HYDRANTID ROOT CA
CERTIFICATE POLICY AND
CERTIFICATION PRACTICE STATEMENT

June 9, 2015
Version: 1.0

Important Note about this Document

This document is the Certificate Policy/Certification Practice Statement herein after referred to as the Certificate Policy & Certification Practice Statement (CP/CPS), adopted by Avalanche Cloud Corporation, which is a Delaware Corporation doing business as (DBA) HydrantID ("HydrantID"). This HydrantID CP/CPS contains an overview of the practices and procedures that HydrantID employs for its operation. This document is not intended to create contractual relationships between HydrantID and any other person. Any person seeking to rely on Certificates or participate within the HydrantID PKI must do so pursuant to definitive contractual documentation. This document is intended for use only in connection with HydrantID and its business. This version of the CP/CPS has been approved for use by the HydrantID Policy Management Authority (PMA) and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the PMA and as otherwise set out herein. The date on which this version of the CP/CPS becomes effective is indicated on this CP/CPS. The most recent effective copy of this CP/CPS supersedes all previous versions. No provision is made for different versions of this CP/CPS to remain in effect at the same time.

Contact Information:

Corporate Offices:
HydrantID
Suite 500
222 South Main Street
Salt Lake City, Utah 84101

Mailing Address:
HydrantID
Suite 500
222 South Main Street
Salt Lake City, Utah 84101 USA

Website: www.hydrantid.com
Electronic mail: support@hydrantid.com

Table of Contents

1. INTRODUCTION

Overview

This Certificate Policy/Certification Practice Statement (CP/CPS) sets out the certification processes that HydrantID uses in the generation, issue, use, and management of Certificates and serves to notify Certificate Holders and Relying Parties of their roles and responsibilities concerning Certificates.

HydrantID ensures the integrity of its Public Key Infrastructure (PKI) operational hierarchy by binding Participants to contractual agreements. This CP/CPS is not intended to create a contractual relationship between HydrantID and any Participant in the HydrantID PKI. Any person seeking to rely on Certificates or participate within the HydrantID PKI must do so pursuant to definitive contractual documentation.

HydrantID maintains three production offline root CAs for the signing of digital certificates:
- HydrantID Root CA 1
- HydrantID Root CA 2
- HydrantID Root CA 3

Each of the three HydrantID Root CAs has one or more associated online Issuing CA (ICA).

For the purposes of this document, the three offline Root CAs and the online Issuing CAs are together referred to as the "HydrantID PKI" and are more particularly described in The HydrantID Certificate Profiles document.

The HydrantID Trust Infrastructure is divided into two primary components: Offline CA Services and Online CA Services. The Offline CA Services consist of an isolated (not ever attached to a network) system stored in a safe when not supporting the issuance of subordinate CAs or revocation information. CA keys are protected using a three-party multi-user control scheme enforced with smart cards. The Online CA Services are designed to provide the issuance and management of customer certificates. The software services are housed in a virtual private cloud connected to the public internet. The subordinate CA private keys are maintained in FIPS 140-2 Level 3 compliant Hardware Security Modules (HSM's). Subordinate (or Issuing) CA keys are protected using a multi-factor authentication control scheme enforced with smart cards. The HSMs are housed in dedicated racks and are accessible only via virtual private network connected to the virtual private cloud. No direct connection to the public internet is supported or allowed.

HydrantID SSL Certificates are issued for use with the SSL/TLS protocol to enable secure transactions of data through privacy, authentication, and data integrity. HydrantID Client Certificates are issued to enable digital signing and encryption.

HydrantID issues three forms of Certificates according to the terms of this CP/CPS:

i. Business SSL Certificates are Certificates for which limited authentication and authorization checks are performed on the Certificate Holder and the individuals acting for the Certificate Holder.

ii. Extended Validation SSL Certificates are Certificates issued in compliance with the "Guidelines for the Issuance and Management of Extended Validation Certificates" (EV Guidelines) published by the CA/Browser Forum. The EV Guidelines are intended to provide enhanced assurance of identity of the Certificate Holder by enforcing uniform and detailed validation procedures across all EV-issuing CAs.

iii. Identity certificates used for digital signing and encryption

HydrantID Certificates comply with Internet standards (x509 v.3) as set out in RFC 5280. This CP/CPS follows the IETF PKIX RFC 3647 framework with 9 sections that cover practices and procedures for identifying Certificate applicants; issuing and revoking Certificates; and the security controls related to managing the physical, personnel, technical, and operational components of the CA infrastructure. To preserve the outline specified by RFC 3647, some sections will have the statement "Not applicable" or "No Stipulation."

For Business SSL Certificates HydrantID conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

For EV SSL Certificates HydrantID conforms to the current version of the CA/Browser Forum "Guidelines for the Issuance and Management of Extended Validation Certificates" (EV Guidelines) published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

1.1. Document Name and Identification

This document is the HydrantID Root CA CP/CPS which was adopted by the HydrantID Policy Management Authority (PMA). The Object Identifier (OID) assigned to HydrantID is 1.3.6.1.4.1.44058.

The provisions of this CP/CPS, as amended from time to time, are incorporated by reference into all HydrantID Certificates that are issued on or after the effective date of publication of this CP/CPS. HydrantID shall make amendments to this CP/CPS in accordance with Section 9.10.

1.1.1. Revisions

Author	Date	Version	Comment
HydrantID Policy Management Authority (PMA)	June 1, 2015	1.0	Initial Version

1.1.2. Relevant Dates

No Stipulation

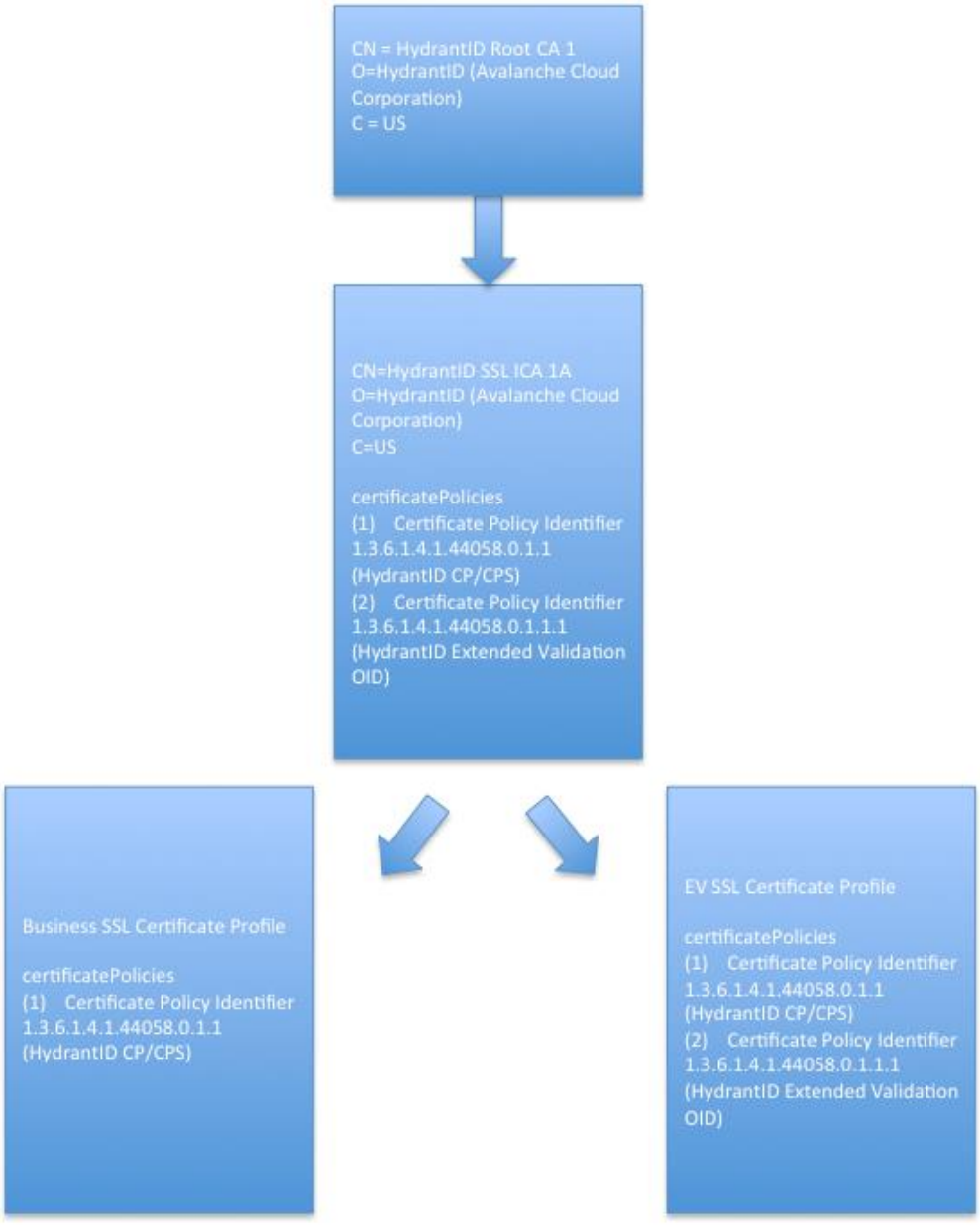
1.2. PKI Participants

Participants (Participants) within the HydrantID PKI include:

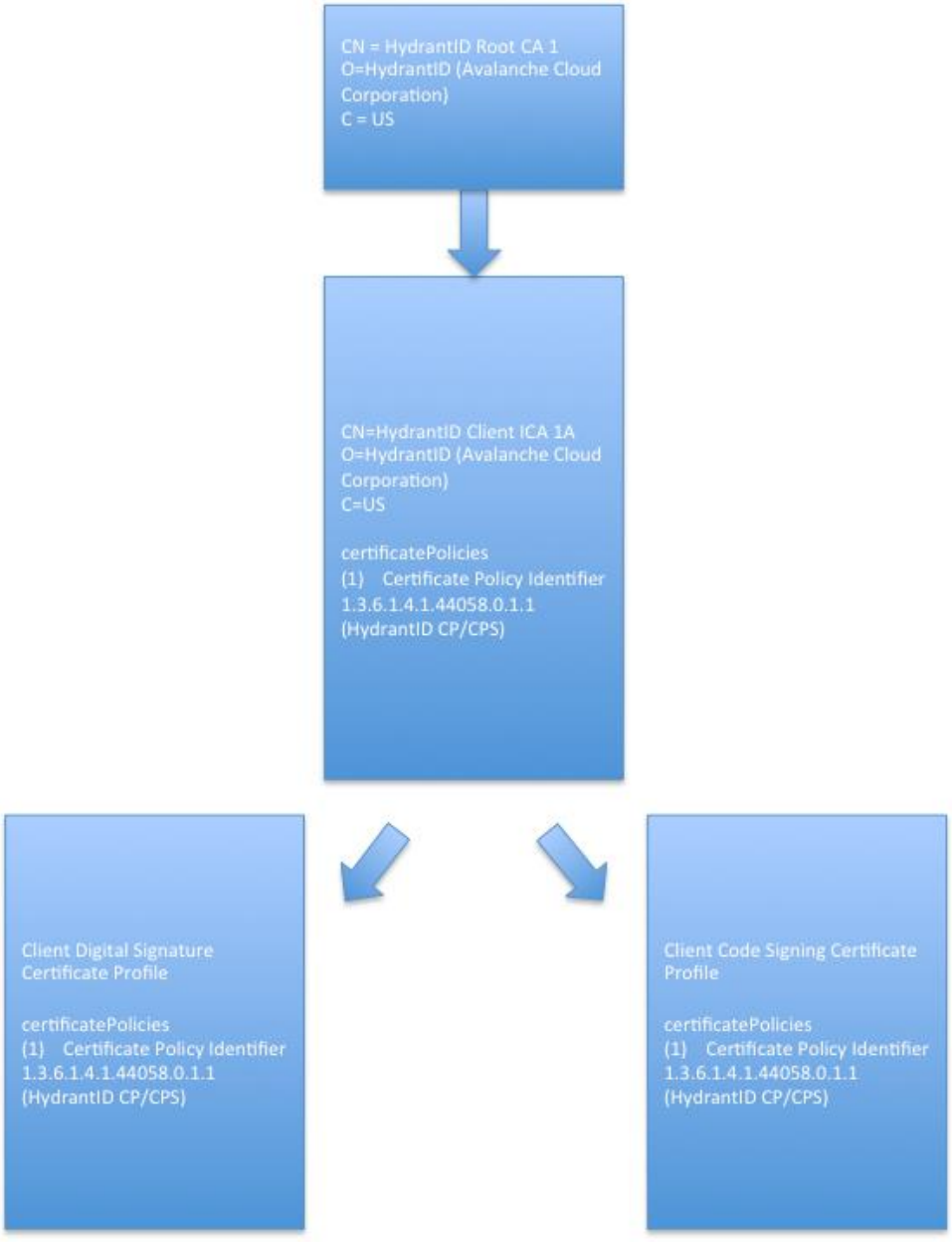
- Certification Authorities (Root and Issuing CAs);
- Registration Authorities ("RA");
- Certificate Holders including Applicants for Certificates prior to Certificate issuance;
- Relying Parties; and
- Other Parties.

The diagrams below illustrates the components of the HydrantID SSL ICA PKI:

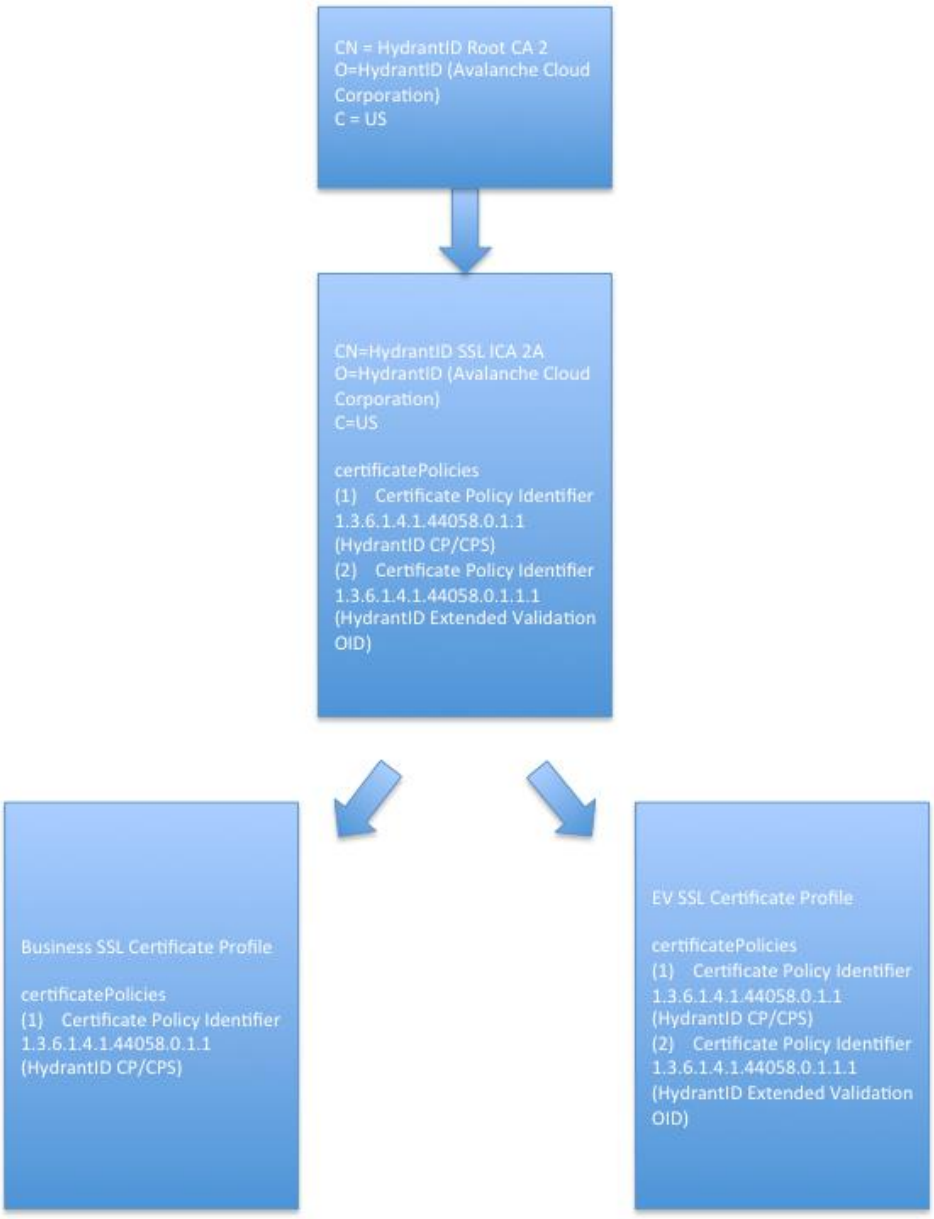
Root CA 1 Hierarchy-SSL



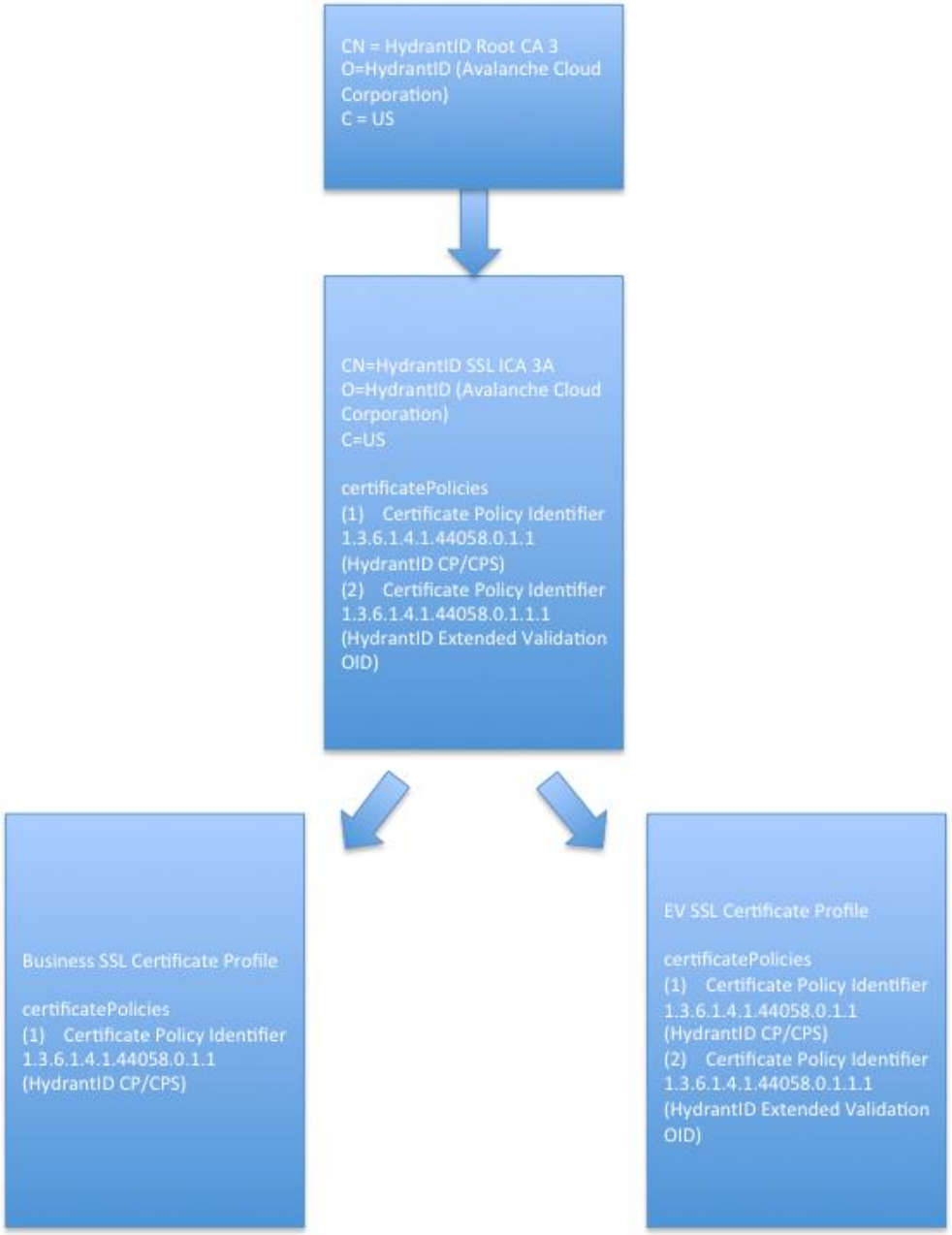
Root CA 1 Hierarchy- Client



Root CA 2 Hierarchy



Root CA 3 Hierarchy



The HydrantID Root CA 1, HydrantID Root CA 2, and HydrantID Root CA 3 are self-signed by Avalanche Cloud Corporation and HydrantID hosts and provides support for the HydrantID PKI. Avalanche Cloud Corporation is doing business as HydrantID.

1.2.1. Certification Authority

The following OIDs are pertinent to this CP/CPS:

NAME	Object Identifier (OID)
HydrantID	1.3.6.1.4.1.44058
HydrantID Extended Validation SSL	1.3.6.1.4.1.44058.0.1.1.1

The HydrantID PKI issues Certificates to Certificate Holders in accordance with this CP/CPS. In its role as a CA, HydrantID performs functions associated with public key operations that include receiving requests; issuing, revoking and renewing a Certificate; and the maintenance, issuance, and publication of CRLs for users within the PKI. In its capacity as a CA, HydrantID will:

- Conform its operations to this CP/CPS (or other relevant business practices);
- Issue and publish Certificates in a timely manner;
- Perform verification of Certificate Holder information in accordance with this CP/CPS;
- Revoke Certificates upon receipt of a valid request from an authorized person or on its own initiative when circumstances warrant; and
- Notify Certificate Holders of the imminent expiry of their Certificates.

1.2.2. Registration Authorities

HydrantID acts as Registration Authority (RA) for Certificates it issues. An RA is an entity that performs verification of Certificate Holder information in accordance with this CP/CPS, and revokes Certificates upon receipt of a valid request from an authorized person.

HydrantID's Enterprise Management Console is a secure web application that facilitates RAs' activities as well as the ongoing management of the SSL Certificates for which they are responsible.

1.2.3. Subscribers (Certificate Holders)

In the context of this CP/CPS, the Certificate Holder is either the Individual to whom an end user Certificate is issued (referred to as a Registrant in the HydrantID Enterprise Management Console) or the Individual responsible for requesting, installing and maintaining the trusted system for which an SSL Certificate has been issued (referred to as a Subscriber in the HydrantID Enterprise Management Console). Prior to verification of identity and issuance of a Certificate, a Certificate Holder is an Applicant for HydrantID services.

Before accepting and using a Certificate, a Certificate Holder must:

(i) generate its own key pair;

(ii) submit an application for a HydrantID Certificate; and

(iii) accept and agree to the terms and conditions of the applicable HydrantID Certificate Holder Agreement. The Certificate Holder is solely responsible for the generation of the key pair to which its HydrantID Certificate relates and for the protection of the Private Key underlying the HydrantID Certificate. A Certificate Holder shall immediately notify HydrantID if any information contained in a HydrantID Certificate changes or becomes false or misleading, or in the event that its private key has been compromised or the Certificate Holder suspects that it has been compromised. A Certificate Holder must immediately stop using a Certificate and delete it from the Certificate Holder's server upon revocation or expiration.

1.2.4. Relying Parties

Relying Parties are Individuals who reasonably rely on HydrantID Certificates in accordance with the terms and conditions of this CP/CPS and all applicable laws and regulations.

Before relying on or using a HydrantID Certificate, Relying Parties are advised to: (i) read this CP/CPS in its entirety; (ii) visit the HydrantID Repository to determine whether the Certificate has expired or been revoked and to find out more information concerning the Certificate; and (iii) make their own judgment as to whether and to what degree to rely upon a Certificate.

1.2.5. Other Parties

No stipulation

1.4 Certificate Usage

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this CP/CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate.

1.4.2. Prohibited Certificate Usage

HydrantID Certificates may not be used and no participation is permitted in the HydrantID PKI (i) in circumstances that breach, contravene, or infringe the rights of others; or (ii) in circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental order; or (iii) in connection with fraud, pornography, obscenity, hate, defamation, harassment, or other activity that is contrary to public policy.

No reliance may be placed on Certificates and Certificates may not be used in circumstances (i) where applicable law or regulation prohibits their use; (ii) in breach of this CP/CPS or the relevant Certificate Holder Agreement; (iii) in any circumstances where the use of Certificates could lead to death, injury, or damage to property; or (iv) as otherwise may be prohibited by the terms of issue.

1.5. Policy Administration

1.5.1. Organization Administering the CP/CPS

This CP/CPS and related agreements and security policy documents referenced within this document are administered by the HydrantID Policy Management Authority (PMA).

Corporate Office and Mailing Address:
HydrantID
222 South Main Street
5th Floor
Salt Lake City, Utah 84101

1.5.2. Contact Person

The Contact Person for the HydrantID CP/CPS is HydrantID's Chief Authentication Officer (CAO):

Mailing Address:
HydrantID
Attn: Chief Authentication Officer
222 South Main Street
5th Floor
Salt Lake City, Utah 84101

1.5.3. Person determining CPS suitability for the policy

The person that determines the suitability of the HydrantID CP/CPS is, HydrantID's Chief Executive Officer (CEO):

Mailing Address:
HydrantID
Attn: Chief Executive Officer
222 South Main Street
5th Floor
Salt Lake City, Utah 84101

1.5.4. CP/CPS Approval Procedures

Approval of this CP/CPS and any amendments hereto is by the HydrantID PMA. Amendments may be made by updating this entire document or by addendum. The HydrantID PMA, at its sole discretion, determines whether changes to this CP/CPS require notice or any change in the OID of a Certificate issued pursuant to this CP/CPS.

1.6. Definitions and Acronyms

Applicant: The Applicant is an entity applying for a Certificate.

Application Software Vendors: Mean those developers of Internet browser software or other software that displays or uses Certificates and distribute Root Certification Authority Certificates embedded in their software, including but not limited to KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, Red Hat, Inc., Adobe, etc.

Authority Letter: The Authority Letter is a signed by a Confirming Person acting for the Applicant for EV Certificates to establish the authority of individuals to act as the Certificate Holder's agents.

Certificate Approver: A Certificate Approver is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to: (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requesters, and (ii) to approve Certificate Requests submitted by other Certificate Requesters.

Certificate Application: Any of several forms completed by Applicant or HydrantID and used to process the request for an EV Certificate, including but not limited to agreements signed by Contract Signers and online forms submitted by Certificate Requesters.

Certificate Holder: Means either the Individual to whom an end user Certificate is issued, referred to as a Registrant in the HydrantID Enterprise Management Console or the Individual responsible for requesting, installing and maintaining the trusted system for which an SSL Certificate has been issued, referred to as a Subscriber in the HydrantID Enterprise Management Console and this CP/CPS document.

Certificate Holder Agreement: The agreement executed between a Certificate Holder and HydrantID relating to the provision of designated Certificate-related services that governs the Certificate Holder's rights and obligations related to the Certificate.

Certificate Requester: A Certificate Requester is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company), and who completes and submits a Certificate Request on behalf of the Applicant.

Confirming Person: A confirming Person is a natural person who must be a senior officer of the Applicant (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) who has express authority to sign the HydrantID Authority Letter on behalf of the Applicant.

Contract Signer: A Contract Signer is a natural person who is employed by the Applicant and who has express authority to sign Certificate Holder Agreements on behalf of the Applicant.

Individual: Any natural person or any limited liability company, partnership, corporation, joint venture, trust, estate, association, or other entity.

Internal Name: An Internal Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

Participants: A Participant is an individual or entity that participates in the HydrantID PKI and includes CAs and their Subsidiaries and the persons identified in Section 1.2.

Relying Party: The Relying Party is an individual or entity that relies upon the information contained within the Certificate and who has accepted a Relying Party Agreement.

Relying Party Agreement: The Relying Party Agreement is an agreement which must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate or accessing or using the HydrantID Repository.

Repository: The Repository refers to the CRL, OCSP, and other directory services provided by HydrantID containing issued and revoked Certificates.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Validation Specialists: Personnel that perform the information verification duties specified by this document in accordance with the requirements of the CA/B Forum.

Acronyms

CA	Certificate Authority or Certification Authority
CP/CPS	Certificate Policy & Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request

ECDSA	Elliptic Curve Digital Signature Algorithm
EV	Extended Validation
FIPS	Federal Information Processing Standard
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
PMA	HydrantID Policy Management Authority
RA	Registration Authority
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The HydrantID Repository serves as the primary repository for revocation data on issued Certificates. However, copies of HydrantID directories may be published at such other locations as required for efficient operation of the HydrantID PKI. The HydrantID Repository resides online at https://www.hydrantid.com/support/repository

2.2. Publication of Certificate Information

HydrantID operates and maintains its Repository with resources sufficient to provide a commercially reasonable response time for the number of queries generated by all of the Certificates issued by its CAs.

HydrantID publishes Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) resources to allow Relying Parties to determine the validity of a HydrantID Certificate. Each CRL contains entries for all revoked un-expired Certificates issued. HydrantID maintains revocation entries on its CRLs, or makes Certificate status information available via OCSP, until after the expiration date of the revoked Certificate.

2.3. Time or Frequency of Publication

HydrantID issues a new CRL at least every twelve (12) hours and prior to the expiration of the current CRL. HydrantID also provides an OCSP resource that is updated at least every twelve (12) hours. Certificate information is published promptly following generation and issue, and within 20 minutes of revocation.

2.4. Access Controls on Repositories

Participants (including Certificate Holders and Relying Parties) may access the HydrantID Repository directly. Only HydrantID personnel authorized by the HydrantID PMA have access to update the repository contents.

3. IDENTIFICATION AND AUTHENTICATION

The identification and authentication procedures used by HydrantID depend on the class of Certificate being issued. See the HydrantID Certificate Profiles document for the relevant verification requirements.

3.1. Naming

3.1.1. Types Of Names

All Certificate Holders require a distinguished name that is in compliance with the ITU X.500 standard for Distinguished Names (DN). SSL Certificates are issued using the Fully Qualified Domain Name (FQDN) name of the server, service, or application that has been confirmed with the Certificate Holder. The Baseline Requirements contain provisions relating to Certificates containing Internal Server Names or Reserved IP Addresses. As of the Effective Date of the Baseline Requirements, the use of such Certificates is deprecated by the CA / Browser Forum and that the practice will be prohibited effective October 31, 2015, HydrantID will revoke any unexpired Certificate whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name. Wildcard SSL Certificates have a wildcard asterisk character for the server name in the Subject field. Wildcard EV Certificates may not be issued under the EV Guidelines. The FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field and the Subject Alternative Name extension.

3.1.2. Need for Names to be Meaningful

Distinguished names must be meaningful, unambiguous, and unique. HydrantID ensures that the Organization (O) and Organizational Unit (OU) attributes in the Subject field accurately identify the legal entity that is the subject of

the Certificate. Similarly, HydrantID uses non-ambiguous designations in the Issuer field to identify itself as the Issuer of a Certificate.

3.1.3. Anonymity or Pseudonymity of Certificate Holders

HydrantID does not issue anonymous or pseudonymous Certificates.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates shall be interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references. In addition, see the Certificate Profiles detailed in Appendix B.

3.1.5. Uniqueness of Names

Name uniqueness for SSL Certificates is ensured through the use of the Common Name attribute of the Subject Field, which contains the authenticated domain name or IP Address, which is controlled under the auspices of the Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6. Recognition, Authentication, and Role of Trademarks

Certificate Holders shall solely be responsible for the legality of the information they present for use in Certificates issued under this CP/CPS in any jurisdiction in which such content may be used or viewed. Certificate Holders represent and warrant that when submitting Certificate Requests to HydrantID and using a domain and distinguished name (and all other Certificate Application information) they do not interfere with or infringe upon the rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, or to confuse or mislead any person, whether natural or corporate. Certificate Holders shall defend, indemnify, and hold HydrantID harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions against HydrantID.

3.2. Initial Identity Validation

3.2.1. Method To Prove Possession Of Private Key

The Applicant must submit a digitally signed PKCS#10 Certificate Signing Request (CSR) to establish that it holds the private key corresponding to the public key to be included in a Certificate. HydrantID parses the PKCS#10 CSR submitted by the Applicant in a secure manner and verifies that the Applicant's digital signature on the PKCS#10 was created by the private key corresponding to the public key in the PKCS#10 CSR. If any doubt exists, HydrantID will not perform certification of the key.

3.2.2. Authentication of Organization Identity

Authentication of Organization identity is conducted in compliance with this CP/CPS and the Certificate Profiles described in the HydrantID Certificate Profiles document.

3.2.3. Authentication of Individual Identity

Where applicable, authentication of Individual identity is conducted in compliance with this CP/CPS and the Certificate Profiles described detailed in the HydrantID Certificate Profiles document.

3.2.4. Non-Verified Certificate Holder Information

HydrantID does not verify information contained in the Organization Unit (OU) field in Certificates. Other information may be designated as non-verified in specific Certificate Profiles.

3.2.5. Validation of Authority

Validation of authority is conducted in compliance with this CP/CPS and the Certificate Profiles detailed in the HydrantID Certificate Profiles document.

For Certificates issued at the request of a Certificate Holder's Agent, both the Agent and the Certificate Holder shall jointly and severally indemnify and hold harmless HydrantID, and its parent companies, subsidiaries, directors, officers, and employees. The Certificate Holder shall control and be responsible for the data that an Agent of the Certificate Holder supplies to HydrantID. The Certificate Holder must promptly notify HydrantID of any misrepresentations and omissions made by an Agent of the Certificate Holder.

3.2.6. Criteria for interoperation
To be determined

3.3. Identification and Authentication for Re-Key Requests
3.3.1. Identification and Authentication for Routine Re-key
Identification and Authentication procedures are the same for re-key as for a new application. Key pairs must always expire at the same time as the associated Certificate.

3.3.2. Identification and Authentication For Re-Key After Revocation
After revocation, a Certificate Holder must submit a new application.

3.4. Identification and Authentication for Revocation Requests
See Section 4.9 for information about Certificate Revocation procedures.

4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1. Certificate Application
The process to apply for HydrantID Certificates varies by Certificate Policy and is described in the HydrantID Certificate Profiles document.

4.2. Certificate Application Processing
4.2.1. Performing Identification And Authentication Functions
During application processing, HydrantID Validation Specialists employ controls to validate the identity of the Certificate Holder and other information featured in the Certificate Application to ensure compliance with this CP/CPS. HydrantID trusted personnel check DNS registration information. If a CAA record is encountered as part of the DNS record and HydrantID is not listed as an approved issuer, then HydrantID will contact the applicant to verify authorization to issue the certificate.

4.2.2. Approval or Rejection of Certificate Applications
From time to time, HydrantID may modify the requirements related to application information requested, based on HydrantID requirements, business context of the usage of Certificates, or as may be required by law, changes to the EV Guidelines or changes to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

HydrantID, in its sole discretion, may refuse to accept an application for a Certificate or for the renewal of a Certificate, and may refuse to issue a Certificate, without incurring any liability for loss or damages arising out of such refusal. HydrantID reserves the right not to disclose reasons for such a refusal. Applicants whose applications have been rejected may subsequently re-apply.

4.2.3. Time to Process Certificate Applications
HydrantID makes commercially reasonable efforts to confirm Certificate Application information and issue a Certificate within a commercially reasonable time frame, which is dependent on the Applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, HydrantID aims to confirm submitted application data and to complete the validation process and issue or reject a Certificate Application commercially reasonable timeframe.

From time to time, events outside of the control of HydrantID may delay the issuance process. However, HydrantID will make every reasonable effort to meet its issuance times and to make Applicants aware of any factors that may affect issuance times in a timely manner.

4.3. Certificate Issuance
4.3.1. CA Actions During Certificate Issuance
Certificate issuance is governed by the practices described in and any requirements imposed by this CP/CPS.

4.3.1.1. HydrantID Root Certification Authority
The HydrantID Root CA Certificates have been self-generated and self-signed.

4.3.1.2. HydrantID Issuing Certification Authority Certificates
Upon accepting the terms and conditions of the HydrantID Issuing CA Agreement by the Issuing CA, successful completion of the Issuing CA application process as prescribed by HydrantID and final approval of the application by the HydrantID Root Certification Authority, the HydrantID Root Certification Authority issues the Issuing CA Digital Certificate to the relevant Issuing CA.

4.3.2. Notification of Certificate Issuance

Certificates are delivered to the Certificate Requester designated in the Certificate Application.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The Certificate Requester is responsible for installing the issued Certificate on the Certificate Holder's computer or cryptographic module according to the Certificate Holder's system specifications. A Certificate Holder is deemed to have accepted a Certificate when:

- The Certificate Holder downloads, installs, or otherwise takes delivery of the Certificate; or
- 30 days pass since issuance of the Certificate.

BY ACCEPTING A CERTIFICATE, THE CERTIFICATE HOLDER ACKNOWLEDGES THAT THEY AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS CP/CPS AND THE APPLICABLE CERTIFICATE HOLDER AGREEMENT. BY ACCEPTING A CERTIFICATE, THE CERTIFICATE HOLDER ASSUMES A DUTY TO RETAIN CONTROL OF THE CERTIFICATE'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE REASONABLE PRECAUTIONS TO PREVENT ITS LOSS, EXCLUSION, MODIFICATION OR UNAUTHORIZED USE.

4.4.2. Publication of the Certificate by the CA

All User Encryption Certificates issued within the HydrantID PKI are made available in public repositories, except in cases where the Certificate Holder has requested that the Certificate not be published.

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

Some certificate types may be published to additional repositories to support initiatives, such as Certificate Transparency.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key And Certificate Usage

Certificate Holders shall protect their private keys from access by unauthorized personnel or other third parties. Certificate Holders shall use private keys only in accordance with the usages specified in the key usage field extension.

4.5.2. Relying Party Public Key and Certificate Usage

A Party seeking to rely on a Certificate issued within the HydrantID PKI agrees to and accepts the Relying Party Agreement by querying the existence or validity of, or by seeking to place or by placing reliance upon, on a Certificate.

HydrantID assumes that all user software will be compliant with X.509, the SSL/TLS protocol, and other applicable standards that enforce the requirements and requirements set forth in this CP/CPS. HydrantID does not warrant that any third party's software will support or enforce such controls or requirements, and all Relying Parties are advised to seek appropriate technical or legal advice.

Parties relying on a Certificate must adhere to the SSL/TLS protocol and verify a digital signature at all times by checking the validity of the associated Certificate against the relevant CRL or OCSP resource provided by HydrantID. Relying on an unverifiable digital signature or SSL/TLS session may result in risks that the Relying Party assumes in whole and which HydrantID does not assume in any way.

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Certificate for any given purpose and that the use is not prohibited by this CP/CPS;
- That the Certificate is being used in accordance with its key usage field extensions specified in this CP/CPS and contained in the Certificate; and
- That the Certificate is valid at the time of reliance by reference to the HydrantID CRL or OCSP and the Certificate has not been revoked.

Warranties are only valid if the steps detailed above have been carried out.

4.6. Certificate Renewal

Renewal of a Certificate means reissuance of the Certificate using the same key pair. HydrantID does not support Renewal; key pairs must always expire at the same time as the associated Certificate. HydrantID makes reasonable efforts to notify Certificate Holders of the imminent expiration of a Certificate. Identification and Authentication procedures are the same for replacement Certificates as for a new application.

4.6.1. Circumstance for certificate renewal

No stipulation

4.6.2. Who may request renewal

No stipulation

4.6.3. Processing certificate renewal requests

No stipulation

4.6.4. Notification of new certificate issuance to subscriber

No stipulation

4.6.5. Conduct constituting acceptance of a renewal certificate

No stipulation

4.6.6. Publication of the renewal certificate by the CA

No stipulation

4.6.7. Notification of certificate issuance by the CA to other entities

No stipulation

4.7. Certificate Re-Key

Re-keying a Certificate means to request a new Certificate with the same contents except for a new key pair. Identification and Authentication procedures are the same for re-key as for a new application.

4.7.1. Circumstance for certificate re-key

No stipulation

4.7.2. Who may request certification of a new public key

No stipulation

4.7.3. Processing certificate re-keying requests

No stipulation

4.7.4. Notification of new certificate issuance to subscriber

No stipulation

4.7.5. Conduct constituting acceptance of a re-keyed certificate

No stipulation

4.7.6. Publication of the re-keyed certificate by the CA

No stipulation

4.7.7. Notification of certificate issuance by the CA to other entities

No stipulation

4.8. Certificate Modification

HydrantID may reissue or replace a valid Certificate when the Certificate Holder's common name, organization name, device name, or geographic location changes. Modified information must undergo the same Identification and Authentication procedures as for a new Certificate.

4.8.1. Circumstance for certificate modification

No stipulation

4.8.2. Who may request certificate modification
No stipulation

4.8.3. Processing certificate modification requests
No stipulation

4.8.4. Notification of new certificate issuance to subscriber
No stipulation

4.8.5. Conduct constituting acceptance of modified certificate
No stipulation

4.8.6. Publication of the modified certificate by the CA
No stipulation

4.8.7. Notification of certificate issuance by the CA to other entities
No stipulation

4.9. Certificate Revocation and Suspension
4.9.1. Circumstances for Revocation
Revocation of a Certificate is to permanently end the operational period of the Certificate prior to reaching the end of its stated validity period. HydrantID may revoke any Certificate at its sole discretion or based on information confirmed in a Certificate Problem Report. HydrantID will revoke a Certificate if:

- HydrantID determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Certificate Holder requests in writing the revocation of their Certificate;
- The Certificate Holder indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;
- HydrantID obtains reasonable evidence that there has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key corresponding to the Public Key within the Certificate, or that the Certificate has otherwise been misused;
- HydrantID receives notice or otherwise becomes aware that a Certificate Holder has breached a material obligation under the Certificate Holder Agreement or other contractual obligations;
- HydrantID receives a lawful and binding order from a government or regulatory body to revoke the Certificate;
- HydrantID is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- HydrantID is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- HydrantID is made aware of a material change in the information contained in the Certificate;
- HydrantID determines, in its sole discretion, that the Certificate was not issued in accordance with the terms and conditions of the EV Guidelines or HydrantID' CP/CPS;
- HydrantID receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the Certificate Holder that is contained within the Certificate;
- The Certificate Holder fails or refuses to comply, or to promptly correct inaccurate, false or misleading information after being made aware of such inaccuracy, misrepresentation or falsity;
- HydrantID determines, in its sole discretion, that the Private Key corresponding to the Certificate was used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, phishing, or other content, or that is harmful, malicious, hostile or downloaded onto a user's system without their consent;
- If HydrantID receives notice or otherwise becomes aware that a Certificate Holder has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination;
- Either the Certificate Holder's or HydrantID's obligations under this CP/CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- a HydrantID CA Private Key used to issue that Certificate has been compromised;
- Revocation is required by the HydrantID CP/CPS

- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).
- HydrantID's right to issue and manage Certificates under the EV Guidelines or the Baseline Requirements expires or is revoked or terminated (unless arrangements have been made to continue maintaining the CRL/OCSP Repository); or
- HydrantID ceases operations for any reason and has not arranged for another suitable CA to provide revocation support for the Certificate.

4.9.2. Who Can Request Revocation

HydrantID may revoke any Certificate issued within the HydrantID PKI at its sole discretion. The Certificate Holder and its appropriately authorized representatives can request revocation of a Certificate. HydrantID may, if necessary, also confirm the revocation request by contact with additional, authorized representatives of the Certificate Holder.

Parties who are not the Certificate Holder (such as Relying Parties, Application Software Vendors, and other third parties) may file a Certificate Problem Report to initiate a Certificate revocation request. Problem reports may include complaints; suspected private key compromise or Certificate misuse; or other types of fraud, compromise, misuse, or inappropriate conduct related to the Certificate.

4.9.3. Procedure for Revocation Request

HydrantID will revoke a Certificate upon receipt of a valid request from the Certificate Holder, verified through an out-of-band communication.
HydrantID will begin an investigation of all Certificate Problem Reports within twenty-four (24) hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

(i) The nature of the alleged problem;
(ii) Number of Certificate Problem Reports received about a particular Certificate or website;
(iii) The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
(iv) Relevant legislation in force.

HydrantID maintains a continuous 24/7 ability to internally respond to any high priority Certificate Problem Report and will take such action as deemed appropriate based on the nature of such a report. This may include, but not be limited to, the revocation of a Certificate that is the subject of such a complaint.

HydrantID will take commercially reasonable steps to revoke the Digital Certificate within four (4) hours of verifying a valid revocation request.

4.9.4. Revocation Request Grace Period

No grace period is permitted once a revocation request has been verified. HydrantID will revoke Certificates as soon as reasonably practical following verification of a revocation request.

4.9.5. Time within which the CA Must Process the Revocation Request

HydrantID will take commercially reasonable steps to revoke the Digital Certificate within four hours of receipt of a valid revocation request.

4.9.6. Revocation Checking Requirement for Relying Parties

Relying Parties are required to consult the HydrantID Repository of issued and revoked Certificates at all times prior to relying on information featured in a Certificate. Failure to do so negates the ability of the Relying Party to claim that it acted on a Certificate with reasonable reliance.

4.9.7. CRL Issuance Frequency

HydrantID manages and makes publicly available directories of revoked Certificates through the use of CRLs. All CRLs issued by HydrantID adhere to X.509v2 CRL as profiled in RFC 5280.

HydrantID updates and publishes a new CRL of revoked Certificates on a 12-hour basis (or more frequently under special circumstances) and within a commercially-reasonable period of time in the case of a Certificate Revocation. The CRLs for Certificates issued pursuant to this CP/CPS can be accessed via the URLs contained in the Certificate

Profile for that Certificate. The CRL is published and is available 24 hours a day, 7 days a week, and 52 weeks of the year every year

4.9.8. Maximum Latency for CRL
The maximum latency for the CRL is within a commercially-reasonable period of time.

4.9.9. On-Line Revocation/Status Checking Availability
HydrantID provides Online Certificate Status Protocol (OCSP) checking. The URL for the OCSP responder may be found within the Authority Information Access extension of the Certificate. Under normal operating conditions, revocation response times will be less than ten seconds.

4.9.10. On-Line Revocation Checking Requirement
Relying Parties are required to consult the HydrantID Repository of issued and revoked Certificates at all times prior to relying on information featured in a Certificate. Failure to do so negates the ability of the Relying Party to claim that it acted on a Certificate with reasonable reliance.

4.9.11. Other Forms of Revocation Advertisements Available
Not applicable.

4.9.12. Special Requirements for Key Compromise
HydrantID will use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that a CA's private key has been compromised.

4.9.13. Circumstances for Suspension
The HydrantID PKI does not support suspension of Certificates.

4.9.14. Who Can Request Suspension
The HydrantID PKI does not support suspension of Certificates.

4.9.15. Procedure for Suspension Request
The HydrantID PKI does not support suspension of Certificates.

4.9.16. Limits on Suspension Period
The HydrantID PKI does not support suspension of Certificates.

4.10. Certificate Status Services
The Status of Digital Certificates issued within the HydrantID PKI is published in a Certificate Revocation List (location published in the certificate) or is made available via Online Certificate Status Protocol checking (location published in the certificate) where available.

4.11. End of Subscription
A Certificate Holder may terminate its subscription to the HydrantID PKI by allowing a Certificate or applicable agreement to expire without renewal, or by voluntarily revoking a Certificate.

4.12. Key Escrow and Recovery
The HydrantID PKI does not support key escrow or recovery of Certificate Holder private keys.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS
The section of the CP/CPS provides a high level description of the security policy, physical and logical access control mechanisms, service levels, and personnel policies used by HydrantID to provide trustworthy and reliable CA operations.

5.1. Physical Security Controls
5.1.1. Site Location and Construction
HydrantID CA operations are performed from secure commercial datacenters. Each datacenter used is designed production hosting facility that provides physical and environmental protection including fire, water, smoke, temperature, humidity, burglary, and vandalism.

5.1.2. Physical Access
Access to the secure operating area within each datacenter is granted only to security- cleared and authorized personnel, whose movements within the facility are logged and audited. Physical access is controlled by a combination of physical access cards and biometric readers. Dual-access control is required for physical access to all trust infrastructure.

5.1.3. Power and Air-Conditioning
All critical components are connected to multiple uninterrupted power supply (UPS) units to prevent abnormal shutdown in the event of a power failure. Automatic failover to a standby generator is provided.

5.1.4. Water Exposures
Each datacenter provides protection against water exposure.

5.1.5. Fire Prevention and Protection
Each datacenter provides protection against fire with an automatic extinguishing system.

5.1.6. Media Storage
All magnetic media containing HydrantID PKI information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities and are located either within each datacenter area or in a secure off-site storage area.

5.1.7. Waste Disposal
Paper documents and magnetic media containing HydrantID PKI information or confidential information are securely disposed of by:
- in the case of magnetic media: physical damage to or complete destruction of the asset; or the use of an approved utility to wipe or overwrite magnetic media; or
- in the case of printed material, shredding or destruction by an approved service.

5.1.8. Off-Site Backup
An offsite location is used for the storage and retention of backup data. The offsite storage is available to authorized personnel 24 hours per day seven days per week for the purpose of retrieving software and data; and has appropriate levels of physical security in place (i.e. located behind access-controlled doors in areas accessible only by authorized personnel).

5.2. Procedural Controls
Administrative processes are described in detail in the various documents used within and supporting the HydrantID PKI. Administrative procedures related to personnel and procedural requirements, as well as physical and technological security mechanisms, are maintained in accordance with this CP/CPS and other relevant operational documents.

5.2.1. Trusted Roles
In order to ensure that one person acting alone cannot circumvent security, trusted responsibilities are shared by multiple roles and individuals. This is accomplished by creating separate roles and accounts on various components of the CA system, and each role has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles. Oversight may be in the form of a person who is not directly involved in issuing Certificates examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy. This is accomplished by creating separate roles and accounts on the service workstation, each of which has a limited amount of capability. This method allows a system of checks and balances to occur among the various roles.

5.2.2. Number of Persons Required Per Task
At least two people are assigned to each trusted role to ensure adequate support at all times, except verifying and reviewing audit logs. Some roles are assigned to different people to ensure no conflict of interest occurs and to prevent the possibility of accidental or intentional compromise of any component of the PKI, most especially the Root CA and Issuing CA private keys.

CA key pair generation and initialization of each offline Root CA shall require the active participation of at least three trusted individuals in each case. Such sensitive operations also require the active participation and oversight of senior management.

CA key pair generation and initialization of each online Issuing CA shall require the active participation of at least two trusted individuals in each case. Such sensitive operations also require the active participation and oversight of senior management.

5.2.3. Identification and Authentication for Trusted Roles

Persons filling trusted roles undergo an appropriate security screening procedure, designated "Position of Trust". Each individual performing any of the trusted roles shall use a Certificate stored on an approved cryptographic smart card to identify themselves to the Certificate Server and Repository.

5.2.4. Roles Requiring Separation of Duties

Sensitive operations involving roles that are segregated between M of N employees, where M is equal to or greater than two. Roles requiring a separation of duties include:

1. authorization functions, such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. backups, recording, and record keeping functions;
3. audit, internal review, management oversight, or reconciliation functions; and
4. CA/ICA key management or CA administration.

HydrantID designates individuals to the trusted roles defined in Section 5.2.1 above and appoints individuals to only one of the Registration Officer, Administrator, Operator, or Internal Auditor roles. Individuals designated as Registration Officer or Administrator may perform Operator duties. Internal Auditors may not assume any other operational role. HydrantID's system identify and use multi-factor authentication of individuals acting in trusted roles. HydrantID's policies restrict one individual from assuming multiple roles.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, And Clearance Requirements

Background checks are conducted on all individuals selected to take up a trusted role in the HydrantID PKI in accordance with a designated security screening procedure.

For purposes of mitigating the risk that one individual acting alone could compromise the integrity of the HydrantID PKI or any Certificate issued therein, background checks are performed on individuals assigned to trusted roles. HydrantID determines the nature and extent of any background checks in its sole discretion. The foregoing fully stipulates HydrantID's obligations with respect to personnel controls and HydrantID shall have no other duty or responsibility with respect to the foregoing. Without limitation, HydrantID shall not be liable for employee conduct that is outside of their duties and for which HydrantID has no control including, without limitation, acts of espionage, sabotage, criminal conduct, or malicious interference.

5.3.2. Background Check Procedures

Background check procedures include but are not limited to checks and confirmation of:

- Previous employment
- Professional references
- Educational qualifications
- Criminal records
- Credit/financial history and status
- Driver licenses

Where the above checks and confirmations cannot be obtained due to a prohibition or limitation of law or other circumstances, HydrantID will utilize available substitute investigation techniques permitted by law that provide similar information including background checks performed by applicable government agencies.

5.3.3. Training Requirements and Procedures

HydrantID provides its personnel with on-the-job and professional training in order to maintain appropriate and required levels of competency to perform job responsibilities. This includes specific vetting training for Validation Specialists, who may not undertake Certificate validation and issuance until they have passed a suitable examination on knowledge and skills.

5.3.4. Retraining Frequency and Requirements

Validation Specialists engaged in Certificate validation and issuance must maintain adequate skill levels in order to have issuance privilege, consistent with HydrantID's training and performance programs.

5.3.5. Job Rotation Frequency and Sequence
HydrantID provides and maintains a program of job rotation in order to maintain appropriate and required levels of competency across key roles.

5.3.6. Sanctions for Unauthorized Actions
Appropriate disciplinary actions are taken for unauthorized actions.

5.3.7. Independent Contractor Requirements
The HydrantID PKI does not support the use of independent contractors to fulfill trusted roles.

5.3.8. Documentation Supplied To Personnel
HydrantID provides personnel all required training materials needed to perform their job function and their duties under the job rotation program. This includes specific documentation of the validation, issuance, and revocation processes for Certificates.

5.4. Audit Logging Procedures
5.4.1. Types Of Events Recorded
All pertinent events involved in the generation of the Root and Issuing CA key pairs are recorded on videotape. This includes all configuration data used in the process.

Individuals who have access to particular key pairs and passwords are background-checked and the process audited. Key pair access will take the form of PIN-protected cryptographic smart cards. Access to the database will take the form of a user name and password. Access control in certain cases may take the form of one individual having access to the smart card and another individual having access to the corresponding PIN to unlock the smart card. This ensures that a minimum of two people being present to perform certain tasks on HydrantID CAs. The types of data recorded by HydrantID include but are not limited to:

- All data involved in each individual Certificate registration process will be recorded for future reference if needed;
- All data and procedures involved in the certification and distribution of Certificates will be recorded, including records of verification checks;
- All data relevant to the publication of Certificates and CRL and OSCP entries will be recorded;
- All Certificate revocation request details are recorded including reason for revocation;
- Certificate and hardware security lifecycle management;
- Logs recording all HTTP/HTTPS traffic to and from trusted machines are recorded and audited;
- All aspects of the configuration of the backup site are recorded. All procedures involved in the backup process are recorded;
- All data recorded as mentioned in the above sections is backed up. Therefore, there will be two copies of all record/audit material, stored in separate locations to protect against disaster scenarios;
- All aspects of the installation of new or updated software;
- All aspects of hardware updates;
- All aspects of shutdowns and restarts;
- Time and date of log dumps;
- Time and date of transaction archive dumps; and
- Security profile changes

All audit logs will be appropriately time stamped and their integrity protected.

5.4.2. Frequency of Processing and Archiving Audit Logs
Audit logs are verified and consolidated periodically and at least quarterly.

5.4.3. Retention Period for Audit Log
Audit logs are retained as archive records for at least seven (7) years for audit trail files and for key and Certificate information. Audit logs are stored until at least seven (7) years after the HydrantID Root CA ceases operation.

5.4.4. Protection of Audit Log
The relevant audit data collected is regularly analyzed for any attempts to violate the integrity of any element of the HydrantID PKI. Only trusted personnel designated by the HydrantID PMA and auditors may view audit logs in whole. HydrantID decides whether particular audit records need to be viewed by others in specific instances and makes those records available. Consolidated logs are protected from modification and destruction. All audit logs are protected in an encrypted format via a Key and Digital Certificate generated especially for the purpose of protecting the logs.

5.4.5. Audit Log Backup Procedures
Each Issuing CA performs an automatic onsite backup of the audit log. The backup process includes weekly duplication of the audit log copy from the datacenter premises to storage at a secure, offsite location.

5.4.6. Audit Log Accumulation System
The security audit process of each Root CA runs independently of the Root CA software. Security audit processes are invoked at system start up and cease only at system shutdown.

5.4.7. Notification to Event-Causing Subject
Where an event is logged, no notice is required to be given to the Individual, device, or application that caused the event.

5.4.8. Vulnerability Assessment
Both baseline and ongoing threat and risk vulnerability assessments are conducted on all parts of the HydrantID PKI environment, including the equipment, physical location, records, data, software, personnel, administrative processes, communications, and each Root CA. Vulnerability assessment procedures intend to identify HydrantID PKI threats and vulnerabilities, and determine a risk value based upon existing safeguards and control practices. Management can then make informed choices on determining how to best provide a secure environment with risk reduced to an acceptable level at an acceptable cost to management, clients, and shareholders. Vulnerability assessments are conducted at least quarterly and penetration and risk assessments are conducted at least annually.

5.5. Records Archival
5.5.1. Types Of Records Archived
HydrantID archives and makes available upon authorized request documentation subject to the HydrantID Document Access Policy. For each Certificate, the records will address creation, issuance, use, revocation, expiration, and renewal activities. These records will include all relevant evidence in the Root CA's possession including:
- Audit logs;
- Certificate Requests and all related actions;
- Evidence produced in verification of Applicant details;
- Contents of issued Certificates;
- Evidence of Certificate acceptance and signed (electronically or otherwise) Certificate Holder Agreements;
- Certificate renewal requests and all related actions;
- Revocation requests and all related actions;
- CRL lists posted; and
- Audit Opinions as discussed in this HydrantID CP/CPS.

5.5.2. Retention Period for Archive
HydrantID Root CA archives will be retained for a period of at least seven (7) years after the expiration of the relevant certificate.

5.5.3. Protection of Archive
Archives shall be retained and protected against modification or destruction.

5.5.4. Archive Backup Procedures
Adequate backup procedures will be in place so that in the event of the loss or destruction of the primary archives a complete set of backup copies will be readily available.

5.5.5. Requirements for Time-Stamping Of Records
HydrantID supports non-cryptographic time stamping of all of its CA records. All events that are recorded within the HydrantID CA include the date and time of when the event took place. This date and time are based on the system time on which the CA program is operating. HydrantID uses procedures to review and ensure that all systems operating within the HydrantID PKI rely on a trusted time source.

5.5.6. Archive Collection System
The HydrantID Archive Collection System is internal.

5.5.7. Procedures to Obtain and Verify Archive Information
Only authorized Root CA officers and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. HydrantID may decide to release records of individual

transactions upon request of any of the entities involved in the transaction or their authorized representatives. A reasonable handling fee per record (subject to a minimum fee) may be assessed to cover the cost of record retrieval.

5.6. Key Changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA private key's lifetime, HydrantID ceases using its expiring CA private key to sign Certificates (well in advance of expiration) and uses the old private key only to sign CRLs associated with that key. A new CA signing key pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active.

5.7. Key Compromise and Disaster Recovery

HydrantID has a Disaster Recovery Plan in place. The purpose of this plan is to restore core business operations as quickly as practicable when systems and/or operations have been significantly and adversely impacted by fire, strikes, or other crisis events.

HydrantID has Business Continuity procedures in place that provide for the continuation of Certificate revocation services in the event of an unexpected emergency. HydrantID regards its Disaster Recovery and Business Continuity plan as proprietary and it contains sensitive confidential information. Accordingly, it is not made generally available.

HydrantID has in place an appropriate key compromise plan detailing its activities in the event of a compromise of a Root CA private key. This plan includes procedures for:

- Revoking all Certificates signed with that Root CA's private key;
- Promptly notifying all Certificate Holders with Certificates issued by that Root CA; and
- Generating a new key pair and signing a new CA Certificate.

5.7.1. Incident and Compromise Handling Procedures

The HydrantID Business Continuity Plan is strictly confidential and provides for:

- Incident and compromise handling procedures;
- Computing resources, software, and/or corrupted data handling procedures;
- Entity private key compromise procedures; and
- Entity public key revocation procedures; and
- Business continuity capabilities and procedures after a disaster.

5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

5.7.3. Entity Private Key Compromise Procedures

5.7.4. Business Continuity Capabilities after a Disaster

5.8. CA and/or RA Termination

In case of termination of CA operations, HydrantID will provide timely notice and transfer of responsibilities to succeeding entities. Before terminating its own CA activities, HydrantID will where possible take the following steps:

- Give timely notice of revocation to each affected Certificate Holder.
- Revoke all Certificates that are still un-revoked or un-expired at the end of the notice period without seeking Certificate Holder's consent.
- Make reasonable arrangements to preserve its records according to this CP/CPS.
- Reserve its right to provide succession arrangements for the re-issuance of Certificates by a successor CA that has all relevant permissions to do so and complies with all necessary standards.
- Notify relevant government and accreditation bodies under applicable laws and related regulations or standards.

Upon termination of a CA, HydrantID personnel shall destroy the CA private key by deleting, overwriting, or physical destruction.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

CA private keys are generated in a physically secure environment within cryptographic modules that are validated to FIPS 140-2 Level-3. CA Certificate signing keys are only used within this secure environment. Access to the modules within the HydrantID environment, including the private keys, is restricted by the use of token/smart cards and

associated pass phrases. These smartcards and pass phrases are allocated among multiple trusted roles. Such allocation ensures that no one member of the team holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

6.1.2. Private Key Delivery to Subscriber

Certificate Holders are solely responsible for the generation of the private keys used in their Certificate Requests unless specifically agreed to in writing by HydrantID. HydrantID does not provide SSL key generation, escrow, recovery or backup facilities.

6.1.3. Public Key Delivery to Certificate Issuer

Upon making a Certificate Application, the Certificate Holder is solely responsible for generating an RSA or ECDSA cryptographic key pair and submitting the public key to HydrantID in the form of a PKCS#10 CSR. Certificate requests are generated using the key generation facilities available in the Certificate Holder's web server or application software.

6.1.4. Certification Authority Public Key Delivery to Relying Parties

HydrantID public keys are securely delivered to software providers to serve as trust anchors in commercial browsers and operating system root stores, or may be specified in a Certificate validation or path discovery policy file. Relying Parties may also obtain HydrantID self-signed CA Certificates containing its public key from the HydrantID web site.

6.1.5. Key Sizes

Key lengths within the HydrantID PKI are determined by Certificate Profiles more fully disclosed in the HydrantID Certificate Profiles document. The HydrantID Issuing CAs use an RSA minimum key length of 4,096 bit modulus or equivalent. Certificate Holders may submit 2048-bit keys or equivalent to HydrantID.

6.1.6. Public Key Parameters Generation and Quality Checking

The cryptographic hardware security modules (HSMs) used by HydrantID have been validated to conforming to FIPS 140-2 Level-3. Creation of suitable key lengths for RSA and ECDSA public keys meet the requirements of FIPS 186-2, which ensures the proper parameters and their quality (e.g., random-generation and primality).

6.1.7. Key Usage Purposes

HydrantID CA Certificates include key usage extension fields to specify the purposes for which the Certificate may be used and also to technically limit the functionality of the Certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of HydrantID. Key usages are specified in the Certificate Profiles in the HydrantID Certificate Profiles document.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards And Controls

The cryptographic hardware security modules (HSMs) used by the HydrantID PKI are validated to provide FIPS 140-2 Level-3 security standards in both the generation and the maintenance of all Root and Issuing CA private keys.

6.2.2. Private Key (n Out Of m) Multi-Person Control

Subject to the requirements of this CP/CPS, the HydrantID Root CA uses trusted multi-person control for both access control and authorization control.

6.2.3. Private Key Escrow

Private keys shall not be escrowed.

6.2.4. Private Key Backup

Issuing CA private keys are stored in an encrypted state (using an encryption key to create a "cryptographic wrapper" around the key. Access is only by N-of-M control as defined in this CP/CPS. Backup copies are maintained on site and in secure, offsite storage facilities.

6.2.5. Private Key Archival

The HydrantID PKI does not support private key archival.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

See Section 6.2.4.

6.2.7. Private Key Storage on Cryptographic Module
See Section 6.2.4.

6.2.8. Activating Private Key
An authorized user must be authenticated to the cryptographic module before the activation of the private key. This authentication may be in the form of a password. When deactivated, private keys must be kept in encrypted form only.

Certificate Holders are solely responsible for protection of their private keys. HydrantID maintains no involvement in the generation, protection, or distribution of such keys. HydrantID suggests that Certificate Holders use a strong password or equivalent authentication method to prevent unauthorized access and usage of the Certificate Holder private key.

6.2.9. Deactivating Private Key
Cryptographic modules that have been activated must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated using, for example, a manual logout procedure or a passive timeout. When not in use, cryptographic modules should be removed and securely stored, unless they are within the sole control of an authorized user.

Certificate Holders should also deactivate their private keys via logout and removal procedures when they are not in use.

6.2.10. Destroying Private Key
Private keys should be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked.

All Certificate Holders have an obligation to protect their private keys from compromise. Private keys shall be destroyed in a way that prevents their loss, theft, modification, unauthorized disclosure or unauthorized use.

Upon expiration of a CA key pair's allowed lifetime, or upon CA termination, HydrantID personnel shall destroy the CA private key by deleting and overwriting the data (e.g., via re-initialization or zeroization) or physical destruction (e.g., with a metal shredder or hammer). Such destruction shall be documented.

6.2.11. Cryptographic Module Capabilities
The cryptographic hardware security modules (HSMs) used by the HydrantID PKI are validated to FIPS 140-2 Level-3 security standards.

6.3. Other Aspects of Key Pair Management
6.3.1. Public Key Archival
Public keys will be recorded in Certificates that will be archived in the HydrantID Repository. No separate archive of public keys will be maintained by HydrantID. The validity period of Certificates will be dependent on the Certificate Policy in question.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods
The maximum validity periods for Certificates issued within the HydrantID PKI are:

Root CA Certificate	25 years
Issuing CA Certificates	10 years
Business SSL and Client Certificates	3 years
EV SSL Certificates	2 years

6.4. Activation Data
6.4.1. Activation Data Generation and Installation
Two-factor authentication shall be used to protect access to a private key.

6.4.2. Activation Data Protection
No activation data other than access control mechanisms is required to operate cryptographic modules. Personal Identification Codes may be supplied to Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third party interception. Activation data should be

memorized, not written down. Activation data must never be shared. Activation data must not contain the user's personal information.

6.4.3. Other Aspects of Activation Data
No stipulation.

6.5. Computer Security Controls
HydrantID has a formal Information Security Policy that documents the HydrantID policies, standards and guidelines relating to information security. This Information Security Policy has been approved by management and is communicated to all employees.

Computer security technical requirements are achieved utilizing a combination of hardware security modules and software, operating system security features, PKI and CA software and physical safeguards, including security Policies and Procedures that include but are not limited to:

- Access controls to CA services and PKI roles;
- Enforced separation of duties for CA Services and PKI roles;
- Identification and Authentication of personnel that fulfill roles of responsibility in the HydrantID PKI;
- Use of cryptography for session communication and database security;
- Archive of CA history and audit data;
- Use of cryptographic smart cards and x.509 Certificates for all administrators.

6.5.1. Specific Computer Security Technical Requirements
No stipulation.

6.5.2. Computer Security Rating
No stipulation.

6.6. Life Cycle Technical Controls
All hardware and software procured for the HydrantID PKI must be purchased in a manner that will mitigate the risk that any particular component was tampered with, such as random selection of specific components.

A continuous chain of accountability, from the location where all HydrantID-owned hardware and software that has been identified as supporting a CA within the HydrantID PKI, must be maintained by causing it to be shipped or delivered via controlled methods. Issuing CA equipment shall not have installed applications or component software that is not part of the Issuing CA configuration. All subsequent updates to Issuing CA equipment must be purchased or developed in the same manner as the original equipment and be installed by trusted and trained personnel in a defined manner.

6.6.1. System Development Controls
Formal procedures are followed for the development and implementation of new systems. An analysis of security requirements is carried out at the design and requirements specification stage. Outsourced software development projects are closely monitored and controlled.

6.6.2. Security Management Controls
Formal procedures and controls are in place to relating to the security-related configurations of CA systems.

6.6.3. Life Cycle Security Controls
HydrantID employs a configuration management methodology for installation and ongoing maintenance of the CA systems. The CA software, when first loaded, provides a method for HydrantID to verify that the software on the system:

- originated from the software developer;
- has not been modified prior to installation; and
- is the version intended for use.

The HydrantID Chief Security Officer periodically verifies the integrity of the CA software and monitors the configuration of the CA systems.

6.7 Network Security Controls

All access to Issuing CA equipment via a network is protected by network firewalls and filtering routers. Firewalls and filtering routers used for Issuing CA equipment limits services to and from the Issuing CA equipment to those required to perform Issuing CA functions.

All unused network ports and services on Issuing CA equipment are turned off to provide protection against known network attacks. Any network software present on the Issuing CA equipment is software required for the functioning of the Issuing CA application. All Root CA equipment is maintained and operated in stand-alone (offline) configurations.

6.8. Time-Stamping

See Section 5.5.5.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

Certificate profile information and details are maintained in a separate document. Certificates issued by HydrantID generally conform to IETF RFC 5280 and the ITU X.509v3 standard.

7.1.1. Version Numbers

CA and end-entity certificates shall be X.509 version 3.

7.1.2. Certificate Contents and Extensions; Application of RFC 5280

HydrantID CA and end-entity certificates shall contain certificate extensions that conform to applicable industry standards including, but not limited to, IETF RFC 5280 and the ITU X.509v3 standard.

7.1.3. Algorithm Object Identifiers

Algorithm object identifiers are populated according to the IETF RFC 5280 standard and industry recommendations.

7.1.4. Name Forms

Certificates will be issued with name forms that conform to Section 3.1.1. The Issuer Name shall be populated in each Certificate issued containing the Country, Organization Name and the Common Name of the Issuer CA.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a CP/CPS such as this. The Certificate Policy OIDs that incorporate this CP/CPS into a given Certificate by reference (and identify that this CP/CPS applies to a given Certificate containing the OID) are listed in the HydrantID Certificate Policies document.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

7.2.1. Version Number

For online Issuing CAs, HydrantID issues version 2 CRLs conforming to RFC 5280, and which contain the basic fields listed below:

- Version
- Issuer Signature Algorithm Issuer Distinguished Name thisUpdate (UTC format)
- nextUpdate (UTC format – thisUpdate plus 7 days)
- Revoked Certificates list

- Serial Number
- Revocation Date (see CRL entry extension for Reason Code below) Issuer's Signature

7.2.2. CRL and CRL Entry Extensions

- CRL Number (monotonically increasing integer - never repeated)
- Authority Key Identifier (same as Authority Key Identifier in Certificates issued by CA) CRL Entry Extensions
- Invalidity Date (UTC - optional)
- Reason Code (optional)

7.3. Online Certificate Status Protocol (OCSP) Profile

OCSP is enabled for all Certificates within the HydrantID PKI.

7.3.1. Online Certificate Status Protocol (OCSP) Version Numbers

OCSP Version 1, as defined by RFC 2560, is supported within the HydrantID PKI.

7.3.2. Online Certificate Status Protocol (OCSP) Extensions

No Stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or Circumstance of Assessment

The practices specified in this CP/CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including:

- AICPA/CICA Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- AICPA/CICA Network and Certificate System Security
- AICPA/CICA WebTrust for Certification Authorities, and
- WebTrust Extended Validation Program;

8.2. Identity and Qualifications of Assessor

The audit services described in Section 8.1 are performed by independent, recognized, credible, and established audit firms having significant experience with PKI and cryptographic technologies.

8.3. Assessor's Relationship to Assessed Entity

HydrantID and the auditors do not have any other relationship that would impair their independence and objectivity under Generally Accepted Auditing Standards. These relationships include financial, legal, social, or other relationships that could result in a conflict of interest.

8.4. Topics Covered By Assessment

Topics covered by the annual audits include but are not limited to CA business practices disclosure (i.e., this CP/CPS), the service integrity of CA operations and CA environmental controls.

8.5. Actions Taken As A Result Of Deficiency

Actions taken as the result of deficiency will be determined by the nature and extent of the deficiency identified. Any determination will be made by HydrantID with input from auditors. HydrantID at its sole discretion will determine an appropriate course of action and time frame to rectify the deficiency.

8.6. Communication of Audit Results

The results of these audits in the form of publicly available audit reports or opinions as provided by the external auditors responsible for these audits are published on the HydrantID website or are available upon request.

8.7 Self-Audits

HydrantID controls service quality by performing ongoing internal audits against a randomly selected sample of Certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance Or Renewal Fees

HydrantID charges Certificate Holder fees for verification, issuance, and renewal. Such fees are detailed on the HydrantID web site and/or in specific customer contracts or agreements. HydrantID retains its right to effect changes to such fees. HydrantID customers will be suitably advised of price amendments as detailed in relevant customer agreements.

9.1.2. Certificate Access Fees

HydrantID reserves the right to establish and charge a fee for access to its Repository.

9.1.3. Revocation or Status Information Access Fees

HydrantID does not charge fees for the revocation of a Certificate or for a Relying Party to check the validity status of a HydrantID issued Certificate through the use of CRLs. HydrantID reserves the right to establish and charge a fee for providing Certificate status information services via OCSP.

9.1.4. Fees for Other Services

HydrantID reserves the right to establish and charge a fee for Other Services.

9.1.5. Refund Policy

HydrantID may establish a refund policy, details of which may be contained in relevant contractual agreements.

9.2. Financial Responsibilities

9.2.1. Insurance Coverage

HydrantID maintains the following insurance related to its respective performance and obligations:

- Commercial General Liability insurance (occurrence form) with policy limits of at least $1 million in coverage, and
- Professional Liability/Errors & Omissions insurance, with policy limits of at least $1 million in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, or unintentional breach of contract, and (ii) claims for damages arising out of invasion of privacy and advertising injury.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.2.4. No Partnership or Agency

Certificate Holder shall not represent itself as being the affiliate nor an agent, partner, employee or representative of HydrantID and shall not hold itself out as such nor as having any power or authority to incur any obligation of any nature express or implied on behalf of HydrantID. Nothing in this CP/CPS shall operate nor be construed so as to constitute Certificate Holder as an agent, partner, employee, or representative of HydrantID.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

HydrantID keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- All private keys;
- Any activation data used to access private keys or gain access to the CA system;
- Any business continuity, incident response, contingency, and disaster recovery plans;
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information;
- Any information held by HydrantID as private information in accordance with Section 9.4;
- Any transactional, audit log, and archive records deemed confidential by HydrantID, including Certificate Application records and documentation submitted in support of Certificate Applications whether successful or rejected; and
- Transaction records, financial audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP/CPS).
- Any data to which HydrantID is granted access under a written Non-Disclosure Agreement

9.3.2. Information Not Within the Scope of Confidential Information

Information appearing in Certificates or stored in the Repository is considered public and not within the scope of confidential information, unless statutes or special agreements so dictate.

9.3.3. Responsibility to Protect Confidential Information

HydrantID secures private information from compromise and disclosure to unauthorized third parties.

9.4. Responsibility to Protect Private Information

HydrantID while accessing any personal data in connection with matters dealt with this CP/CPS shall comply with the protection of individuals with regard to the processing of personal data and on the free movement of such data, and any amending and/or implementing legislation enacted from time to time, and any other relevant legislation relating to data protection, and any equivalent legislation or regulations in any relevant jurisdiction.

9.4.1. Privacy Plan

HydrantID has implemented a privacy policy in compliance with this CP/CPS. The HydrantID privacy policy is published on the HydrantID web site.

9.4.2. Information Treated As Private

Personal information about an individual that is not publicly available (e.g., the contents of a Certificate or CRL) is considered private.

9.4.3. Information Not Deemed Private

Certificates, CRLs, and personal or corporate information appearing in them are not considered private. This copyrighted HydrantID CP/CPS is a public document and is not confidential information and is not treated as private.

9.4.4. Responsibility to Protect Private Information

Information supplied to HydrantID as a result of the practices described in this CP/CPS may be covered by national or state government or other privacy legislation or guidelines. HydrantID will not divulge any private personal information to any third party for any reason, unless compelled to do so by law or competent regulatory authority.

9.4.5. Notice and Consent to Use Private Information

In the course of accepting a Certificate, Individuals have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the HydrantID CA, and used as explained in the registration process and Certificate Holder Agreement. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data to appear in publicly accessible directories and be communicated to others.

9.4.6. Disclosure Pursuant To Judicial or Administrative Process

As a general principle, no document or record belonging to HydrantID is released to law enforcement agencies, officials, or persons relating to civil discovery proceedings except where a properly constituted instrument, warrant, order, judgment, subpoena, or demand is produced requiring production of the information, having been issued by a court of competent jurisdiction, and not known to HydrantID to be under appeal when served on HydrantID (HydrantID being under no obligation to determine the same).

9.4.7. Use of De-Identified Data

Notwithstanding anything herein to the contrary, HydrantID may use any data or information provided to it in connection with the issuance, maintenance or use of Certificates for HydrantID's internal analytic purposes, either during or after the term of this CP/CPS, provided such data or information is de-identified to prevent any person's identity from being connected with such data or information.

9.5. Intellectual Property Rights

All intellectual property rights, including all copyright, in all Certificates and all documents (electronic or otherwise) belong to and will remain the property of HydrantID.

Certificates are the exclusive property of HydrantID. Pursuant to separate, definitive contractual documentation, HydrantID gives permission to reproduce and distribute Certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. HydrantID reserves the right to revoke a Certificate at any time and at its sole discretion. Private keys and public keys are the property of the applicable Certificate Holders who rightfully issue and hold them.

This HydrantID CP/CPS and the Proprietary Marks are the intellectual property of HydrantID. HydrantID retains exclusive title to, copyright in, and the right to license this HydrantID CP/CPS. HydrantID excludes all liability for breach of any other intellectual property rights.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

HydrantID warrants and represents to Client that:
i. the HydrantID PKI, the software and any other services provided by HydrantID under this CP/CPS will be provided to internationally accepted standards and/ or such standard of care as is to be expected from an authorized accredited professional certification provider of digital signature Certificates;
ii. HydrantID has the right to grant or allow Client to use the HydrantID PKI, Certificates and any other products or services provided by HydrantID under this CP/CPS;
iii. the use of the HydrantID PKI, any Certificate and any other services provided by HydrantID, by Client, its employees or any Counterparty in accordance with this CP/CPS will not require any royalty or intellectual property license or export license payment to or consents, authorization, permission or license from any third party (including governmental authorities) except as have already been obtained by HydrantID;
iv. the HydrantID PKI, the Certificates and any other services provided by HydrantID under this CP/CPS shall achieve the objectives and aims as set out in the CP/CPS (including without limitation, that the Private Keys and Public Keys will function together in a complementary manner) when used by Client, its employees or any counterparty in accordance with the CP/CPS and the appropriate software application; and
v. the HydrantID PKI, software and any other services provided by HydrantID under this CP/CPS will have the functionalities, integrity, authenticity, security and confidentiality features as more particularly described in the CP/CPS.

9.6.2. RA Representations and Warranties

HydrantID does not currently use third-party Registration Authorities

9.6.3. Subscriber Representations and Warranties

As part of the Certificate Holder Agreement published at https://hydrantid.com/support/repository agreed to by all Certificate Holders, the following commitments and warranties are made for the express benefit of HydrantID and all Relying Parties and Application Software Vendors:

- **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to HydrantID, both in the Certificate Request and as otherwise requested by HydrantID in connection with the issuance of the Certificate(s) to be supplied by HydrantID;
- **Protection of Private Key:** An obligation and warranty by the Certificate Holder or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated access information or device such as a password or token);
- **Acceptance of EV Certificate:** An obligation and warranty that it will not install and use the Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;
- **Use of Certificate:** An obligation and warranty to
  - Server Certificates: install the Certificate only on the server accessible at the domain name listed on the Certificate,
  - Client Certificates: not use the Certificate to digitally sign hostile code, spyware or other malicious software and to use the Certificate in compliance with all applicable laws, and in accordance with the Certificate Holder Agreement;
- **Reporting and Revocation Upon Compromise:** An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request that HydrantID revoke the Certificate, in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Certificate Holder's Private Key associated with the Public Key listed in the Certificate; and
- **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of that Certificate.

Without limiting other Certificate Holder obligations stated in this CP/CPS, Certificate Holders are solely liable for any misrepresentations they make in Certificates to third parties that reasonably rely on the representations contained therein.

Upon accepting a Certificate, the Certificate Holder represents, warrants and covenants to HydrantID and to Relying Parties that at the time of acceptance and until further notice:

- The Certificate Holder shall retain control of the Certificate Holder's private key, use a trustworthy system, take reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use, and ensure that no unauthorized person ever has access to the Certificate Holder's private key.
- All representations made by the Certificate Holder to HydrantID regarding the information contained in the Certificate are accurate and true to the best of the Certificate Holder's knowledge, and to the extent that the Certificate Holder receives notice of such information, the Certificate Holder shall act promptly to notify HydrantID of any material inaccuracies contained in the Certificate.
- The Certificate shall be used exclusively for authorized and legal purposes, consistent with this CP/CPS, and the Certificate Holder will use the Certificate only in conjunction with the entity named in the Organization field of the Certificate.
- The Certificate Holder agrees to the terms and conditions of this CP/CPS and other agreements and policy statements of HydrantID.

9.6.4. Relying Parties Representations and Warranties

The Relying Party is solely responsible for making the decision to rely on a HydrantID Certificate. A Relying Party accepts that in order to reasonably rely on a HydrantID Certificate, the Relying Party must:

- Read and agree with the terms of the HydrantID Relying Party Agreement including the limitations on the usage of the Certificate and also the limitations of liability for reliance on a HydrantID Certificate.
- Verify the HydrantID Certificate by referring to the relevant CRL in the HydrantID Repository and trust the Certificate only if it is valid and has not been revoked or has expired.
- Rely on a HydrantID Certificate only as may be reasonable under the circumstances, given (i) the Relying Party's previous course of dealing with the Certificate Holder, (ii) the economic value of the transaction or communication, (iii) the potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the transaction or communication, (iv) all facts listed in the Certificate, or of which the Relying Party has or should have notice, including this CP/CPS, and (v) any other indicia of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining to the Certificate Holder and/or the communication or transaction.

9.6.5. Representations and Warranties of Other Participants

Not applicable.

9.7. Disclaimers of Warranties

EXCEPT FOR THE EXPRESS LIMITED WARRANTIES PROVIDED HEREIN, HydrantID DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. HydrantID LIKEWISE DISCLAIMS ANY WARRANTY CONCERNING THE SUCCESS, IMPLEMENTATION, AND OPERATION OF THE HydrantID PKI, AND DOES NOT WARRANT THAT THE SERVICES WILL MEET CLIENT'S REQUIREMENTS, OR THAT USE OR OPERATION OF ANY SYSTEMS OR SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE.

9.8. Limitations of Liability

9.8.1. HydrantID Liability

HydrantID shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CP/CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage. For the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

HydrantID's liability to any person for damages arising under, out of or related in any way to this CP/CPS, Certificate Holder Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or any other legal theory, shall, subject as hereinafter set out, be limited to actual damages suffered by that person. HydrantID shall not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if HydrantID has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise. As a condition to

participation within the HydrantID PKI (including, without limitation, the use of or reliance upon Certificates), any Participant irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to HydrantID their acceptance of the foregoing and the fact that HydrantID has relied upon the foregoing as a condition and inducement to permit that person to participate within the HydrantID Public Key Infrastructure.

9.8.2. Exclusions of Liability

HydrantID shall bear absolutely no liability for any loss whatsoever involving or arising from any one (or more) of the following circumstances or causes:

- If the Certificate held by the claiming party or otherwise the subject of any claim has been compromised by the unauthorized disclosure or unauthorized use of the Certificate or any password or activation data used to control access thereto;
- If the Certificate held by the claiming party or otherwise the subject of any claim was issued as a result of any misrepresentation, error of fact, or omission of any Individual;
- If the Certificate held by the claiming party or otherwise the subject of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim;
- If the Certificate held by the claiming party or otherwise the subject of any claim has been modified or altered in any way or been used otherwise than as permitted by the terms of this HydrantID CP/CPS and/or the relevant Certificate Holder Agreement;
- If the private key associated with the Certificate held by the claiming party or otherwise is the subject of any claim that it has been compromised;
- If the Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation;
- Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided that HydrantID uses commercially reasonable practices to protect against breaches in security resulting from such hardware, software, or algorithms;
- Power failure, power interruption, or other disturbances to electrical power, provided HydrantID uses commercially reasonable methods to protect against such disturbances;
- Failure or defects of one or more computer systems, cryptographic algorithms, protocols , operating systems, software, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of HydrantID and/or its subcontractors or service providers; or
- One or more of the following events: a natural disaster or Act of God (including without limitation flood, earthquake, or other natural or weather related cause); a labor disturbance (strike); war, insurrection, or overt military hostilities; adverse legislation or governmental action, prohibition, embargo, or boycott; riots or civil disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of telecommunications availability or integrity; legal compulsion including, any judgments of a court of competent jurisdiction to which HydrantID is, or may be, subject; and any event or occurrence or circumstance or set of circumstances that is beyond the control of HydrantID.

9.8.3. Certificate Loss Limits

WITHOUT PREJUDICE TO ANY OTHER PROVISION OF THIS SECTION 9, HydrantID's LIABILITY TO ANY PARTICIPANT OR OTHER PARTY ARISING OUT OF THIS CP/CPS OR ANY CERTIFICATE ISSUED HEREUNDER FOR ANY REASON AND UPON ANY CAUSE OF ACTION, WHETHER SOUNDING IN TORT, CONTRACT, NEGLIGENCE, STRICT LIABILITY IN TORT OR BY STATUTE OR ANY OTHER LEGAL THEORY, SHALL AT ALL TIMES AND IN THE AGGREGATE BE LIMITED TO AN AMOUNT EQUAL TO THE LESSER OR (I) $5,000 USD PER CLAIMANT FOR ANY AND ALL CLAIMS THAT SUCH CLAIMANT MAY MAKE AGAINST HydrantID, or (ii) $500 PER CERTIFICATE FOR ALL ANY AND ALL CLAIMS RELATING TO SUCH CERTIFICATE.

In no event shall HydrantID's liability exceed the loss limits set out in paragraph 9.8 and 9.8.3. The loss limits apply to the life cycle of a particular Certificate to the intent that the loss limits reflect HydrantID's total potential cumulative liability per Certificate (irrespective of the number of claims per Certificate). The foregoing limitation applies regardless of the number of transactions or causes of action relating to a particular Certificate during that Certificate's life cycle.

9.9. Indemnities

Certificate Holders shall indemnify HydrantID and its officers, directors, employees and agents (collectively, the "Indemnified Parties") and hold the Indemnified Parties harmless from and against any losses, costs, damages, expenses and fees (including attorneys' fees) incurred by the Indemnified Parties in connection with: (a) any breach by Certificate Holder of any representation, warranty, guarantee, term, condition or obligation under this CP/CPS (including but not limited to infringement of any intellectual property right); (b) misrepresentation or omission of

material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional; (c) tampering with a HydrantID Certificate; (d) the unauthorized use of any Certificate; (e) failure to protect the Private Key, or (f) any content or other information or data supplied by the Certificate Holder (collectively, Indemnity Conditions). Upon appropriate notice, Certificate Holder shall defend, at their expense, any claim brought against one or more of the Indemnified Parties based on or arising from one or more of the Indemnity Conditions.

9.10. Term and Termination

9.10.1. Term

This CP/CPS and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2. Termination

This CP/CPS shall remain in force until it is terminated by notice from HydrantID or amended or replaced by a new version in accordance with this Section 9.

9.10.3. Effect of Termination and Survival

The conditions and effect resulting from termination of this CP/CPS will be communicated via the HydrantID website upon termination. That communication will outline the provisions that may survive termination of this CP/CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

9.11. Individual Notices and Communications with Participants

Electronic mail, postal mail, and fax will all be valid means of providing any notice required pursuant to this CP/CPS to HydrantID unless specifically provided otherwise (for example, with respect to revocation procedures).

9.12. Amendments

9.12.1. Procedure For Amendment

Amendments to this CP/CPS are made and approved by the HydrantID Policy Management Authority (PMA). Amendments shall be in the form of an amended CP/CPS or a replacement CP/CPS. Updated versions of this CP/CPS supersede any designated or conflicting provisions of the referenced version of the CP/CPS.

9.12.2. Notification Mechanism and Period

The HydrantID PMA reserves the right to amend this CP/CPS without notification for amendments that are not material, including typographical corrections, changes to URLs, and changes to contact details. The decision to designate amendments as material or non-material to this CP/CPS is at the sole discretion of the HydrantID PMA.

9.12.3. Circumstances under which OID must be changed

Unless the HydrantID PMA determines otherwise, the OID for this CP/CPS shall not change. If a change in HydrantID's certification practices is determined by the PMA to warrant a change in the currently specified OID for a particular Certificate Policy, then the revised version of this CP/CPS will also contain a revised OID for that Certificate Policy.

9.13. Dispute Resolution Provisions

Notwithstanding anything to the contrary in this CP/CPS, if the Participant involved in any legal action or proceeding with HydrantID is located outside the United States or Canada, then any disputes, actions, claims or causes of action arising out of or in connection with this Agreement (or the Service) with such Participant shall be settled by arbitration in English in Salt Lake City, Utah, administered by the American Arbitration Association under its Commercial Arbitration Rules, and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof. Notwithstanding the foregoing agreement to arbitrate, either party may seek interim or provisional relief, including a temporary restraining order, preliminary injunction or other interim equitable relief, in any court of competent jurisdiction concerning any dispute, if necessary to protect the interests of such party.

9.14. Governing Law

This CP/CPS and any HydrantID Certificates issued by HydrantID shall be construed pursuant to the laws of the State of Utah, without giving effect to conflict of laws rules. Any legal action or proceeding with respect to this CP/CPS shall be brought exclusively in the state or federal courts of Salt Lake County, Utah, and each Participant hereby irrevocably (a) accepts for itself and in respect of its property, generally and unconditionally, the exclusive jurisdiction of the aforesaid courts, (b) waives any claim that any such courts lack personal jurisdiction over it, and agrees not to plead or claim, in any legal action proceeding with respect to this CP/CPS in any such courts, that such courts lack personal jurisdiction

over it and (c) waives any objection that it may now or hereafter have to the laying of venue of any of the aforesaid actions or proceedings arising out of or in connection with this CP/CPS brought in the aforesaid courts and hereby further irrevocably, to the extent permitted by applicable law, waives its rights to plead or claim and agrees not to plead or claim in any such courts that any such action or proceeding brought in any such courts has been brought in an inconvenient forum

9.15. Compliance with Applicable Law

Certificate Holders and Relying Parties shall use HydrantID Certificates and any other related information and materials provided by HydrantID only in compliance with all applicable laws and regulations. HydrantID may refuse to issue or may revoke Certificates if, in the reasonable opinion of HydrantID, issuance or the continued use of the HydrantID Certificates would violate applicable laws or regulations.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

Unless otherwise agreed to in writing, this CP/CPS comprises the Entire Agreement between HydrantID and each Participant.

9.16.2. Assignment

Parties to this CP/CPS may not assign any of their rights or obligations under this CP/CPS or applicable agreements without the written consent of HydrantID, and any such attempted assignment shall be void.

9.16.3. Severability

Any provision of this HydrantID CP/CPS that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this HydrantID CP/CPS or affecting the validity or enforceability of such remaining provisions.

9.16.4. Enforcement (Waiver of Rights)

Except where an express time frame is set forth in this CP/CPS, no delay or omission by HydrantID to exercise any right, remedy, or power it has under this CP/CPS shall impair or be construed as a waiver of such right, remedy, or power. A waiver by HydrantID of any breach or covenant in this CP/CPS shall not be construed to be a waiver of any other or succeeding breach or covenant. No waiver shall be effective unless it is in writing. Bilateral agreements between HydrantID and any Participant may contain additional provisions governing enforcement.

9.16.5. Waiver of Jury Trial

HydrantID and EACH PARTICIPANT HEREBY IRREVOCABLY WAIVES, TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, ANY RIGHT IT MAY HAVE TO A TRIAL BY JURY IN ANY LEGAL PROCEEDING DIRECTLY OR INDIRECTLY ARISING OUT OF OR RELATING TO THIS CP/CPS OR ANY OTHER PURCHASE DOCUMENTS OR THE TRANSACTIONS CONTEMPLATED HEREBY OR THEREBY (WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY).

9.17 Other Provisions

No stipulation

[END OF DOCUMENT – THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

