X.509 CERTIFICATE POLICY FOR THE HALLIBURTON COMMON PKI

VERSION 3.7

March 14, 2011

REVISION HISTORY

Document Version	Document Date	Revision Details
3.1	4/20/2010	First working draft circulated for comment.
3.2	4/26/2010	Incorporated first round of comments.
3.3	5/21/2010	Added policy summary chart to intro, minor typos, and rephrased “Common Policy” to “Halliburton Common” (e.g. Halliburton Common Root CA) for CA role clarity
3.4	5/26/2010	Modified key validity period, replaced the HAL Policy Authority references with Halliburton IT Security.
3.5	6/6/2010	Changed naming convention of the policies, added no assurance OID tree (509.0).
3.6	09/21/2010	Minor formatting changes and removal of specific types of audit events required to be recorded (section 5.4.1). Changed required FIPS 140-2 Level (3 to 2) for HSM for HalPkiHigh Issuing CA. Clarification of CRL publication and auditing log requirements.
3.7	03/14/2011	Change IT Security Manager references to IT Security Director. Replaced references to the Halliburton Management Authority (HAL-MA) with IT Security Operations. Created new production issuance policy (HalPkiDeviceVeryLow) for certificates not used for either nonrepudiation or authentication.

CONTENTS

1: INTRODUCTION

This Certificate Policy (CP) includes eight distinct certificate issuance policies: two policies for Active Directory (AD) enrolled or AD authenticated human sponsored devices with different assurance levels, a policy for devices with an RA validated, human sponsor, a policy for Active Directory (AD) auto-enrolled users not for nonrepudiation functions (i.e. file encryption only), and three user nonrepudiation policies (users with software cryptographic modules, users with hardware cryptographic modules, and a high assurance user policy). Where a specific policy is not stated, the policies and procedures in this specification apply equally to all policies.

Following is a table summarizing the policies and their differences:

Policy	HalPkiDevicesVery Low	HalPkiDevicesLow	HalPkiDevices	HalPkiEncrypt	HalPkiLow	HaPkiSoftware	HalPkiHardware	HalPkiHigh
OID 1.3.6.1.4.1.17493	.509.1.2	.509.1.0	509.1.1	.509.1.10	.509.1.11	.509.1.12	.509.1.13	.509.1.14
Subject Type	Device	Device	Device	User	User	User	User	User
Use	Neither Nonrepudiation nor Data Encryption	Nonrepudiation	Nonrepudiation	Data Encryption Only	Nonrepudiation	Nonrepudiation	Nonrepudiation	Nonrepudiation
Assurance Level	Very Low	Low	Medium	Low	Low	Medium	High	Very High
Subscriber private key Storage	Software	Software	Software (FIPS 140-2 level 1 or higher)	Software (FIPS 140-2 level 1 or higher)	Software (FIPS 140-2 level 1 or higher)	Software (FIPS 140-2 level 1 or higher)	Hardware (FIPS 140-2 level 2 or higher)	Hardware (FIPS 140-2 level 2 or higher)
Authentication Requirements	AD	AD	RA: In Person or Enrollment Agent	AD	AD	RA: In Person or Enrollment Agent	RA: In Person or Enrollment Agent	RA: In Person Only
Enrollment Method	Enrollment Agent	Domain Auto or Manual	Manual	Domain Auto	Domain Auto or Manual	Manual	Manual	Manual
In-person Re-Registration	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	At least every 9 years	At least every 9 years	At least every 3 years
Issuing CA FIPS 140-2 Level	No stipulation	2 or higher	2 or higher	2 or higher	2 or higher	2 or higher	2 or higher	2 or higher
Key Escrow Permitted	**Yes**	**Yes**	**Yes**	**Yes**	**No**	**No**	**No**	**No**

The 1.3.6.1.4.1.17493.509.0 tree has been set aside for testing.

The user policies apply to certificates issued to Halliburton employees and other affiliated personnel for the purposes of authentication, signature, and/or confidentiality.

A PKI under this CP will provide the following security management services:

- Key generation/storage
- Certificate generation, modification, re-key, and distribution
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g. security audit, configuration management, archive.)

The nonrepudiation, user policies (HalPkiLow, HalPkiSoftware, HalPkiHardware, and HalPkiHigh) require Halliburton employees and other affiliated personnel to use FIPS 140-2 validated cryptographic modules (hardware or software) for cryptographic operations and the protection of private keys. With the exception of HalPkiDeviceVeryLow, all policies require the use of FIPS 140-2 validated, hardware cryptographic modules at all levels of the CA hierarchy. CAs issuing only end-entity certificates under the HalPkiDeviceVeryLow policy are exempt from the FIPS 140-2 validated, hardware cryptographic modules requirement.

The HalPkiDeviceVeryLow issuance policy is not to be used for either nonrepudiation, including primary authentication of people or devices, or data encryption purposes. Its purpose is to facilitate infrastructure capabilities that require certificates to enable them such as a health certificates for Microsoft Network Access Protection. Use for the authentication to remote network, wireless network, system, or data access is strictly prohibited.

Any CA that asserts this CP in certificates must obtain written approval from Halliburton IT Security prior to beginning operations. CAs that issue certificates under this policy may operate simultaneously under other policies. Such CAs must not assert the OIDs in this policy in certificates unless they are issued in accordance with all the requirements of this CP.

This CP is consistent with RFC 3647***, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework***.

1.1: OVERVIEW

1.1.1: CERTIFICATE POLICY (CP)

Certificates issued under this CP contain a registered certificate policy Object Identifier (OID) which a relying party may use to decide whether a certificate is trusted for a particular purpose. This CP applies only to CAs owned by or operated on behalf of Halliburton that issue certificates according to this Certificate Policy.

1.1.2: RELATIONSHIP BETWEEN THE CP AND THE CPS

This CP states what assurance can be placed in a certificate issued by the CA. The certificate practice statement (CPS) states how the CA establishes that assurance. Each CA that issues certificates under this CP shall have a corresponding CPS.

1.1.3: SCOPE

This CP applies to certificates issued to CAs, devices, and Halliburton employees and other affiliated personnel.

1.1.4: INTEROPERATION WITH CAS ISSUING UNDER DIFFERENT POLICIES

Interoperation with CAs that issue under different Certificate Policies will be achieved through policy mapping and cross-certification. Cross certification will be done at the sole of Halliburton IT Security. Note that interoperability may also be achieved through other means, such as trust lists.

Root and Policy CA certificates are available from http://aia.halliburton.com.

1.2: DOCUMENT NAME AND IDENTIFICATION

The 1.3.6.1.4.1.17493.509.0 OID tree has been set aside for CA testing. The 1.3.6.1.4.1.17493.509.1 OID tree has been designated for production issuance policies under this CP. The 1.3.6.1.4.1.17493.509.3 OID tree has been set aside for Certificate Policy and Certificate Practice Statement identification. This CP has been assigned the OID 1.3.6.1.4.1.17493.509.3.0.

Certificates issued in accordance with this CP shall assert at least one of the following OIDs in the certificate policy extension:

HalTestNoTrust::={1.3.6.1.4.1.17493.509.0.1}
HalPkiDevicesVeryLow::= {1.3.6.1.4.1.17493.509.1.2}
HalPkiDevicesLow::= {1.3.6.1.4.1.17493.509.1.0}
HalPkiDevices::= {1.3.6.1.4.1.17493.509.1.1}
HalPkiEncrypt::= {1.3.6.1.4.1.17493.509.1.10}
HalPkiLow::= {1.3.6.1.4.1.17493.509.1.11}
HalPkiSoftware::= {1.3.6.1.4.1.17493.509.1.12}
HalPkiHardware::= {1.3.6.1.4.1.17493.509.1.13}
HalPkiHigh::= {1.3.6.1.4.1.17493.509.1.14}

Certificates issued to CAs may contain any or all of these OIDs. Issuing CAs may not issue under both the trusted and non-trusted policies. Subscriber certificates issued to devices under this CP shall include HalPkiDevices, HalPkiDevicesLow, and HalPkiDevicesVeryLow. Subscriber certificates issued to human users may contain HalPkiEncrypt, HalPkiLow, HalPkiSoftware, HalPkiHardware, or HalPkiHigh.

CAs operating solely under the 1.3.6.1.4.1.17493.509.0 OID tree are explicitly exempt from all Policy requirements with the exception of an identified CA Management Authority, written approval from IT Security to begin operation, and notice of termination of CA operations. Subscriber certificates issued under such CAs must be issued with the Issuance Policy name of HalTestNoTrust and an OID of 1.3.6.1.4.1.17493.509.0.1 No trust should be placed within a certificate with such an OID.

1.3: PKI PARTICIPANTS

1.3.1: PKI AUTHORITIES

1.3.1.1: HALLIBURTON IT SECURITY

The Halliburton IT Security organization, under the direction of the IT Security Director, will:

- Oversee and manage this CP
- Review and approve the CPS of each CA issuing certificates under this CP, and
- Review compliance audit results of the Halliburton Root CA and subordinate CAs

1.3.1.2: CA MANAGEMENT AUTHORITIES

The Halliburton Common Root CA is operated and maintained by IT Security Operations.

Organizations that operate a CA under this CP, or contract for the services of a CA under this policy, shall establish a management body to manage any non-IT Security operated components (e.g. RAs or repositories) and resolve name space collisions. This body shall be referred to as a CA Management Authority (CA-MA).

1.3.1.3: CERTIFICATION AUTHORITY

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The CA is responsible for the issuing and managing certificates including:

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7: CERTIFICATE STATUS SERVERS

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through on-line transactions. In particular, PKIs may include OCSP responders to provide on-line status information. Such an authority is termed a certificate status server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. Examples include OCSP servers that are identified in the authority information access (AIA) extension. OCSP servers that are locally trusted, as described in RFC 2560, ***X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP***, are not covered by this CP.

1.3.2: REGISTRATION AUTHORITIES

Registration Authorities (RAs) collect and verify each subscriber's identity and information that is to be entered into the subscriber's public key certificate. The RA performs its function in accordance with a CPS approved by Halliburton IT Security. The RA is responsible for:

- Control over the registration process
- The identification and authentication process.

1.3.3: ENROLLMENT AGENTS

The Enrollment Agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA. The Enrollment Agent records information from and verifies biometrics (e.g. photographs) on presented credentials for applicants who cannot appear in person at an RA. The CPS will identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness.

1.3.4: SUBSCRIBERS

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the key and certificate in accordance with the policy asserted in the certificate, and does not issue certificates. For this CP, subscribers are limited to Halliburton employees, affiliated personnel, and devices operated by or on behalf of Halliburton. While technically CAs may be considered "subscribers" in a PKI, "subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

A subset of human subscribers may be issued role-based certificates. These certificates will identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name and are issued in the interest of supporting accepted business practices. The role-based certificate can be used in situations where nonrepudiation is desired. Normally, it will be issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of "IT Security Forensic Investigator" however, each of the four individual

certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that are held by a unique individual within an organization (e.g. Chief Information Officer).

1.3.5: RELYING PARTIES

A relying party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A relying party may use information in the certificate to determine the suitability of the certificate for a particular use.

For this CP, the relying party may be any entity that wishes to validate the binding of a public key to the name (or role) of a Halliburton employee or other affiliated personnel.

1.3.6: OTHER PARTICIPANTS

The CAs and RAs operating under this CP may require the services of other security, community, and application authorities, such as Compliance Auditors and attribute authorities. The CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.4: CERTIFICATE USAGE

1.4.1: APPROPRIATE CERTIFICATE USES

Halliburton PKI Certificates are strictly for Halliburton business use only.

1.4.2: PROHIBITED CERTIFICATE USES

No stipulation.

1.5: POLICY ADMINISTRATION

1.5.1: ORGANIZATION ADMINISTERING THE DOCUMENT

Halliburton IT Security is responsible for oversight and management of this Certificate Policy.

1.5.2: CONTACT PERSON

Questions regarding this CP should be directed to:

Director, IT Security
Halliburton
10200 Bellaire Blvd
Houston, TX 77072-5206

1.5.3: PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The Halliburton IT Security Director must determine the suitability of any CPS under this CP.

1.5.4: CPS APPROVAL PROCEDURES

CAs issuing under this CP are required to meet all facets of the policy. Halliburton IT Security will not issue waivers/exceptions to this CP.

The Halliburton IT Security Director shall make the determination that a CPS complies with this CP. The CA and RA must meet all requirements of an approved CPS before commencing operations. In some cases, additional approval of another Halliburton organization (e.g. Legal, Risk Management) may be required. The Halliburton IT Security Director will make this determination based on the nature of the system function, the type of communications, or the operating environment.

1.6: DEFINITIONS AND ACRONYMS

AD: Active Directory (specifically Microsoft Active Directory)
CA: Certification Authority
CA-MA: CA Management Authority (Non- Halliburton Common Root CA)
CP: Certificate Policy
CPS: Certificate Practice Statement
CRL: Certificate Revocation List
CSS: Certificate Status Server
DN: Distinguished Name
ECDSA: Elliptic Curve Digital Signature Algorithm
FIPS: Federal Information Processing Standards
HTTP: Hypertext Transfer Protocol
IETF: Internet Engineering Task Force
LDAP: Lightweight Directory Access Protocol
OCSP: Online Certificate Status Protocol
OID: Object Identifier
PII: Personally Identifying Information
PKCS: Public Key Cryptography Standards
PKI: Public Key Infrastructure
PSS: Probabilistic Signature Scheme
RA: Registration Authority
RFC: Request for Comments (Internet Engineering Task Force (IETF) standards document)
RSA: Rivest-Shamir-Adleman (encryption algorithm)
RSASSA: RSA Signature Scheme with Appendix
SHA: Secure Hash Algorithm
S/MIME: Secure/Multipurpose Internet Mail Extensions
SSL: Secure Sockets Layer
UPS: Uninterruptible power supply
URL: Uniform Resource Locator

Administrator: One of the four defined Trusted Roles within each CA Management Authority. See section 5.2.1.1 for additional details.

Backup Operator: One of the four defined Trusted Roles within each CA Management Authority. See section 5.2.1.4 for additional details.

CA Management Authority - entity created by an organization that operates a CA under this CP to manage any non-IT Security operated components and resolve name space collisions.

Certificate Manager: One of the four defined Trusted Roles within each CA Management Authority. See section 5.2.1.2 for additional details.

Compliance Auditor: A person with sufficient training, experience, qualifications, and independence from the CA being audited to perform a compliance audit to verify that a CA, and its recognized RAs, comply with all the requirements of the current versions of this CP and the CA's CPS. All aspects of the CA/RA operation are subject to compliance audit inspections. Note this is not the same function as the Trusted Role of Security Auditor.

Enrollment Agent: A person who satisfies all the trustworthiness requirements for a Registration Authority (RA) and who performs identity proofing as a proxy for the RA.

Management Authority: See *CA Management Authority.*

Registration Authority: An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates.

Relying Party: A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Security Auditor: One of the four defined Trusted Roles within each CA Management Authority. See section 5.2.1.3 for additional details. Note this is not the same as the Compliance Auditor.

Subscriber: An entity that (1) is the subject named or identified in a certificate issued to that entity, (2) that holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.

Trusted Certificate: A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Role: A CA functional/operational role whose incumbent performs functions that can introduce security problems if not carried out properly (accidentally or maliciously). The primary Trusted Roles defined in this policy are Administrator, Certificate Manager, Security Auditor, and Backup Operator.

Two-Person Control: Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.

Zeroize: A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

2: PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1: REPOSITORIES

All CAs that issue certificates under this CP are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a directory that is publicly accessible through the Lightweight Directory Access Protocol (LDAP) and Hypertext

Transport Protocol (HTTP). To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the CA or other parties.

2.2: PUBLICATION OF CERTIFICATION INFORMATION

2.2.1: PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

The publicly accessible directory system shall be designed and implemented so as to provide a minimum of 99% availability overall and limit scheduled down-time to at most 0.5% annually. Where applicable, the certificate status server (CSS) shall be designed and implemented to meet these same requirements.

2.2.2: PUBLICATION OF CA INFORMATION

This Certificate Policy shall be made publicly available at http://pki.halliburton.com. There is no requirement for the publication of CPSs of CAs that issue certificates under this CP.

2.2.3: INTEROPERABILITY

No stipulation.

2.3: TIME OR FREQUENCY OF PUBLICATION

This CP and any subsequent changes shall be made publicly available within thirty days of approval.

Publication requirements for CRLs are provided in sections 4.9.7 and 4.9.12

2.4: ACCESS CONTROLS ON REPOSITORIES

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. Direct and/or remote access to other information in the CA repositories shall be determined by CA-MA pursuant to their authorizing and controlling statutes. The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions the restricted information may be made available.

3: IDENTIFICATION AND AUTHENTICATION

3.1: NAMING

3.1.1: TYPES OF NAMES

For certificates issued under this CP, a clearly distinguishable and unique X.501 Distinguished Name shall be assigned to all subscribers for use within the subject name field. Signature certificates issued under HalPkiHardware or HalPkiHigh may be issued with a common name that specifies an organizational role. The combination of organizational role and department within the common name must unambiguously identify a *single* person. Where the department is implicit in the role, it may

be omitted. Where the role alone is ambiguous (e.g. Vice President) the department/PSL must be present in the common name. Widely held roles, such as System Administrator, cannot be included since they do not identify a particular person. Chief Executive Officer could be included as it specifies a role held by a single person.

Devices that are the subject of certificates issued under this CP shall be assigned either an Active Directory Distinguished Name or an Internet domain component name. The DN must be from a production domain that is IT managed and implements all of the standard controls. The common name should be a descriptive name for the device. Where a device is fully described by the Internet domain name, the common name attribute is optional.

3.1.2: NEED FOR NAMES TO BE MEANINGFUL

The subscriber certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates must identify in a meaningful way the subscriber to which they are assigned.

The common name must represent the subscriber in a way that is easily understandable for humans. While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this CP. If included, the common name must describe the issuer.

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 3280, ***Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile***.

3.1.3: ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The CA shall not issue anonymous certificates. Pseudonymous certificates may be issued by the CA to support internal operations. CAs may also issue pseudonymous certificates that identify subjects by their organizational roles, as described in section 3.1.1. CA certificates issued by the CA shall not contain anonymous or pseudonymous identities.

3.1.4: RULES FOR INTERPRETING VARIOUS NAME FORMS

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in RFC 2822, ***Internet Message Format***.

3.1.5: UNIQUENESS OF NAMES

Name uniqueness for certificates issued by each CA must be enforced. Each CA and its associated RAs shall enforce name uniqueness within the X.500 name space. When other name forms are used, they too must be allocated such that name uniqueness is ensured for certificates issued by that CA.

The CPS shall identify the method for the assignment of subject names. Directory information trees may be assigned to a single CA, or shared between CAs. Where multiple CAs share a single directory information tree, Halliburton IT Security shall review and approve the method for assignment of subject names.

3.1.6: RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

CAs operating under this CP shall not issue a certificate knowing that it infringes the trademark of another.

3.2: INITIAL IDENTITY VALIDATION

3.2.1: METHOD TO PROVE POSSESSION OF PRIVATE KEY

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key corresponding to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value supplied by the CA. The CA shall then validate the signature using the party's public key. Halliburton IT Security may allow other mechanisms that are at least as secure as those cited here.

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required.

3.2.2: AUTHENTICATION OF ORGANIZATION IDENTITY

Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing CA certificates, an authority for the issuing CA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

3.2.3: AUTHENTICATION OF INDIVIDUAL IDENTITY

This CP allows a certificate to be issued only to a single entity. Certificates shall not be issued that contain a public key whose associated private key is shared.

3.2.3.1: AUTHENTICATION OF HUMAN SUBSCRIBERS

With the exception of HalPkiLow, an RA shall ensure that the applicant's identity information is verified for certificates supporting user nonrepudiation (i.e. authentication, digital signatures): HalPkiSoftware, HalPkiHardware, and HalPkiHigh. The validation of identity of the subscriber under HalPkiLow and HalPkiEncrypt is conducted via standard Halliburton domain authentication against Active Directory: HalPkiEncrypt is not intended for nonrepudiation purposes. The domain must be a production domain that is IT managed and implements all of the standard account controls.

For HalPkiHigh, the applicant must appear at the RA in person. For HalPkiSoftware, HalPkiHardware, and HalPkiHigh, RAs may accept authentication of an applicant's identity attested to and documented by an Enrollment Agent to support identity proofing of remote applicants. Identity shall be verified no more than 30 days before initial certificate issuance. Authentication by an Enrollment Agent does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g. by checking official records) in step 3), and the maintenance of biometrics in step 4) as listed below.

At a minimum, authentication procedures for employees must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by Halliburton management.
2) Verify Applicant's employment through use of official company records.
3) Establish applicant's identity by in-person proofing before the registration authority, based on either of the following processes:
    a) The applicant presents a government-issued form of identification (e.g. a passport, or driver's license) as proof of identity, and
    b) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and

c) The applicant presents current corroborating information (e.g. current credit card bill or recent utility bill) to the RA. The identifying information (e.g. name and address) on the credential presented in step 3) a) above shall be verified by the RA for currency and legitimacy.

4) Record and maintain a biometric of the applicant (e.g. a photograph or fingerprint) by the RA or CA. This establishes an audit trail for dispute resolution. Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this CP.

For affiliated personnel, the authentication procedures must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring Halliburton manager.
2) Verify sponsoring Halliburton manager's identity and employment through either one of the following methods:
   a) A digitally signed request from the sponsoring Halliburton employee, verified by a currently valid employee signature certificate issued by a Halliburton Common PKI CA, may be accepted as proof of both employment and identity,
   b) In-person identity proofing of the sponsoring Halliburton employee may be established before the registration authority as specified in employee authentication above and employment validated through use of the official Company records.
3) Establish applicant's identity by in-person proofing before the registration authority, based on either of the following processes:
   a) The applicant presents a government-issued form of identification (e.g. a passport, or driver's license) as proof of identity, and
   b) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and
   c) The applicant presents current corroborating information (e.g. current credit card bill or recent utility bill) to the RA. The identifying information (e.g. name and address) on the credential presented in step 3) a) above shall be verified by the RA for currency and legitimacy.
4) Record and maintain a biometric of the applicant (e.g. a photograph or fingerprint) by the RA or CA. This establishes an audit trail for dispute resolution. Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Applicant;
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication.

For all nonrepudiation, user policies except HalPkiHigh where it is not possible for applicants to appear in person before the RA, an Enrollment Agent may serve as proxy for the RA. The Enrollment Agent forwards the information collected from the applicant directly to the RA in a secure manner. The requirement for recording a biometric of the applicant may be satisfied by providing passport-style photographs to the Enrollment Agent. The Enrollment Agent shall verify the photographs against the appearance of the applicant and the biometrics on the presented credentials and securely incorporate the

biometric as a component in the notarized package. Packages secured in a tamper-evident manner by the Enrollment Agent satisfy this requirement; other secure methods are also acceptable.

3.2.3.2: AUTHENTICATION OF DEVICES

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. Under the HalPkiDevices policy, the device must have a human sponsor. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g. serial number) or service name (e.g. DNS name)
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required.

The identity of the sponsor shall be authenticated by:

- Verification of digitally signed messages sent from the sponsor using a certificate issued under this CP; or
- In-person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of section 3.2.3.1.

Under the HalPkiDevicesLow or HalPkiDevicesVeryLow policy, authentication is to be conducted via:

- Halliburton domain membership of the device against Active Directory; or
- Halliburton domain authentication of the sponsor against Active Directory.

In either case, the domain must be a production domain that is IT managed and implements all of the standard account controls.

3.2.4: NON-VERIFIED SUBSCRIBER INFORMATION

Information that is not verified shall not be included in certificates. This includes, but it not limited to, information included in the Subject Alternative Name (SAN) field.

3.2.5: VALIDATION OF AUTHORITY

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the individual's authority to act in the name of the organization. For pseudonymous certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

3.2.6: CRITERIA FOR INTEROPERATION

Halliburton IT Security shall determine the interoperability criteria for CAs operating under this CP.

3.3: IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1: IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

CA certificate re-key shall follow the same procedures as initial certificate issuance.

Identity may be established through use of current signature key, except that identity shall be established through an in-person registration process at least once every three years under HalPkiHigh and at least once every nine years for all other policies requiring in-person registration.

3.3.2: IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per section 3.2 above.

3.3.2: IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

4: CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1: CERTIFICATE APPLICATION

The certificate application process must provide sufficient information to:

- Establish the applicant's authorization to obtain a certificate. (per section 3.2.3)
- Establish and record identity of the applicant. (per section 3.2.3)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required. (per section 3.2.1)
- Verify any role or authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the PKI Authorities and applicants that does not defeat security, but all must be completed before certificate issuance.

4.1.1: WHO CAN SUBMIT A CERTIFICATE APPLICATION

4.1.1.1: CA CERTIFICATES

An application for a CA certificate shall be submitted by an authorized representative of the applicant CA.

4.1.1.2: USER CERTIFICATES

An application for a user (subscriber) certificate shall be submitted by either the applicant or an Enrollment Agent.

4.1.1.3: DEVICE CERTIFICATES

An application for a device certificate shall be submitted by the human sponsor of the device.

4.1.2: ENROLLMENT PROCESS AND RESPONSIBILITIES

All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

4.2: CERTIFICATE APPLICATION PROCESSING

Information in certificate applications must be verified as accurate before certificates are issued. PKI Authorities shall specify procedures to verify information in certificate applications.

4.2.1: PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in sections 3.2 and 3.3 of this CP. The PKI Authority must identify the components of the PKI Authority (e.g. CA or RA) that are responsible for authenticating the subscriber's identity in each case.

4.2.2: APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

For the Halliburton Common Root CA, the Halliburton IT Security Operations Manager may approve or reject a certificate application.

For CAs operating under this CP, approval or rejection of certificate applications is at the discretion of the CA-MA or its designee.

4.2.3: TIME TO PROCESS CERTIFICATE APPLICATIONS

Certificate applications must be processed and a certificate issued within 30 days of identity verification.

4.3: CERTIFICATE ISSUANCE

4.3.1: CA ACTIONS DURING CERTIFICATE ISSUANCE

Upon receiving the request, the CAs/RAs will—

- Verify the identity of the requester.
- Verify the authority of the requester and the integrity of the information in the certificate request.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in section 9.6.3.

The certificate request may already contain a certificate built by either the RA or the subscriber. This certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in a CA's CPS.

4.3.2: NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

CAs operating under this CP shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA shall inform the human sponsor.

4.4: CERTIFICATE ACCEPTANCE

Before a subscriber can make effective use of its private key, a PKI Authority shall explain to the subscriber its responsibilities as defined in section 9.6.3.

4.4.1: CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

For the Halliburton Common Root CA, failure to object to the certificate or its contents shall constitute acceptance of the certificate.

For all other CAs operating under this CP, no stipulation.

4.4.2: PUBLICATION OF THE CERTIFICATE BY THE CA

As specified in 2.1, all CA certificates shall be published in repositories.

This CP makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.4.3: NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Halliburton IT Security must be notified whenever a CA operating under this CP issues a CA certificate.

4.5: KEY PAIR AND CERTIFICATE USAGE

4.5.1: SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

The intended scope of usage for a private key is specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2: RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Halliburton Common PKI-issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this CP shall issue CRLs specifying the current status of all unexpired certificates with the exception of OCSP responder certificates that include the id-pkix-ocsp-nocheck extension. It is recommended that relying parties process and comply with this information whenever using Common Policy certificates in a transaction.

4.6: CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1: CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Subscriber certificates issued under this CP shall not be renewed, except during recovery from CA key compromise (see 5.7.3). In such cases, the renewed certificate shall expire as specified in the original subscriber certificate.

CA Certificates and OCSP responder certificates may be renewed so long as the aggregated lifetime of the public key does not exceed the certificate lifetime specified in section 6.3.2.

The CA may automatically renew certificates during recovery from key compromise.

4.6.2: WHO MAY REQUEST RENEWAL

For all CAs and OCSP responders operating under this CP, the corresponding operating authority may request renewal of its own certificate. For the Halliburton Common Root CA, the IT Security Operations may also request renewal of CA certificates.

4.6.3: PROCESSING CERTIFICATE RENEWAL REQUESTS

For the Halliburton Common Root CA, CA certificate renewal for reasons other than re-key of the Halliburton Common Root CA shall be approved by Halliburton IT Security.

For all other renewal requests, no stipulation.

4.6.4: NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

The CA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate.

4.6.5: CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

For certificates issued by the Halliburton Common Root CA, failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this CP, no stipulation.

4.6.6: PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

This CP makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.6.7: NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No stipulation.

4.7: CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Subscribers shall identify themselves for the purpose of re-keying as required in section 3.3.

4.7.1: CIRCUMSTANCE FOR CERTIFICATE RE-KEY

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers.) Examples of circumstances requiring certificate re-key include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

4.7.2: WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Requests for certification of a new public key shall be considered as follows:

Subscribers with a currently valid certificate may request certification of a new public key. CAs and RAs may request certification of a new public key on behalf of a subscriber. For device certificates, the human sponsor of the device may request certification of a new public key.

4.7.3: PROCESSING CERTIFICATE RE-KEYING REQUESTS

Digital signatures on subscriber re-key requests shall be validated before electronic re-key requests are processed. Alternatively, subscriber re-key requests may be processed using the same process used for initial certificate issuance.

4.7.4: NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

No stipulation.

4.7.5: CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

For certificates issued by the Halliburton Common Root CA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this CP, no stipulation.

4.7.6: PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

All CA certificates must be published as specified in section 2.1.

This CP makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.7.7: NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No stipulation.

4.8: CERTIFICATE MODIFICATION

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1: CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

A CA operating under this CP may modify a CA or OCSP responder certificate whose characteristics have changed (e.g. assert new policy OID). The new certificate may have the same or a different subject public key.

A CA may perform certificate modification for a subscriber whose characteristics have changed (e.g. name change due to marriage). The new certificate shall have a different subject public key.

4.8.2: WHO MAY REQUEST CERTIFICATE MODIFICATION

Requests for certification of a new public key shall be considered as follows:

Subscribers with a currently valid certificate may request certificate modification. CAs and RAs may request certificate modification on behalf of a subscriber. For device certificates, the human sponsor of the device may request certificate modification.

4.8.3: PROCESSING CERTIFICATE MODIFICATION REQUESTS

If an individual's name changes (e.g. due to marriage), then proof of the name change must be provided to the RA or Enrollment Agent in order for a certificate with the new name to be issued. If an individual's authorizations or privileges change, the RA will verify those authorizations. If authorizations have reduced, the old certificate must be revoked.

Proof of all subject information changes must be provided to the RA or other Enrollment Agent and verified before the modified certificate is issued.

4.8.4: NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

No stipulation.

4.8.5: CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

For certificates issued by the Halliburton Common Root CA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this CP, no stipulation

4.8.6: PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

All CA certificates must be published as specified in section 2.1.

This CP makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.8.7: NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No stipulation.

4.9: CERTIFICATE REVOCATION AND SUSPENSION

CAs operating under this CP shall issue Certificate Revocation Lists (CRLs) covering all unexpired certificates issued under this policy except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

CAs operating under this CP shall make public a description of how to obtain revocation information for the certificates they publish. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

Certificate suspension for CA certificates is not allowed by this CP. However, the use of certificate suspension for subscriber certificates is permitted.

4.9.1: CIRCUMSTANCES FOR REVOCATION

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are—

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Privilege attributes asserted in the subscriber's certificate are reduced.
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2: WHO CAN REQUEST REVOCATION

Within the PKI, a CA may summarily revoke certificates within its domain. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the relevant CPS. A subscriber may request that its own certificate be revoked. Other authorized Halliburton employees may request revocation as described in the relevant CPS.

4.9.3: PROCEDURE FOR REVOCATION REQUEST

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g. digitally or manually signed). The steps involved in the process of requesting a certification revocation must be detailed in the relevant CPS.

Where subscribers use hardware tokens, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise;
- the hardware token does not permit the user to export the signature private key;
- the subscriber surrendered the token to the PKI;
- the token was zeroized or destroyed promptly upon surrender;
- the token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

4.9.4: REVOCATION REQUEST GRACE PERIOD

There is no grace period for revocation under this CP. Subscribers are expected to request revocation of any certificate thought to be compromised immediately to the issuing CA-MA.

4.9.5: TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next full CRL is published, excepting those requests received within two hours of CRL issuance.

4.9.6: REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

No stipulation.

4.9.7: CRL ISSUANCE FREQUENCY

Certificate Revocation Lists (CRLs) shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. Certificate status information shall be published no later than the next scheduled update and certificate overlap is permitted. This will facilitate the local caching of certificate status information for off-line or remote operation.

The Halliburton Common Root CA will issue a full CRL at least once every 26 weeks with an overlap of up to 10 days: the nextUpdate time in the CRL may be no later than 182 days after issuance time (e.g. the thisUpdate time). Other CAs that only issue certificates to CAs and operate off-line (i.e. Policy CAs) must issue a full CRL at least once every 13 weeks with an overlap of up to 10 days: the nextUpdate time in the CRL may be no later than 91 days after issuance time (e.g. the thisUpdate time).

CAs that issue certificates to subscribers and/or operate on-line must issue a full CRL at least once every 7 days with delta CRLs every 12 hours. CAs that issue subscriber certificates under the HalPkiHigh policy must issue a full CRL every 48 hours with delta CRLs every 12 hours. An overlap period for Online CAs of up to 2 days and up to 6 hours is acceptable for full and delta CRLs respectively.

Resigning the previous CRL is permitted in the event of CA failure with a new CRL issued as soon as possible.

4.9.8: MAXIMUM LATENCY FOR CRLS

CRLs for offline CAs and online CAs shall be published within 8 hours and 4 hours of generation respectively and no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

4.9.9: ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

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

4.9.10: ON-LINE REVOCATION CHECKING REQUIREMENTS

If available, relying party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

4.9.11: OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA's approved CPS;
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the issuance and latency requirements for CRLs stated in sections 4.9.7 and 4.9.8.

4.9.12: SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

When a CA certificate is revoked, a CRL must be issued within 24 hours of notification.

No additional stipulation for subscriber certificates.

4.9.13: CIRCUMSTANCES FOR SUSPENSION

For CA certificates, suspension is not permitted.

For subscriber certificates, no stipulation.

4.9.14: WHO CAN REQUEST SUSPENSION

No stipulation for subscriber certificates.

4.9.15: PROCEDURE FOR SUSPENSION REQUEST

No stipulation for subscriber certificates.

4.9.16: LIMITS ON SUSPENSION PERIOD

No stipulation for subscriber certificates.

4.10: CERTIFICATE STATUS SERVICES

No stipulation.

4.10.1: OPERATIONAL CHARACTERISTICS

No stipulation.

4.10.2: SERVICE AVAILABILITY

No stipulation.

4.10.3: OPTIONAL FEATURES

No stipulation.

4.11: END OF SUBSCRIPTION

No stipulation.

4.12: KEY ESCROW AND RECOVERY

4.12.1: KEY ESCROW AND RECOVERY POLICY AND PRACTICES

Under no circumstances shall a subscriber's private key for use in nonrepudiation functions (signature or authentication) be held in trust by a third party. Escrowed keys for other functions shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

4.12.2: SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

CAs that support session key encapsulation and recovery shall identify the document describing the practices in the applicable CPS.

5: FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1: PHYSICAL CONTROLS

CA equipment shall be protected from unauthorized access while the cryptographic modules are installed and activated. The CA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens shall be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to the Halliburton Common Root CA and subordinate CAs.

5.1.1: SITE LOCATION AND CONSTRUCTION

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2: PHYSICAL ACCESS

5.1.2.1: PHYSICAL ACCESS FOR CA EQUIPMENT

At a minimum, the physical access controls for CA equipment, as well as remote workstations used to administer the CAs, shall—

- Ensure that no unauthorized access to the hardware is permitted.
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers.

In addition, for all off-line CAs:

- Require two-person physical access control to both the cryptographic module and computer systems.

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

5.1.2.2: PHYSICAL ACCESS FOR RA EQUIPMENT

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic modules is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.2.3: PHYSICAL ACCESS FOR CSS EQUIPMENT

Physical access control requirements for CSS equipment shall meet the CA physical access requirements specified in 5.1.2.1.

5.1.3: POWER AND AIR CONDITIONING

The directories (containing CA certificates and CRLs) shall be provided with uninterrupted power/generator sufficient for a minimum of 24 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4: WATER EXPOSURES

CA equipment shall be installed such that it is not in danger of exposure to water (e.g. on tables or elevated floors).

Potential water damage from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

5.1.5: FIRE PREVENTION AND PROTECTION

No stipulation.

5.1.6: MEDIA STORAGE

Media shall be stored so as to protect them from accidental damage (e.g. water, fire, or electromagnetic) and unauthorized physical access.

5.1.7: WASTE DISPOSAL

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.1.8: OFF-SITE BACKUP

Full system backups sufficient to recover from system failure shall be made on a periodic schedule and described in a CA's CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location (separate from CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

For offline CAs, the full system backup shall be performed each time the system is turned on or once a week, whichever is less frequent.

Requirements for CA private key backup are specified in section 6.2.4.1

5.2: PROCEDURAL CONTROLS

5.2.1: TRUSTED ROLES

A Trusted Role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensure that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The primary Trusted Roles defined in this policy are Administrator, Certificate Manager, Security Auditor, and Backup Operator. Individual personnel shall be specifically designated to assume these four roles as defined below. These four roles are employed at the CA, RA, and CSS locations as appropriate.

Additional role creation for the purpose of additional role separation is permitted (e.g. New role of Template Manager to configure certificate templates with Administrator limited to publishing the templates).

5.2.1.1: ADMINISTRATOR

The Administrator role shall be responsible for:

- Installation, configuration, and maintenance of the CA and CSS (where applicable);
- Establishing and maintaining CA and CSS system accounts;
- Configuring certificate profiles or templates;
- Configuring CA, RA, and CSS audit parameters;
- Configuring CSS response profiles; and
- Generating and backing up CA and CSS keys.

Administrators do not issue certificates to subscribers.

5.2.1.2: CERTIFICATE MANAGER (CERTIFICATE OFFICER)

The Certificate Manager role shall be responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates; and
- Requesting, approving and executing the revocation of certificates.

5.2.1.3: SECURITY AUDITOR

The Security Auditor role shall be responsible for:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA, associated RAs, and CSS (where applicable) are operating in accordance with its CPS.

5.2.1.4: BACKUP OPERATOR

The Backup Operator role shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.2: NUMBER OF PERSONS REQUIRED PER TASK

Two or more persons are required for the following tasks:

- CA key generation;
- CA signing key activation;
- CA private key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants must serve in a Trusted Role as defined in section 5.2.1. Multiparty control shall not be achieved using personnel that serve in the Security Auditor Trust Role.

5.2.3: IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4: ROLES REQUIRING SEPARATION OF DUTIES

Individuals may only assume one of the Certificate Manager, Administrator, or Security Auditor roles, but any individual may assume the Backup Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both the Administrator and the Certificate Manager roles, assume the Administrator and the Security Auditor roles, or assume both the Security Auditor and the Certificate Manager roles. For CAs that issue at HalPkiHigh, the Security Auditor may not assume any other role. No individual shall have more than one identity.

5.3: PERSONNEL CONTROLS

5.3.1. QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

All persons filling Trusted Roles shall be selected on the basis of loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the CPS.

5.3.2: BACKGROUND CHECK PROCEDURES

CA personnel shall, at a minimum, pass a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence; and
- Law Enforcement.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified.

5.3.3: TRAINING REQUIREMENTS

All personnel performing duties with respect to the operation of the CA or RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA (or RA) security principles and mechanisms;
- All PKI software versions in use on the CA (or RA) system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of this CP.

5.3.4: RETRAINING FREQUENCY AND REQUIREMENTS

All individuals responsible for PKI roles shall be made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5: JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6: SANCTIONS FOR UNAUTHORIZED ACTIONS

The CA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its RAs that are not authorized in this CP, CPSs, or other published procedures.

5.3.7: INDEPENDENT CONTRACTOR REQUIREMENTS

Contractors may not assume Trusted Roles: all Trusted Roles must be Halliburton employees.

PKI vendors who provide any services shall establish procedures to ensure that any subcontractors perform in accordance with this CP and the CPS.

5.3.8: DOCUMENTATION SUPPLIED TO PERSONNEL

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4: AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with section 5.5.2.

5.4.1: TYPES OF EVENTS RECORDED

All Security auditing capabilities of CA operating system and CA applications shall be enabled during installation. Details of auditable events must be identified within the CPS for each CA.

5.4.2: FREQUENCY OF PROCESSING LOG

For Offline CAs, review of the audit log shall be required at least once each year.

For online CAs that issue certificates under HalPkiHigh, review of the audit log shall be required at least once every three months. For online CAs that do not issue certificates under HalPkiHigh, review of the audit log shall be required at least every six months.

Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA since the last review shall be examined. This amount will be described in the CPS.

All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

5.4.3: RETENTION PERIOD FOR AUDIT LOG

Audit logs shall be retained on-site for at least 6 months in addition to being archived as described in section 5.5. The individual who removed audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key.

5.4.4: PROTECTION OF AUDIT LOG

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. CA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period. Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.

5.4.5: AUDIT LOG BACKUP PROCEDURES

No stipulation.

5.4.6: AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

The audit log collection system may or may not be external to the CA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g. overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operation shall be suspended until the problem has been remedied.

5.4.7: NOTIFICATION OF EVENT-CAUSING SUBJECT

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

5.4.8: VULNERABILITY ASSESSMENTS

The CA will perform routine self-assessments of security controls. This is delegated to the Security Auditor Trusted Role.

5.5: RECORDS ARCHIVAL

5.5.1: TYPES OF EVENTS ARCHIVED

CA archive records shall be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issues by the CA. At a minimum, the following data shall be recorded for archive:

- Certificate Policy
- Certificate Practice Statement
- Contractual obligations and other agreements concerning the operations of the CA

- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of re-key
- Security audit data (in accordance with section 5.4.1)
- Revocation Requests
- Subscriber identity authentication data as per section 3.2.2
- Subscriber agreements
- Documentation of receipt of tokens

5.5.2: RETENTION PERIOD FOR ARCHIVE

Archive records must be kept for a minimum of 5 years and 6 months: this corresponds with the maximum key validity of the online/issuing CAs plus 6 months.

5.5.3: PROTECTION OF ARCHIVE

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA, archived records may be moved to another medium. The contents of the archive shall not be released except in accordance with sections 9.3 and 9.4. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the CA.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Applications required to process the archive data shall be maintained for a period that equals or exceeds the archive requirements for the data.

5.5.4: ARCHIVE BACKUP PROCEDURES

No stipulation.

5.5.5: REQUIREMENTS FOR TIME-STAMPING OF RECORDS

CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6: ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Archive data may be collected in any expedient manner.

5.5.7: PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Procedures, detailing how to create, verify, package, transmit, and store the CA archive information, shall be published in the CPS.

5.6: KEY CHANGEOVER

It is best practice to change a CA's private signing key periodically to minimize the likelihood and impact of the improbable event of CA key compromise. Once a new private signature key has been generated, only the new key will be used to sign CA and subscriber certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

The CA's signing key shall have a validity period as described in section 6.3.2.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. When a CA that distributes self-signed certificates updates its private signature key, the CA may generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are also optional for CAs that do not distribute self-signed certificates.

5.7: COMPROMISE AND DISASTER RECOVERY

5.7.1: INCIDENT AND COMPROMISE HANDLING PROCEDURES

Halliburton IT Security shall be notified if any CA operating under this CP experiences the following:

- suspected or detected compromise of the CA systems;
- suspected or detected compromise of a certificate status server (CSS) if (1) the CSS certificate has a lifetime of more than 72 hours and (2) the CSS certificate cannot be revoked;
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components; or
- any incident preventing the CA from issuing a CRL within prescribed window.

Halliburton IT Security will take appropriate steps to protect the integrity of the Halliburton PKI.

The CA's Management Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.

5.7.2: COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

When computing resources, software, and/or data are corrupted, CAs operating under this CP shall respond as follows:

- Before returning to operation, ensure the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in section 4.9.7.
- If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

The CA-MA shall be notified as soon as possible.

5.7.3: ENTITY (CA) PRIVATE KEY COMPROMISE

In the event of a CA private key compromise, the following operations must be performed.

- Halliburton IT Security shall be immediately informed, as well as any superior or cross-certified CAs and any entities known to be distributing the CA certificate (e.g. in a root store).
- The CA must generate new keys in accordance with section 6.1.1.1.

If the CA distributed the private key in a Trusted Certificate, the CA shall perform the following operations:

- Generate a new Trusted Certificate
- Securely distribute the new Trusted Certificate as specific in section 6.1.4.

Subscriber certificates may be renewed automatically by the CA under the new key pair (see section 4.6), or the CA may require subscribers to repeat the initial certificate application process.

5.7.4: BUSINESS CONTINUITY CAPABILITIES

All CAs operating under this CP shall have operational procedures, recovery procedures and/or a distributed, resilient architecture to ensure that required functionality (e.g. timely CRL publication) is not lost if a single datacenter or site is rendered unusable or significantly degraded.

In the case of a disaster whereby all copies of the CA signature key are destroyed as a result, Halliburton IT Security shall be notified at the earliest feasible time, and Halliburton IT Security shall take whatever action it deems appropriate.

5.8: CA OR RA TERMINATION

When a CA operating under this CP terminates operations before all certificates have expired, the CA signing keys shall be surrendered to Halliburton IT Security. Prior to the CA termination, the CA shall provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of it termination, using an agreed-upon method of communication specified in the CPS.

6: TECHNICAL SECURITY CONTROLS

6.1: KEY PAIR GENERATION AND INSTALLATION

6.1.1: KEY PAIR GENERATION

6.1.1.1: CA KEY PAIR GENERATION

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140-2 validated cryptographic modules. For CAs that issue subscriber certificates the module(s) shall meet or exceed FIPS 140-2 Level 2. CAs issuing end-entity certificates under only the HalPkiDeviceNoTrust policy are exempt from the FIPS 140-2 validated cryptographic modules requirement. Multiparty control is required for CA key pair generation, as specified in section 6.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2: SUBSCRIBER KEY PAIR GENERATION

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. For the HalPkiHardware and HalPkiHigh policies, subscriber key pairs shall be generated in FIPS 140-2 Level 2 hardware cryptographic modules. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

6.1.1.3: CSS KEY PAIR GENERATION

Cryptographic keying material used by CSSs to sign status information shall be generated and stored in FIPS 140-2 validated cryptographic modules.

6.1.2: PRIVATE KEY DELIVERY TO SUBSCRIBER

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a subscriber shall not retain any copy of the key after delivery of the private key to the subscriber.
- The private key(s) must be protected from activation, compromise, or modification during the delivery process.
- The subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

The CA must maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3: PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Where key pairs are generated by the subscriber or RA, the public key and the subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4: CA PUBLIC KEY DELIVERY TO RELYING PARTIES

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in cross-certificates.

Self-signed certificates shall be conveyed to relying parties in a secure fashion. Acceptable methods for self-signed certificate delivery are:

- Loading a self-signed certificate onto tokens delivered to relying parties via secure mechanisms; such as
  - The Trusted Certificate is loaded onto the token during the subscriber's appearance at the RA.
  - The Trusted Certificate is loaded onto the token when the RA generates the subscriber's key pair and loads the private key onto the token, which is then delivered to the subscriber in accordance with section 6.1.2.
- Secure distribution of self-signed certificates through secure out-of-band mechanisms;
- Comparison of the hash of the self-signed certificates against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along the certificate are not acceptable as an authentication mechanism); and
- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

Key Rollover certificates are signed with the CA's current private key, so secure distribution is not required.

6.1.5: KEY SIZES

This CP requires the use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this CP shall contain RSA or elliptic curve public keys.

Certificate Type	**Algorithm - Key Size**
Common Root CA	RSA - 4096 bit, SHA-1
Non Common Root CAs – Signature Keys	RSA – 2048 or 4096 bits, Elliptic Curve - 256 or 384 bit
Non Common Root CAs – Hash	For RSA: SHA-1 or SHA-256, For Elliptic: SHA-256 or SHA-384 (as appropriate for the key length)
CSSs	Same signature algorithm, key size, and hash algorithm as CA signing relevant CRL
End entity certificates - Devices	RSA - 1024, 2048, or 3072 bits, Elliptic Curve - 256 or 384 bit
End entity certificates - Users	RSA - 2048, or 3072 bits, Elliptic Curve - 256 or 384 bit
TLS – Symmetric Key	3DES or AES
TLS – Signature Key	At least RSA-2048 bit or Elliptic Curve - 224 bit

6.1.6: PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Elliptic Curve public key parameters shall always be selected from the set specified in section 7.1.3.

6.1.7: KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

6.2: PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1: CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Offline CAs shall use a FIPS 140-2 Level 3 or higher validated hardware cryptographic module. Online CAs, RAs, and CSSs shall use a FIPS 140-2 Level 2 or higher validated hardware cryptographic module.

Subscribers shall use a FIPS 140-2 Level 1 or higher validated cryptographic module for all cryptographic operations for all nonrepudiation, user policies. Subscribers issued certificates under the hardware user policy (HalPkiHardware) or High policy (HalPkiHigh) shall be generate and stored on a FIPS 140-2 Level 2 or higher validated hardware cryptographic module for all private key operations.

6.2.2: PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery shall be under least two-person control.

6.2.3: PRIVATE KEY ESCROW

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.12.1.

6.2.4: PRIVATE KEY BACKUP

6.2.4.1: BACKUP OF CA PRIVATE SIGNATURE KEY

The CA private signature keys shall be backed up under the same multi-person control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA's CPS.

6.2.4.2: BACKUP OF SUBSCRIBER PRIVATE SIGNATURE KEY

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the HalPkiHigh policy shall not be backed up or copied. Subscriber private signature keys whose corresponding public key is contained in a certificate that does not assert HalPkiHigh may be backed up or copied, but must be held in the subscriber's control. Backed up subscriber private signature keys shall not be stored in the plaintext outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.3: BACKUP OF SUBSCRIBER PRIVATE KEY MANAGEMENT KEY

Backed up subscriber private key management keys shall not be stored in plaintext outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.4: BACKUP OF CSS PRIVATE KEY

CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.2.5: PRIVATE KEY ARCHIVAL

CA private signature keys and subscriber private signatures keys shall not be archived. CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys, in accordance with section 5.5.

6.2.6: PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in section 6.2.4.1. At no time shall the CA private key exist in plaintext outside the cryptographic module.

All other keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protect from disclosure.

6.2.7: PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

No stipulation beyond that specified in FIPS 140-2.

6.2.8: METHOD OF ACTIVATING PRIVATE KEY

For certificates issued under HalPkiLow, HalPkiSoftware, HalPkiHardware, and HalPkiHigh, the subscriber must be authenticated to the cryptographic token (hardware or software) before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs, or biometrics. Entry of activation data shall be protected from disclosure (i.e. the data should not be displayed while it is entered) and must not be automated (i.e. scripted).

6.2.9: METHOD OF DEACTIVATING PRIVATE KEY

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated (e.g. via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS). CA cryptographic modules shall be removed and stored in a secure container when not in use unless the CA hardware itself is secured within a secure container.

6.2.10: METHOD OF DESTROYING PRIVATE KEY

Individuals in Trusted Roles shall destroy CA, RA, and CSS private signature keys when they are no longer needed. Subscribers shall either surrender their cryptographic module to the CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of hardware is not required.

To ensure future access to encrypted data, subscriber private key management keys should be secured in long-term backups or archived.

6.2.11: CRYPTOGRAPHIC MODULE RATING

See section 6.2.1.

6.3: OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1: PUBLIC KEY ARCHIVAL

The public key is archived as part of the certificate archival.

6.3.2: CERTIFICATE OPERATIONAL PERIODS AND KEY USAGE PERIODS

The usage period for the Halliburton Common Root CA key pair is a maximum of 20 years. For offline, policy (intermediate) CAs, the usage period for a CA key pair is a maximum of 10 years. For online CAs, the usage period for a CA key pair is a maximum of 5 years. The CA private key may be used to sign certificates for at most five years, but may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

For OCSP responders operating under this CP and all other subscriber public keys, the maximum usage period is 18 months. Subscriber signature private keys have the same usage period as their corresponding public keys. The usage period of subscriber key management private keys is not restricted.

6.4: ACTIVATION DATA

6.4.1: ACTIVATION DATA GENERATION AND INSTALLATION

CA activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

RA and subscriber activation data may be user-selected. The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in FIPS 140-2. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2: ACTIVATION DATA PROTECTION

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be:

- memorized;
- biometric in nature; or
- recorded and secured at the level of assurance associated with the cryptographic module, and shall not be stored with the cryptographic module.

6.4.3: OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5: COMPUTER SECURITY CONTROLS

6.5.1: SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

Computer security controls are required to ensure CA/RA operations are performed as specified in this CP. The following computer security functions pertaining to the Halliburton Common Root CA may be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated login
- Provide discretionary access control
- Provide a security audit capability
- Enforce access control for CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security-related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the CA system
- Enforce domain integrity boundaries for security-critical processes.

For other CAs operating under this CP, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts shall include the following functionality:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

For certificate status servers operating under this CP, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions;
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

All communications between any PKI Trusted Role and the CA shall be authenticated and protected from modification.

6.5.2: COMPUTER SECURITY RATING

No stipulation.

6.6: LIFE CYCLE TECHNICAL CONTROLS

6.6.1: SYSTEM DEVELOPMENT CONTROLS

The system development controls for the CA and RA are as follows:

- The CA shall use software that has been designed and developed under a formal, documented develop methodology.
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g. by ensuring the vendor cannot identify the PKI component that will be installed on a particular device).
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs.
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. All applications required to perform the operation of the CA shall be obtained from documented sources. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.

6.6.2: SECURITY MANAGEMENT CONTROLS

The configuration of the CA system, in addition to any modifications and upgrades, shall be document and controlled. There shall be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, shall be verified as being supplied from the vendor, with no modifications, and be the version intended for use. The CA shall periodically verify the integrity of the software as specified in the CPS.

6.6.3: LIFE CYCLE SECURITY CONTROLS

No stipulation.

6.7: NETWORK SECURITY CONTROLS

A firewall or filtering router must protect network access to CA equipment. The firewall or filtering router shall limit services allowed to and from the CA equipment to those required to perform CA functions.

Protection of CA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CA equipment shall be necessary to the functioning of the CA application.

Any boundary control devices (i.e. firewall or filtering router) used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

6.8: TIME-STAMPING

Asserted ties shall be accurate to within three minutes. Electronic or manual procedure may be used to maintain system time. Clock adjustments are auditable events (see section 5.4.1).

7: CERTIFICATE, CRL, AND OCSP PROFILES

7.1: CERTIFICATE PROFILE

7.1.1: VERSION NUMBER(S)

The CA shall issues x.509 v3 certificates (populate version field with integer "2").

7.1.2: CERTIFICATE EXTENSIONS

No stipulation.

7.1.3: ALGORITHM OBJECT IDENTIFIERS

Certificates issued under this CP shall use the following OIDs for signatures:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256withRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
RSA with PSS padding	id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. Certificates issued under this CP must use the SHA-256 hash algorithm when generating RSASSA-PSS signatures. The following OID shall be used to specify the hash in an RSASSA-PSS digital signature:

SHA-256	id-sha256 ::= {joint-iso-itu-t(2) country(16) rganization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates issued under this CP shall use the following OIDs to identify the algorithm associated with the subject key:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

Where the certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34 }

7.1.4: NAME FORMS

The subject field in certificates issued under HalPkiLow, HalPkiSoftware, HalPkiHardware, HalPkiHigh, and HalPkiDevices shall be populated with an X.500 distinguished name as specified in section 3.1.1.

The issuer field of certificates issued under the policies in this document shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1.

7.1.5: NAME CONSTRAINTS

The CAs may assert name constraints in CA certificates.

7.1.6: CERTIFICATE POLICY OBJECT IDENTIFIER

Certificates issued under this CP shall assert at least one of the OIDs identified in section 1.2 in the certificate policies extension, as appropriate.

7.1.7: USAGE OF POLICY CONSTRAINTS ENTENSION

The CAs may assert policy constraints in CA certificates.

7.1.8: POLICY QUALIFIERS SYNTAX AND SEMANTICS

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9: PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

Certificates issued under this CP shall not contain a critical certificate policies extension.

7.2: CRL PROFILE

7.2.1: VERSION NUMBER(S)

The CAs shall issue x.509 Version 2 CRLs.

7.2.2: CRL AND CRL ENTRY EXTENSIONS

No stipulation.

7.3: OCSP PROFILE

Certificate status servers (CSSs) operated under this CP shall sign responses using the algorithms designated for CRL signing.

CSSs shall be able to process SHA-1 hashes when included in the CertID field and the keyHash in the responder field.

7.3.1: VERSION NUMBER(S)

CSSs operated under this CP shall use OCSP version 1.

7.3.2: OCSP EXTENSIONS

Critical OCSP extensions shall not be used.

8: COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs operating under this CP shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced. This specification does not impose a requirement for any particular assessment methodology.

8.1: FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

CAs and RAs operating under this CP shall be subject to a periodic compliance audit at least once per year.

Alternative reviews may be substituted for full compliance audits under exceptional circumstances. The conditions that permit an alternative review are as follows:

1. If no changes to policies, procedures, or operations have occurred during the previous year, an assertion to that effect, signed by the cognizant executive responsible for the CA-MA (Director level or higher), is acceptable in lieu of a full compliance audit.
2. If no significant changes to policies, procedures, or operations have occurred during the previous year, a delta compliance audit is acceptable in lieu of a full compliance audit.

However, a full compliance audit (see section 8.4) must be completed every third year regardless.

Further, Halliburton IT Security has the right to require aperiodic compliance audits of CAs operating under this policy. Halliburton IT Security shall state the reason for any aperiodic compliance audit.

8.2: IDENTITY/QUALIFICATIONS OF ASSESSOR

The Compliance Auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and this CP. In addition to the previous requirements, the Compliance Auditor must be a Certified Information System Auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable mitigation strategies, and industry best practices.

Note that the Compliance Auditor is not the same as the Security Auditor Trusted Role.

8.3: ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The Compliance Auditor either shall be a private firm that is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. To ensure independence and objectivity, the Compliance Auditor may not have served the entity in developing or maintaining the entity's CA Facility or CPS. Halliburton IT Security shall determine whether a Compliance Auditor meets this requirement.

A CA's Management Authority is responsible for identifying and engaging a qualified Compliance Auditor.

8.4: TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current versions of this CP and the CA's CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

Where permitted by section 8.1, CAs operating under this CP may perform a delta compliance audit in lieu of the full compliance audit. A delta compliance audit covers all changes to policies, procedures, or operations that have occurred during the previous year. The following topics must be addressed in a delta compliance audit if no changes have occurred since the last full compliance audit:

1. Personnel controls;
2. Separation of duties;
3. Audit review frequency and scope;
4. Types of events recorded in physical and electronic audit logs;
5. Protection of physical and electronic audit data;
6. Physical security controls; and
7. Backup and archive generation and storage.

8.5: ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the Compliance Auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The Compliance Auditor shall note the discrepancy;
- The Compliance Auditor shall notify the parties identified in section 8.6 of the discrepancy; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to Halliburton IT Security and appropriate CA Management Authority.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, Halliburton IT Security may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate.

8.6: COMMUNICATION OF RESULTS

An audit compliance report shall be provided to the entity responsible for CA operations. The Audit Compliance Report and identification of corrective measures shall be provided to both Halliburton IT Security and, where applicable, the CA-MA within 30 days of completion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9: OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1: CERTIFICATE ISSUANCE OR RENEWAL FEES

No stipulation.

9.1.2: CERTIFICATE ACCESS FEES

Section 2 of this policy requires that CA certificates be publicly available. CAs operating under this policy must not charge additional fees for access to this information.

9.1.3. REVOCATION OR STATUS INFORMATION ACCESS FEES

CAs operating under this CP must not charge additional fees for access to CRLs and OCSP status information.

9.1.4: FEES FOR OTHER SERVICES

No stipulation.

9.1.5: REFUND POLICY

No stipulation.

9.2: FINANCIAL RESPONSIBILITY

This CP contains no limits on the use of certificates issued by CAs under this CP. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1: INSURANCE COVERAGE

No stipulation.

9.2.2: OTHER ASSETS

No stipulation.

9.2.3: INSURANCE OR WARRANTY COVERAGE FOR SUBSCRIBERS

No stipulation.

9.3: CONFIDENTIALITY OF BUSINESS INFORMATION

CA information not requiring protection shall be made publicly available. Public access to organizational information shall be determined by the respective organization.

9.3.1: SCOPE OF CONFIDENTIAL INFORMATION

No stipulation.

9.3.2: INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

No stipulation.

9.3.3: RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

No stipulation.

9.4: PRIVACY OF PERSONAL INFORMATION

9.4.1: PRIVACY PLAN

No stipulation.

9.4.2: INFORMATION TREATED AS PRIVATE

No stipulation.

9.4.3: INFORMATION NOT DEEMED PRIVATE

Information included in certificates is not subject to protections outlined in section 9.4.2.

9.4.4: RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

No stipulation.

9.4.5: NOTICE AND CONSENT TO USE PRIVATE INFORMATION

No stipulation.

9.4.6: DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

No stipulation.

9.4.7: OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

No stipulation.

9.5: INTELLECTUAL PROPERTY RIGHTS

Intellectual property rights held by others must not knowingly be violated.

9.6: REPRESENTATIONS AND WARRANTIES

Halliburton IT Security shall:

- Approve the CPS for each CA that issues certificates under this CP;
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP.
- Revise this CP to maintain the level of assurance and operational practicality;
- Publicly distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs.

The Management Authorities shall:

- Review periodic compliance audits to ensure that RAs and other components under their control are operating in compliance with their approved CPSs; and
- Review name space control procedures to ensure that distinguished names are uniquely assigned within their scope of control.

9.6.1: CA REPRESENTATIONS AND WARRANTIES

CAs operating under this CP shall warrant that their procedures are implemented in accordance with this CP, and any certificate issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this CP.

A CA that issues certificates that assert a policy defined in the document shall conform to the stipulations of this document, including:

- Providing to Halliburton IT Security a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

9.6.2: RA REPRESENTATIONS AND WARRANTIES

An RA that performs registration functions as described in this CP shall comply with the stipulations of this CP, and comply with a CPS approved by Halliburton IT Security for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Ensuring that obligations are imposed on subscribers, in accordance with section 9.6.3, and subscribers are informed of the consequences of not complying with those obligations.

9.6.3: SUBSCRIBER REPRESENTATIONS AND WARRANTIES

A subscriber (or human sponsor for device certificates) shall be required to sign a document containing the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers shall:

- Accurately represent themselves in all communications with the PKI authorities.

- Protect their private key(s) at all times, in accordance with this CP, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

9.6.4: RELYING PARTIES REPRESENTATIONS AND WARRANTIES

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e. certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

9.6.5: REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

None.

9.7: DISCLAIMERS OF WARRANTIES

CAs operating under this CP may not disclaim any responsibilities described in this CP.

9.8: LIMITATIONS OF LIABILITY

Liability is limited to what is contractually agreed upon between Halliburton and any relying third party. Unless otherwise contractually agreed upon, Halliburton has no liability under this CP.

9.9: INDEMNITIES

No stipulation.

9.10: TERM AND TERMINATION

9.10.1 TERM

This CP becomes effective when approved by the Halliburton IT Security Director and published to the Halliburton PKI website. This CP has no specified term.

9.10.2: TERMINATION

Termination of this CP is at the discretion of Halliburton IT Security.

9.10.3: EFFECT OF TERMINATION AND SURVIVAL

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

9.11: INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.12: AMENDMENTS

9.12.1: PROCEDURES FOR AMENDMENT

Halliburton IT Security shall review this CP at least once every year. Corrections, updates, or changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the contact in section 1.5.2; such communications include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2: NOTIFICATION MECHANISM AND PERIOD

No stipulation.

9.12.3: CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

OIDS will be changed if Halliburton IT Security determines that a change in the CP reduces the level of assurance provided.

9.13: DISPUTE RESOLUTION PROVISIONS

Halliburton IT Security shall to facilitate resolution between entities when conflicts arise as a result of the use of certificates under this CP.

9.14: GOVERNING LAW

The construction, validity, performance and effect of certificates issued under this CP for all purposes shall be governed by United States Federal law (statute, case law, or regulation).

9.15: COMPLIANCE WITH APPLICABLE LAW

All CAs operating under this CP are required to comply with applicable law.

9.16: MISCELLANEOUS PROVISIONS

9.16.1. ENTIRE AGREEMENT

No stipulation.

9.16.2: ASSIGNMENT

No stipulation.

9.16.3: SEVERABILITY

Should it be determined that one section of this CP is incorrect or invalid, the other sections of is CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4: ENFORCEMENT (ATTORNEYS' FEE AND WAIVER OF RIGHTS)

No stipulation.

9.16.5 FORCE MAJEURE

No stipulation.

9.17: OTHER PROVISIONS

No stipulation.

10. ACKNOWLEDGEMENTS

This CP was based largely on the ***X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework***.