access system files
- Generation of the CA’s keys
- Failed read and write operations on the certificate database and Repository
- Certificate lifecycle management-related events (e.g., certificate applications, issuance, revocation, and renewal)
- Cryptographic module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement)
- Removing the cryptographic module from its assigned secure storage location
- Replacing the cryptographic module in its assigned secure storage location
- Activation and deactivation of the cryptographic module
- For disaster recovery or any other purpose, cloning the private keys contained within the cryptographic module

5.4.2 Frequency of Processing Log
Audit log processing shall occur on an ad hoc basis and consist of a review of the audit logs and documenting the reason for all significant events in an audit log summary. Audit log reviews shall include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews shall be documented.

5.4.3 Retention Period for Audit Log
Root CA audit logs shall be retained for the life of the PKI and may be archived.

5.4.4 Protection of Audit Log
Audit logs shall be protected by a combination of physical and procedural security controls, which are controlled by Symantec.

5.4.5 **Audit Log Backup Procedures**

Audit log files shall be backed up, and the backup media shall be stored locally in a secure location. Symantec shall send a consolidated copy of the audit log files to a secure off-site storage facility in accordance with Symantec’s established procedures.

5.4.6 **Audit Collection System (Internal vs. External)**

Automated data is collected internally by the Root CA server’s operating system and the Root CA application log. Symantec personnel also record manually generated data.

5.4.7 **Notification to Event-Causing Subject**

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device or application that caused the event.

5.4.8 **Vulnerability Assessments**

Events in the audit process are logged, in part, to monitor system vulnerabilities. Security vulnerability assessments shall be performed by Symantec, reviewed and revised following an examination of these monitored events. These assessments may, at Symantec’s option, be sent to Chevron where they will be an input into the Chevron PKI annual compliance audit.

5.5 **RECORDS ARCHIVAL**

5.5.1 **Types of Records Archived**

The Root CA shall archive:

- The audit logs described in Section 5.4.1
- The certificates it issues
- The published CRLs
- Certificate applications, certification revocation requests and correspondence
- This SoP and any modifications or updates to it
- Any data or applications sufficient to verify and read the archive contents
- Communications to or from the PMA, IMAA, PA, and assessors or auditors

5.5.2 **Retention Period for Archive**

For the Root CA, the archive of the key and certificate information must be retained for at least ten (10) years and six (6) months, the FBCA Medium Assurance Level, after the
certificate expires or is revoked. Archives of audit log files must be retained for the life of the Root CA and protected as described below.

5.5.3 Protection of Archive

The archive media shall be protected either by physical security, or a combination of physical security and cryptographic protection. Additionally, the archive media shall be provided adequate protection from environmental threats such as temperature, humidity and magnetism.

5.5.4 Archive Backup Procedures

Root CA certificates, CRLs and keys shall be backed up and stored locally in a secure location. Whenever the Root CA’s private and public keys are generated, they shall be immediately cloned from the original cryptographic module to another FIPS 140-1 Level 3 device. The clone will be promptly sent to a secure off-site storage facility. Whenever a new CRL is issued, generally once a year, a copy will be sent to a secure off-site storage facility.

Discrepancy and compromise reports, Cross-Certification Agreements and correspondence shall be copied upon receipt and sent to a secure off-site storage facility. Original copies shall be stored locally in a secure location.

5.5.5 Requirements for Time-Stamping of Records

Certificates and CRLs contain time and date stamps supplied by the Root CA.

5.5.6 Archive Collection System (Internal or External)

The events described in Section 5.4.1 are archived by Symantec, whose archived collection system is external to Chevron. All other archived collection systems for correspondence are primarily paper-based, and are internal to Chevron.

System-generated, archived records shall be transferred to separate physical media external to the Root CA host system.

5.5.7 Procedures to Obtain and Verify Archive Information

Once per year, during WebTrust for CA audit of Symantec’s operations, a sample of the archived records is retrieved and verified to ensure that no damage or loss of data has occurred. If any has occurred, the backup archive is retrieved and becomes the new master archive, and a new backup is produced.

5.6 KEY CHANGEOVER

Root CA shall perform the key changeover according to the schedule provided in Section 4.6.1 and procedures described elsewhere in this SoP. This will allow for a “window,” or “overlap” period during which both old keys and new keys are valid.
5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

Any charge or suspicion of compromise must be brought to the attention of the IMAA. While written correspondence is requested, any commercially acceptable means of communication may be used for the initial contact provided written confirmation is submitted in a timely manner. The chairperson of the IMAA will log any reported claim of compromise, and order a prompt investigation. All such investigations will be completely documented, and the documentation will be retained for thirty (30) years. The resolution of the claim will be logged, and the log will be retained for thirty (30) years. If sufficient information has been obtained to substantiate the validity of such a claim, the PA and IMAA shall assess the severity of the compromise in order to determine operational viability. The PMA, upon advisement from the PA and IMAA, shall determine the corrective measures deemed to be appropriate.

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

As the Root CA is normally off-line and revocation of the certificates it issues unlikely, recovery of the Root CA is unlikely to ever be time-critical.

In the event that computing resources, software and/or data are corrupted, Root CA operations will be suspended. An investigation will be conducted to ascertain the cause and extent of the corruption, and the Root CA IMAA will also conduct an assessment of the integrity of the PKI.

The Root CA and RA will be restored to the last good backup before the corruption occurred. Subscribers will be notified of the corruption, and all certificates issued between the time of corruption and CA service re-establishment will be re-issued.

5.7.3 Entity Private Key Compromise Procedure

In the event of compromise of the Root CA’s private key, all active certificates issued by the Root CA, Intermediate CAs and Issuing CAs must be revoked. The process will start with the revocation of the End-Entity certificates by the Issuing CAs. The Intermediate CAs will then revoke the CA certificates of the Issuing CAs, and then proceed up the chain of trust to the Intermediate CA authorities, and will then terminate with revocation of the Root CA’s self-signed certificate.

5.7.4 Business Continuity Capabilities After a Disaster

Symantec maintains a Root CA Disaster Recovery Plan (DRP), which in coordination with Chevron is capable of re-establishing basic CA services.

5.8 CA OR RA TERMINATION

A request for termination of the Root CA must be submitted in writing and delivered to the PMA. If the PMA determines that termination of the Root CA is necessary, the Root CA IMAA shall commence such termination.
6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

The Root CA key pair generation is performed by multiple pre-selected, trained and trusted Symantec individuals and multiple pre-selected, trained and trusted Chevron employees using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. The cryptographic module used for key generation of the Root CA key pair meets the requirements of FIPS 140-1 Level 3.

The Root CA key pair is generated during pre-planned KGCs in accordance with the requirements of the Symantec Key Ceremony Reference Guide, the Symantec CA Key Management Tool User’s Guide, the Symantec Security and Audit Requirements Guide and the requirements of Chevron. Employees of Chevron and Symantec participate in the KGC. The activities performed in the KGC are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for the greater of either (i) the length of time deemed appropriate by the Chevron PMA, or (ii) the length of time deemed appropriate by Symantec.

6.1.2 Private Key Delivery to Subscriber

The Root CA will not sign certificates for End-Entities. The Root and Intermediate CAs’ private keys will be generated and remain within their respective FIPS 140-1 Level 3 certified cryptographic modules.

6.1.3 Public Key Delivery to Certificate Issuer

Each Intermediate CA submits its public key to the Root CA electronically through the use of a PKCS #10 Certificate Signing Request (CSR).

6.1.4 CA Public Key Delivery to Relying Parties

Chevron makes the Root CA certificate available to Subscribers and Relying Parties by publishing it at http://pki.chevron.com/aia/Chevron%20Root%20CA(x).crt. The x indicates the generation of the CA certificate; it is incremented by 1 every time the Root certificate is re-keyed or renewed.

The web servers supporting this Certificate Distribution Point (CDP) consist of a two-node fail-over cluster spanning the San Ramon and Houston sites, and are designed to provide high availability. Additional nodes may be added to improve reliability and performance. The certificates issued to the Intermediate CAs will contain AIA pointers back to this distribution point.

6.1.5 Key Sizes

The Root CA key pair is 2048-bit RSA.
6.1.6 **Public Key Parameters Generation and Quality Checking**

The required Key Parameters will be generated in accordance with FIPS 186-2 (ANSI X9.31) or a PMA-approved equivalent standard.

The quality of the generated Key Parameters shall be verified in accordance with FIPS 186-2 or a PMA-approved equivalent standard.

6.1.7 **Key Usage Purposes**


6.2 **PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS**

Chevron has contracted with Symantec to implement a combination of physical, logical and procedural controls to ensure the security of the Root CA private key. Logical and procedural controls are described in Section 5.2. Physical access controls are described in Section 5.1.2 of this SoP.

6.2.1 **Cryptographic Module Standards and Controls**

The Root CA key pair generation and CA private key storage shall use a hardware cryptographic module that is certified at FIPS 140-1 Level 3.

6.2.2 **Private Key (N out of M) Multi-Person Control**

Chevron has implemented technical and procedural mechanisms that require the participation of multiple Trusted Individuals to perform sensitive CA cryptographic operations. Chevron uses “Secret Sharing” to split the activation data needed to make use of a CA private key into separate parts called “Secret Shares,” which are held separately by trained and trusted individuals called “Shareholders.” A threshold number of Secret Shares (N) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (M) is required to activate a CA’s private key stored on the module. This is also known as N of M control. See Sections 5.2.1 through 5.2.4 for additional details.

6.2.3 **Private Key Escrow**

Chevron does not escrow its Root CA keys.
6.2.4 **Private Key Backup**

Chevron and Symantec will jointly back up, through cloning, the Root CA’s private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. The cloning process requires multi-person controls, both to activate the primary token and to create the clone. Cryptographic modules used for CA private key storage meet the requirements of FIPS 140-1 Level 3. CA private keys are cloned to backup hardware cryptographic modules in accordance with Section 6.2.6. The activation of the clone requires the same multi-person controls as the primary token.

6.2.5 **Private Key Archival**

When the Root CA key pair reaches the end of its validity period, it will be archived for a period of at least ten (10) years and six (6) months. Archived CA key pairs will be securely stored using hardware security modules that meet the requirements of Section 6.2.1 of this SoP. Procedural controls prevent archived CA key pairs from being returned to production use. Upon the end of the archive period, archived CA private keys shall be securely destroyed in accordance with Section 6.2.10.

6.2.6 **Private Key Transfer Into or From a Cryptographic Module**

Chevron Root CA key pair shall be generated on the hardware cryptographic modules in which the keys will be used. In addition, Chevron and Symantec jointly make copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form. The private key never leaves the cryptographic module in unencrypted form.

6.2.7 **Private Key Storage on Cryptographic Module**

The private key is stored in encrypted form and once activated, as it is also stored as plaintext in volatile memory within the cryptographic module.

6.2.8 **Method of Activating Private Key**

First, the HSM must be removed from secure storage at Symantec’s facility. Then the HSM must be connected to the CA server and both powered on. Once the CA application is started, an administrative command is issued to start the activation of the private key. Activation requires the threshold number of Shareholders supplying their activation data (tokens and/or passwords) in accordance with Section 6.2.2. The off-line Root CA private key is normally activated only for a short time (e.g., for the certification of an Intermediate CA or the signing of a CRL/ARL), after which it is promptly deactivated, and the cryptographic module is returned to secure storage within the Symantec facility.

6.2.9 **Method of Deactivating Private Key**

Chevron’s Root CA private keys are normally deactivated through an administrative interface before removal from the token reader. However, the token automatically deactivates itself upon removal from the token reader or power down.
6.2.10 Method of Destroying Private Key

At the conclusion of the Root CA’s operational lifetime, one (1) original and one (1) clone of the CA private key will be archived in accordance with Section 6.2.5. Any remaining clones of the CA private key will be securely destroyed. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. CA key destruction activities require the participation of multiple Trusted Individuals.

When required, Chevron will destroy the Root CA private keys in a manner that reasonably ensures that there are no residual remains of the keys that could lead to the reconstruction of the keys. Chevron will utilize the zeroization function of its hardware cryptographic module and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged.

6.2.11 Cryptographic Module Rating

Due to an error in RFC 3647 this section duplicates Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The Root CA public key is backed up and archived as part of both Chevron’s and Symantec’s standard backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum operational period of the Root CA key pair is twenty (20) years. The certificate will be renewed once after the initial ten (10) year period.

The maximum operational period of an Intermediate CA key pair is ten (10) years. The certificate was renewed during January 2004.

6.4 ACTIVATION DATA

Activation data (Secret Shares) used to protect tokens containing the Root CA’s private key is generated in accordance with the requirements of Section 6.2.2 and the Symantec Key Ceremony Reference Guide. The creation and distribution of Secret Shares are logged.

6.4.1 Activation Data Generation and Installation

During the Root CA KGC, the appropriate Trusted Individuals shall receive their Secret Shares.

6.4.2 Activation Data Protection

Chevron and Symantec Shareholders are required to safeguard their Secret Shares, and sign an agreement acknowledging their Shareholder responsibilities. Both the primary and backup sets of the Chrysalis Green PED Keys, which are used to activate the Root CA private key, will be stored in three (3) safes. Within the primary set, the Green PED Keys will be distributed as follows: Symantec - Mountain View, California, two (2);
Chevron - San Ramon, California, three (3); by their respective Shareholders. Within the clone set, the Green PED Keys will be distributed as follows: Symantec – Herndon, Virginia, two (2); Chevron - Houston, Texas, three (3); by their respective Shareholders. Each set of Green PED Keys is bound to a specific token, and cannot be used to operate any other token.

6.4.3 Other Aspects of Activation Data

No stipulation - this section intentionally left blank.

6.5 COMPUTER SECURITY CONTROLS

The Root CA uses Symantec Trustworthy Systems that meet the requirements of the Symantec Security and Audit Requirements Guide.

6.5.1 Specific Computer Security Technical Requirements

Symantec ensures that the systems maintaining CA software and data files are Trustworthy Systems that are secure from unauthorized access. In addition, Symantec limits access to production servers to only those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

Direct access to Symantec databases supporting the Symantec Repository is limited to Trusted Persons in Symantec’s operations group that have a valid business reason for such access.

6.5.2 Computer Security Rating

No stipulation - this section intentionally left blank.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

Applications are developed and implemented by Symantec in accordance with Symantec systems development and change management standards. Such software is developed in accordance with Symantec system development standards.

6.6.2 Security Management Controls

Symantec has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. Symantec creates a hash of all software packages and Symantec software updates. This hash is used to verify manually the integrity of such software. Upon installation and periodically thereafter, Symantec validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation - this section intentionally left blank.
6.7 NETWORK SECURITY CONTROLS

The Root CA will never be attached to any network, so such controls are not required.

6.8 TIME-STAMPING

Although a Trusted Time Source is not required, the CA administrators are required to see that the Root CA server’s clock is set to within five (5) minutes of the actual time whenever it is brought online.
7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

The following fields of the X.509 v3 certificate format are used in certificates issued by the Chevron Root CA.

Table 4 - Certificate Format and Extensions for the self-signed Root CA certificate

<table>
<thead>
<tr>
<th>Base Certificate</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>MD5 hash of public key</td>
</tr>
<tr>
<td>Issuer DN</td>
<td>cn=Chevron Root CA, o=Chevron, c=US</td>
</tr>
<tr>
<td>Subject DN</td>
<td>cn=Chevron Root CA, o=Chevron, c=US</td>
</tr>
<tr>
<td>NotBefore</td>
<td>020109190000Z (7:00 PM January 9, 2002 GMT)</td>
</tr>
<tr>
<td>NotAfter</td>
<td>220109185959Z (Twenty years later)</td>
</tr>
<tr>
<td>Public Key Algorithm</td>
<td>sha1-WithRSAEncryption (1 2 840 113549 1 1 5)</td>
</tr>
<tr>
<td>Parameters</td>
<td>NULL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard Extensions</th>
<th>OID</th>
<th>Include</th>
<th>Criticality</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BasicConstraints</td>
<td>[id-ce 19]</td>
<td>x</td>
<td>TRUE</td>
<td>n/a</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td>PathLenConstraint</td>
<td></td>
<td></td>
<td>n/a  Do not set!</td>
<td></td>
</tr>
<tr>
<td>KeyUsage</td>
<td>[id-ce 15]</td>
<td>x</td>
<td>TRUE</td>
<td>n/a</td>
</tr>
<tr>
<td>DigitalSignature</td>
<td></td>
<td></td>
<td>clear</td>
<td></td>
</tr>
<tr>
<td>NonRepudiation</td>
<td></td>
<td></td>
<td>clear</td>
<td></td>
</tr>
<tr>
<td>keyEncipherment</td>
<td></td>
<td></td>
<td>clear</td>
<td></td>
</tr>
<tr>
<td>DataEncipherment</td>
<td></td>
<td></td>
<td>clear</td>
<td></td>
</tr>
<tr>
<td>keyAgreement</td>
<td></td>
<td></td>
<td>clear</td>
<td></td>
</tr>
<tr>
<td>keyCertSign</td>
<td></td>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td>cRLSign</td>
<td></td>
<td></td>
<td>set</td>
<td></td>
</tr>
<tr>
<td>certificatePolicies</td>
<td>[id-ce 32]</td>
<td>X</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>policyIdentifier</td>
<td></td>
<td></td>
<td>1.3.6.1.4.1.6646.114176.37.1.1.1.2</td>
<td></td>
</tr>
<tr>
<td>policyQualifiers</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>PolicyQualifierInfo</td>
<td></td>
<td></td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Qualifier</td>
<td></td>
<td></td>
<td>Id-qt</td>
<td></td>
</tr>
<tr>
<td>CPSpointer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OID</td>
<td>1.3.6.1.5.5.7.2.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>value</td>
<td><a href="http://pki.chevron.com/policy">http://pki.chevron.com/policy</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>policyIdentifier</td>
<td>2.5.29.32.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Notice</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OID</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>value</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noticeRef</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>organization</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>noticeNumbers</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>explicitText</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorityKeyIdentifier</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 35]</td>
<td>X</td>
<td>98 16 da c2 82 9e 13 78 1e 77 f2 14 34 fd 44 b2 19 1b 24 e8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>keyIdentifier</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorityCertIssuer</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorityCertSerialNumber</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subjectKeyIdentifier</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 14]</td>
<td>X</td>
<td>98 16 da c2 82 9e 13 78 1e 77 f2 14 34 fd 44 b2 19 1b 24 e8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>privateKeyUsagePeriod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 16]</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>policyMappings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 33]</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subjectAltName</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 17]</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>issuerAltName</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 18]</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subjectDirectoryAttributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 9]</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nameConstraints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 30]</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>permittedSubtrees</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>excludedSubtrees</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>policyConstraints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 34]</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>policySet</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>requireExplicitPolicy</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inhibitPolicyMapping</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cRLDistributionPoints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[id-ce 31]</td>
<td>X</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>distributionPoint</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>distributionPointName</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reasons</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cRLIssuer</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Private Extensions**

Object Identifier | Include | Criticality | Value
---|---|---|---

Table 5 - Certificate Format and Extensions for the Intermediate CA certificate

<table>
<thead>
<tr>
<th>Base Certificate</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>MD5 hash of public key</td>
</tr>
<tr>
<td>Issuer DN</td>
<td>cn=Chevron Root CA, o=Chevron, c=US</td>
</tr>
<tr>
<td>Subject DN</td>
<td>cn=Chevron Intranet Intermediate 10, o=Chevron, c=US</td>
</tr>
<tr>
<td>NotBefore</td>
<td>0201091900000Z (7:00 PM January 9, 2002 GMT)</td>
</tr>
<tr>
<td>NotAfter</td>
<td>120109185959Z (Ten years later)</td>
</tr>
<tr>
<td>Public Key Algorithm</td>
<td>sha1-WithRSAEncryption (1 2 840 113549 1 1 5)</td>
</tr>
<tr>
<td>Parameters</td>
<td>NULL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard Extensions</th>
<th>OID</th>
<th>Include</th>
<th>Criticality</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BasicConstraints</td>
<td>{id-ce 19}</td>
<td>x</td>
<td>TRUE</td>
<td>n/a</td>
</tr>
<tr>
<td>CA</td>
<td></td>
<td></td>
<td></td>
<td>set</td>
</tr>
<tr>
<td>PathLenConstraint</td>
<td></td>
<td></td>
<td></td>
<td>n/a  Do not set!</td>
</tr>
<tr>
<td>KeyUsage</td>
<td>{id-ce 15}</td>
<td>x</td>
<td>TRUE</td>
<td>n/a</td>
</tr>
<tr>
<td>DigitalSignature</td>
<td></td>
<td></td>
<td></td>
<td>clear</td>
</tr>
<tr>
<td>NonRepudiation</td>
<td></td>
<td></td>
<td></td>
<td>clear</td>
</tr>
<tr>
<td>keyEncipherment</td>
<td></td>
<td></td>
<td></td>
<td>clear</td>
</tr>
<tr>
<td>DataEncipherment</td>
<td></td>
<td></td>
<td></td>
<td>clear</td>
</tr>
<tr>
<td>keyAgreement</td>
<td></td>
<td></td>
<td></td>
<td>clear</td>
</tr>
<tr>
<td>keyCertSign</td>
<td></td>
<td></td>
<td></td>
<td>set</td>
</tr>
<tr>
<td>cRLSign</td>
<td></td>
<td></td>
<td></td>
<td>set</td>
</tr>
<tr>
<td>certificatePolicies</td>
<td>{id-ce 32}</td>
<td>X</td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>policyIdentifier</td>
<td></td>
<td></td>
<td></td>
<td>1.3.6.1.4.1.6646.114176.37.1.1.1.2</td>
</tr>
<tr>
<td>policyQualifiers</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>PolicyQualifierInfo</td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>Qualifier</td>
<td></td>
<td></td>
<td></td>
<td>Id-qt</td>
</tr>
<tr>
<td>CPSpointer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OID</td>
<td></td>
<td></td>
<td></td>
<td>1.3.6.1.5.5.7.2.1</td>
</tr>
<tr>
<td>value</td>
<td></td>
<td></td>
<td></td>
<td><a href="http://pki.chevron.com/policy">http://pki.chevron.com/policy</a></td>
</tr>
<tr>
<td>policyIdentifier</td>
<td></td>
<td></td>
<td></td>
<td>2.5.29.32.0</td>
</tr>
<tr>
<td>User Notice</td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>Private Extensions</td>
<td>Object Identifier</td>
<td>Include</td>
<td>Criticality</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Root Set of Provisions**

**Public Key Infrastructure**

<table>
<thead>
<tr>
<th>OID</th>
<th>value</th>
<th>n/a</th>
</tr>
</thead>
<tbody>
<tr>
<td>noticeRef</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>organization</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>noticeNumbers</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>explicitText</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>authorityKeyIdentifier</td>
<td>{id-ce 35} X</td>
<td>98 16 da c2 82 9e 13 78 1e 77 f2 14 34 fd 44 b2 19 1b 24 e8</td>
</tr>
<tr>
<td>keyIdentifier</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>authorityCertIssuer</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>authorityCertSerialNumber</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>subjectKeyIdentifier</td>
<td>{id-ce 14} X</td>
<td>98 16 da c2 82 9e 13 78 1e 77 f2 14 34 fd 44 b2 19 1b 24 e8</td>
</tr>
<tr>
<td>privateKeyUsagePeriod</td>
<td>{id-ce 16}</td>
<td>n/a</td>
</tr>
<tr>
<td>policyMappings</td>
<td>{id-ce 33}</td>
<td>n/a</td>
</tr>
<tr>
<td>subjectAltName</td>
<td>{id-ce 17}</td>
<td>n/a</td>
</tr>
<tr>
<td>issuerAltName</td>
<td>{id-ce 18}</td>
<td>n/a</td>
</tr>
<tr>
<td>subjectDirectoryAttributes</td>
<td>{id-ce 9}</td>
<td>n/a</td>
</tr>
<tr>
<td>nameConstraints</td>
<td>{id-ce 30}</td>
<td>n/a</td>
</tr>
<tr>
<td>permittedSubtrees</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>excludedSubtrees</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>policyConstraints</td>
<td>{id-ce 34}</td>
<td>n/a</td>
</tr>
<tr>
<td>policySet</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>requireExplicitPolicy</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>inhibitPolicyMapping</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>cRLDistributionPoints</td>
<td>{id-ce 31} X</td>
<td>n/a</td>
</tr>
<tr>
<td>distributionPoint</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>distributionPointName</td>
<td>ldap:///CN=Chevron%20Root%20CA(1),CN=ChevronRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=corp,DC=114176,DC=net?certificateRevocationList?base?objectClass=cRLDistributionPoint or NULL</td>
<td></td>
</tr>
<tr>
<td>reasons</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>cRLIssuer</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>
7.2 CRL PROFILE

The following fields from the X.509 v2 CRL format are used.

Table 6 - CRL Format and Extensions

<table>
<thead>
<tr>
<th>Base CRL</th>
<th>OID</th>
<th>Include</th>
<th>Criticality</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>certificateList</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tbsCertList</td>
<td></td>
<td></td>
<td></td>
<td>See TBSCertList</td>
</tr>
<tr>
<td>signatureAlgorithm</td>
<td>sha-1WithRSAEncryption</td>
<td></td>
<td></td>
<td>{1.2.840.113549.1.1.5}</td>
</tr>
<tr>
<td>signatureValue</td>
<td></td>
<td></td>
<td></td>
<td>Computed by the CA when issuing the list.</td>
</tr>
<tr>
<td>tBSCertList</td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>Version</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Signature</td>
<td></td>
<td></td>
<td></td>
<td>sha-1WithRSAEncryption {1.2.840.113549.1.1.5}</td>
</tr>
<tr>
<td>Issuer</td>
<td></td>
<td></td>
<td></td>
<td>cn=Chevron Root CA, o= Chevron, c=US</td>
</tr>
<tr>
<td>thisUpdate</td>
<td></td>
<td></td>
<td></td>
<td>Date and time of CRL issuance</td>
</tr>
<tr>
<td>nextUpdate</td>
<td></td>
<td></td>
<td></td>
<td>Date and time of next expected CRL issuance</td>
</tr>
<tr>
<td>revokedCertificates</td>
<td></td>
<td></td>
<td></td>
<td>List of revoked certificate information</td>
</tr>
<tr>
<td>userCertificate</td>
<td></td>
<td></td>
<td></td>
<td>CertificateSerialNumber</td>
</tr>
<tr>
<td>revocationDate</td>
<td></td>
<td></td>
<td></td>
<td>Date and time of revocation</td>
</tr>
<tr>
<td>crlEntryExtensions</td>
<td></td>
<td></td>
<td></td>
<td>Not used</td>
</tr>
<tr>
<td>crlExtensions</td>
<td></td>
<td></td>
<td></td>
<td>See Extensions</td>
</tr>
<tr>
<td>Extensions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorityKeyIdentifier</td>
<td>[id-ce 35]</td>
<td>X</td>
<td></td>
<td>98 16 da e2 82 9e 13 78 1e 77 f2 14 34 fd 44 b2 19 b4 24 e8</td>
</tr>
<tr>
<td>keyIdentifier</td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>authorityCertIssuer</td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>issuerAltName</td>
<td>[id-ce 18]</td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>cRLNumber</td>
<td>[id-ce 20]</td>
<td>X</td>
<td></td>
<td>Incremented each time a particular CRL is changed</td>
</tr>
<tr>
<td>deltaCRLIndicator</td>
<td>[id-ce 27]</td>
<td></td>
<td></td>
<td>Not present</td>
</tr>
<tr>
<td>issuingDistributionPoint</td>
<td>[id-ce 28]</td>
<td>X</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>distributionPoint</td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>onlyContainsUserCerts</td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Base CRL</strong></td>
<td><strong>OID</strong></td>
<td><strong>Include</strong></td>
<td><strong>Criticality</strong></td>
<td><strong>Value</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>onlyContainsCACerts</td>
<td></td>
<td></td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>onlysomeReasons</td>
<td></td>
<td></td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>IndirectCRL</td>
<td></td>
<td></td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

**CRL Entry Extensions**

<table>
<thead>
<tr>
<th><strong>reasonCode</strong></th>
<th>[id-ce 21]</th>
<th>X</th>
<th>As appropriate</th>
</tr>
</thead>
<tbody>
<tr>
<td>holdInstructionCode</td>
<td>[id-ce 23]</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>invalidityDate</td>
<td>[id-ce 24]</td>
<td>X</td>
<td>As appropriate</td>
</tr>
<tr>
<td>certificateIssuer</td>
<td>[id-ce 29]</td>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

### 7.3 OCSP PROFILE

This PKI does not support either version 1 or version 2 of OCSP.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

An assessment of the PKI’s operations is performed at least once a year. The assessment will be either:

- A WebTrust for Certification Authorities audit,
- A similar examination by its internal audit department, or
- A self assessment under the supervision of the IMAA

In addition, prior to the completion of the initial assessment or audit, the independent CPA has observed the KGC for the Intermediate CA.

A reassessment shall be required every twelve (12) months; however, the PKI may need to be assessed more frequently. The interval between such reassessments will depend on the following:

- The nature and complexity of the PKI’s operations
- The significant changes to the PKI’s operations
- The relative effectiveness of the entity’s monitoring and change management controls
- The assessor’s professional judgment

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The assessor, who performs the audit, shall be approved by the Chevron PMA, and may be a licensed Certified Public Accountant (USA) or Chartered Accountant (Canada). In addition, he may hold the Certified Information Systems Auditor (CISA), Certified Information Systems Manager (CISM) or Certified Information Systems Security Practitioner (CISSP) designations, or other appropriate certifications. The assessor should have experience in the application of public key cryptographic technologies and general computer security.

8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY

If the assessment is not a self-assessment, then the assessor shall be independent of the PKI under audit as well as any service providers to the PKI under audit. For internal auditors, independence is defined in the Information Audit and Control Association’s IS Auditing Guideline – Organisational Relationship and Independence; and, for external auditors engaged in public practice, it is defined by Generally Accepted Auditing Standards.
8.4 TOPICS COVERED BY ASSESSMENT

The assessment compares the operations of the Chevron PKI to the criteria in the WebTrust Principles and Criteria for Certification Authorities. The WebTrust document describes a consistent set of measurement criteria for audit practitioners to use in testing and evaluating CA practices, and is organized into three (3) broad areas:

- CA Business Practices
- CA Service Integrity
- CA Environmental Controls

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

There are three (3) possible actions to be taken as a result of identification of a deficiency:

a) Continue to operate as usual

b) Continue to operate but with additional compensating controls until remedied

c) Suspend operations

If a deficiency is identified, the Chevron PMA, with input from the assessor, will determine which of these actions to take. If action a) or b) is taken, then the Chevron PMA and appropriate IMAA are responsible for ensuring that corrective actions are taken within thirty (30) days. At that time, or earlier if agreed by the PMA and assessor, the assessment team will reassess the PKI. If, upon reassessment, corrective actions have not been taken, the assessor will determine if more severe action [e.g., action c) above] is required. If action c) is taken, all certificates issued in the Chevron PKI, including the Root, any Intermediate, Issuing and Subscriber, and CA cross-certificates, are suspended/revoked prior to suspension of service. The Chevron PMA and appropriate IMAA are responsible for reporting the status of corrective action to the assessor on a weekly basis. The PMA and assessor together will determine when the re-assessment is to occur. Upon reassessment, if it is determined that the deficiencies have been corrected, the Chevron PKI will resume service and new certificates will be issued to PKI users and other external CAs, depending on conditions specified in individual Cross-Certification Agreements.

8.6 COMMUNICATION OF RESULTS

The assessor’s opinion and management letter are provided to the Chevron Audit Committee, the Chevron Director of Internal Audit, the Chevron Chief Technology Officer, the chairperson of the Chevron PMA, and the appropriate PA and IMAA.

Cross-Certification Agreements with business partner organizations may also dictate that cross-certified CAs be informed of any deficiencies. Unless specified in a particular Cross-Certification Agreement, no communication of the assessment results will occur outside of Chevron. Should external cross-certified CAs need to be informed, the chairperson of the Chevron PMA would communicate with his contact point in each of the cross-certified CAs in accordance with the terms of the relevant Cross-Certification Agreement or Bridge Certification Agreement.
9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

No stipulation - this section intentionally left blank.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

No stipulation - this section intentionally left blank.

9.2.2 Other Assets

No stipulation - this section intentionally left blank.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation - this section intentionally left blank.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

All information related to the PKI that is not specifically identified as confidential will be considered public information. A non-exclusive list of some specific examples of confidential information and non-confidential information appears in the following sections.

9.3.1 Scope of Confidential Information

The Root CA’s and Intermediate CAs’ private keys are confidential. Information held in audit trails is considered confidential to Chevron, and shall not be released outside the corporation unless required by law. HSM activation data is considered confidential.

Corporate information held by the Chevron Root CA or Intermediate CAs other than that, which is explicitly made available as part of a certificate, CRL/ARL, or Set of Provisions, or otherwise publicly disclosed, is considered confidential.

When Chevron revokes a certificate, a reason code may, but need not be, included in the CRL/ARL for the revoked certificate. This reason code is not considered confidential, and can be shared with all other users and Relying Parties. However, the details concerning the revocation are considered confidential.

Personal and corporate information held by the Chevron PKI other than that, which is explicitly made available as part of a certificate or CRL/ARL is considered confidential and shall not be released unless required by law.

The assessors management letter is considered confidential and may not be released except with prior approval of the PMA or unless required by law.
9.3.2 **Information Not Within the Scope of Confidential Information**

Information included in certificates and CRLs is not considered confidential, nor is this SoP considered confidential. The external auditor’s opinion letter is not considered confidential.

9.3.3 **Responsibility to Protect Confidential Information**

The individuals assigned to Trusted Roles are obligated to protect confidential information and not to disclose such information except unless required by law, regulation, or order of a court of competent jurisdiction. Any request for release of information shall be authenticated and approved by Chevron’s legal department before the release of that information.

9.4 **PRIVACY OF PERSONAL INFORMATION**

The Subjects of the Root CA are devices, not natural persons, so there is no obligation of the Root CA to protect personal information. The portions of this PKI that deal with personal information will protect the privacy of any personal information it may contain and abide by the privacy laws and regulations of the respective countries within which it operates.

9.5 **INTELLECTUAL PROPERTY RIGHTS**

Certificates and CRLs issued by Chevron are the property of Chevron.

This SoP is the property of Chevron.

The DNs used to represent entities within the Chevron PKI domain, in the directory and in certificates issued to End-Entities within that domain include a Relative Distinguished Name (RDN) for Chevron, and as such are the property of Chevron.

9.6 **REPRESENTATIONS AND WARRANTIES**

9.6.1 **CA Representations and Warranties**

No stipulation - this section intentionally left blank.

9.6.2 **RA Representations and Warranties**

No stipulation - this section intentionally left blank.

9.6.3 **Subscriber Representations and Warranties**

The Intermediate CAs are the only Subscribers of the Root CA. The administrators, who are natural persons, responsible for such Subscribers are obligated to:

- Make true representation at all times to the Root CA regarding information in certificates and other identification and authentication information
- Use certificates exclusively for legal and authorized company business consistent with the applicable certificate procedure and this SoP
- Protect private keys by storing them on a FIPS 140-1 Level 3 cryptographic device
- Maintain cryptographic material in a secure manner according to established Chevron procedures for handling such material
- Use the certificates and related technology in compliance with the laws and regulations of the countries where Chevron operates
- Inform Root CA IMAA immediately of a change to any information included in a certificate or certificate application request
- Inform all Chevron PKI IMAAs immediately of any suspected or actual compromise of the private keys

9.6.4 Relying Party Representations and Warranties

Notwithstanding the remainder of this section 9.6.4, only persons or entities expressly authorized by separate agreement with Chevron may act as Relying Parties or otherwise rely on a certificate issued under this SoP.

A certificate user, also known as a Relying Party, must perform certain checks before accepting a certificate. This obligation extends not only to the certificates issued by the Chevron Root CA, but also to all certificates issued within this PKI used for certificate validation chaining. Often, one wishes to rely on a certificate issued to an End-Entity rather than to the Root CA or an Intermediate CA. One of the checks begins by identifying a certificate chain from the End-Entity’s certificate back to a Root CA, and verifying the digital signatures on all certificates in the certificate chain. Within this PKI, a typical chain for a certificate issued to a Chevron employee would be: employee End-Entity certificate, Intranet Issuing CA certificate, Intranet Intermediate CA certificate and Root CA certificate. In other words, the certificates signed by the Root CA are part of the certificate chain that the putative Relying Party is obligated to check. Before any act of reliance, Chevron PKI users are obliged to:

- Independently assess the suitability of a certificate for any given purpose, and determine that the certificate will, in fact, be used appropriately
- Utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform as a condition of relying on certificates in connection with each such operation. Such operations identify the certificates in the chain, establish the validity period of the certificates, and verify the digital signatures on all certificates in the certificate chain, among other things. Relying Parties shall not rely on a certificate unless these verification procedures are successful
- Check the status of a certificate on which they wish to rely, and all the certificates in its certificate chain. If any of the certificates or cross-certificates in the certificate chain have been revoked, the Relying Party shall not rely on the End-Entity certificate or any other revoked certificate in the certificate chain.
- Relying Parties must conform to any applicable Relying Party Agreement or in the case of Chevron employees and contract workers, execute and conform to the subscriber agreement proffered by Chevron.
• If all of processes in this section 9.6.4 are successfully completed, then the Relying Party shall be entitled to rely on the certificate, provided that reliance upon the certificate is reasonable and in good faith in light of all the circumstances that were known or should have been known to the Relying Party at the time of reliance.

• If the circumstances indicate a need for additional assurances, then the Relying Party must obtain such assurances in order for such reliance to be deemed reasonable

• If a user of the Chevron PKI accepts an encrypted or signed transmission that cannot be validated, the user does so completely at his own risk

9.6.5 **Representations and Warranties of Other Participants**

No stipulation - this section intentionally left blank.

9.7 **DISCLAIMER OF WARRANTIES**

Chevron makes no representations or warranties whatsoever, express or implied, including without limitation, any representation with respect to any claim, cause of action, or any other matter arising from or related to this SoP.

9.8 **LIMITATIONS OF LIABILITY**

Chevron and all CAs in the Chevron PKI shall not be liable to any relying party for any direct, indirect, incidental, consequential or punitive damages whatsoever, for any matter arising out of or relating to this agreement or its subject matter, whether such liability is asserted on the basis of contract, tort, or any other theory of liability, and even if Chevron has been advised of the possibility of such damages. Further, this SoP does not create any right or obligation on behalf of any person or entity outside Chevron. Not withstanding, this section is not intended to abrogate any obligations prescribed under state, federal, or international law.

9.9 **INDEMNITIES**

No stipulation - this section intentionally left blank.

9.10 **TERM AND TERMINATION**

This SoP shall become effective upon its approval by the PMA and shall remain in effect until terminated by the PMA or superseded by a revised SoP.

9.10.1 **Term**

No stipulation - this section intentionally left blank.

9.10.2 **Termination**

The PMA may terminate this PKI upon thirty (30) days’ notice to the Subscribers.
9.10.3 Effect of Termination and Survival

The rights and obligations of the participants under Sections 1.4, 2.2, 2.4, 4.5, 4.9, 4.10, 5.5, 5.8, 6.2.2 through 6.2.11, 6.3.1, and 9 shall survive termination of this agreement.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation - this section intentionally left blank.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Any proposal for modification shall be submitted to the PMA. Any proposed changes to this SoP that the PMA has deemed to have significant impact, shall undergo a review and comment period.

9.12.2 Notification Mechanism and Period

Changes to this SoP which significantly impact the SoP, as determined by the PMA, shall undergo an appropriate public review and comment period.

If the PMA decides to make no changes during the review period, the initially proposed modified document shall become final and shall be published in the Repository.

Participating Subscribers, Sponsors and Relying Parties should periodically check the Repository for notice of intended modifications to this SoP.

9.12.3 Circumstances Under Which OID Must Be Changed

Changes to this SoP that, in the judgment of the PMA may have significant impact, will once effective, require an increment to the last arc of the OID for this SoP as described in Section 1.2. For example the OID of this SoP, which is 1.3.6.1.4.1.6646.114176.37.1.2.1.1, would be superceded by the OID of the new SoP, which would be, 1.3.6.1.4.1.6646.114176.37.1.2.1.2

9.13 DISPUTE RESOLUTION PROVISIONS

Any dispute between Chevron PKI users, one acting as a Subscriber and one acting as a Relying Party; or, between Chevron users and a Chevron PKI CA or RA, shall first be reported to the Chevron IMAA for resolution. In the event the IMAA cannot resolve the dispute, the PMA shall be the final arbiter.

Any dispute between the Chevron PKI and other PKIs where Chevron has established Cross-Certification Agreements, Bridge Certification Agreements, or Relying Party Agreement shall commence pursuant to this Section 9.13 of this agreement.
If a dispute arises out of or relates to this Agreement, or the breach thereof, and the dispute cannot be settled, the parties agree first to try in good faith to settle the dispute by mediation administered by mutually agreed upon mediation service before resorting to arbitration. The parties shall settle any dispute arising out of or related to this Agreement, or the breach thereof, by arbitration in San Francisco Bay Area, California. A single arbitrator shall be agreed upon by the parties, or if the parties cannot agree upon an arbitrator within thirty (30) days, then the parties agree that a single arbitrator shall be appointed by the American Arbitration Association. The arbitrator may award attorneys' fees and costs as part of the award. The award of the arbitrator shall be non-binding.

No waiver of any provision hereof or of any right or remedy hereunder shall be effective unless in writing and signed by the party against whom such waiver is sought to be enforced. No delay in exercising, no course of dealing with respect to, or no partial exercise of any right or remedy hereunder shall constitute a waiver of any other right or remedy, or future exercise thereof.

If any provision of this Agreement is determined to be invalid under any applicable statute or rule of law, it is to that extent to be deemed omitted, and the balance of the Agreement shall remain enforceable.

9.14 GOVERNING LAW

The laws of the State of California, excluding its conflict of laws rules, shall govern the construction, validity, interpretation, enforceability and performance of this SoP and any Subscriber Agreement. Any dispute related to this SoP, any Subscriber Agreement, or any certificate issued by the Root CA or any services provided by Root CA shall be brought in the courts of the State of California; and, each person, entity or organization hereby agrees that such courts shall have personal and exclusive jurisdiction over such disputes. In the event that any matter arising from this agreement is filed in court, the parties to such action waive any right to a jury trial.

9.15 COMPLIANCE WITH APPLICABLE LAW

This SoP is subject to any applicable national and foreign laws, rules, regulations, ordinances, decrees and orders including, but not limited to, restrictions on exporting or importing software, hardware or technical information.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

This SoP constitutes the entire understanding between the parties and supersedes all other terms, whether express or implied by law. No modification of this SoP shall be of any force or effect unless in writing and signed by an authorized signatory. Failure to enforce any or all of these sections in a particular instance or instances shall not constitute a waiver thereof or preclude subsequent enforcement thereof. All provisions in this SoP, which by their nature extend beyond the term of the performance of the services such as, without limitation, those concerning confidential information and intellectual property rights, shall survive such term until fulfilled and will apply to any party’s successors and assigns.

9.16.2 Assignment
9.16.3 Severability

Whenever possible, each provision of SoP, and any Subscriber Agreements shall be interpreted in such manner as to be effective and valid under applicable law. If any part or parts of these terms are held to be invalid, the remainder shall remain valid and enforceable.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation - this section intentionally left blank.

9.16.5 Force Majeure

Under this SoP the PKI shall be relieved from any liability whatsoever for any losses, costs, expenses, liabilities, damages or claims, arising out of or related to delays in performance or from failure to perform due to any natural causes beyond reasonable control.

9.17 OTHER PROVISIONS

9.17.1 Conflict of Provisions

In the event of a conflict between the provisions of this SoP and any Subscriber Agreement, the order of precedence shall be the SoP and then the Subscriber Agreement.

9.17.2 Limitation Period on Actions

Any legal actions involving a dispute that is related to this PKI or any services provided involving a certificate issued by this PKI shall be commenced within one (1) year after the expiration or revocation of such certificate in dispute, or the date of provision of the disputed service or services involving the PKI certificate, whichever is earlier. If any action arising out of a dispute related to a certificate issued by this PKI or any service involving certificates issued by this PKI is not commenced prior to such time, any such action shall be barred.