**Bugzilla ID:**

**Bugzilla Summary:**

Overview:

Avalanche Cloud Corporation, dba HydrantID is submitting three proposed trusted roots for inclusion in Mozilla products:

* HydrantID Root CA 1 (RSA 4,096 SHA-256)
* HydrantID Root CA 2 (RSA 4,096 SHA-512)
* HydrantID Root CA 3 (ECDSA P-384 SHA-384)

HydrantID wishes to have their certificates included in Mozilla products and attests that it:

1. Complies with the requirements of the Mozilla CA certificate policy (<http://www.mozilla.org/projects/security/certs/policy>)
2. Have supplied herein all of the information listed in <http://wiki.mozilla.org/CA:Information_checklist> and
   1. Have reviewed the Recommended Practices at https://wiki.mozilla.org/CA:Recommended\_Practices
   2. Have reviewed the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic\_Practices

**General information about HydrantID’s associated organization**

|  |  |
| --- | --- |
| CA Company Name | Avalanche Cloud Corporation dba HydrantID |
| Website URL | [www.hydrantid.com](http://www.hydrantid.com/) |
| Organizational type | Privately held Delaware Corporation  Doing Business As (DBA) HydrantID |
| Primark Market / Customer Base | Public customers worldwide, primarily Enterprise class businesses  HydrantID issued only EV and OV SSL certificates  HydrantID does not issue DV SSL certificates. |
| Impact to Mozilla Users | HydrantID is a digital identity and advanced authentication company that operates as a trust anchor for the general public. |
| Inclusion in other major browsers | Current applications with Microsoft and Apple |
| CA Primary Point of Contact (POC) | https://wiki.mozilla.org/CA:Information\_checklist#CA\_Primary\_Point\_of\_Contact\_.28POC.29  Jim Palmer  Chief Authentication Officer  HydrantID  POC direct email: jim@hydrantid.com  Email Alias: none  CA Phone Number: +1 801.243.6940  An official representative of the CA must submit and/or participate in the root inclusion request. According to Mozilla's CA Certificate Inclusion Policy: "To request that its certificate(s) be added to the default set a CA should submit a formal request by submitting a bug report into the mozilla.org Bugzilla system ... **The request must be made by an authorized representative of the subject CA**..."  If the CA contracts to another organization to help with the root inclusion request, the official representative of the CA must clarify that relationship in the bug, and must provide clear information about who the ongoing points-of-contact will be for the CA. |

**Technical information about each root certificate**

**HydrantID Root CA 1**

|  |  |
| --- | --- |
| Certificate Name | HydrantID Root CA 1 |
| Certificate Issuer Field | CN=HydrantID Root CA 1  O=HydrantID (Avalanche Cloud Corporation)  C=US |
| Certificate Summary | The HydrantID Roots are used to issue trusted SSL (OV and EV only) certificates and Secure Multipurpose Internet Mail Extensions (S/MIME) identity certiicates |
| Mozilla Applied Constraints | None. |
| Root Cert URL | [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository) |
| SHA1 Fingerprint | ‎e2 c2 25 fe 57 b6 c8 1f 85 88 7e 28 b1 d7 68 02 f3 f5 43 df |
| Valid From | 2015-05-21 (May 21 2015 18:01:08 UTC) |
| Valid To | 2039-05-21 (May 21 2039 18:01:08 UTC) |
| Certificate Version | V3 |
| Certificate Signature Algorithm | Sha256RSA |
| Signing key parameters | RSA modulus length: 2,048 bits |
| Test Website URL (SSL)  Example Certificate (non-SSL) | [https://root1-ssl-v.hydrantid.com](https://root1-ssl-v.hydrantid.com/) (valid OV SSL)  [https://root1-ssl-r.hydrantid.com](https://root1-ssl-r.hydrantid.com/) (revoked OV SSL)  [https://root1-ssl-e.hydrantid.com](https://root1-ssl-e.hydrantid.com/) (expired OV SSL)  [https://root1-ev-v.hydrantid.com](https://root1-ev-v.hydrantid.com/) (valid EV SSL)  [https://root1-ev-r.hydrantid.com](https://root1-ev-r.hydrantid.com/) (revoked EV SSL)  [https://root1-ev-e.hydrantid.com](https://root1-ev-e.hydrantid.com/) (expired EV SSL) |
| CRL URL | <http://crl.hydrantid.com/SSLICA1A/SSLICA1A.crl>  NextUpdate for CRLs of end-entity certs,  actual value: ‎Wednesday, ‎June ‎03, ‎2015 4:04:32 PM  what’s documented in CP/CPS: “(UTC format – thisUpdate plus 7 days)” |
| OCSP URL (Required now for end-­entity certs) | OCSP URI in the AIA of end-entity certs  URL=http://ocsp1.hydrantid.com  OCSP Stapling is supported  Maximum expiration time of OCSP responses  Testing results   1. Browsing to test website with OCSP enforced in Firefox browser 2. If requesting EV: https://wiki.mozilla.org/PSM:EV\_Testing\_Easy\_Version   Regarding Mozilla’s revocation checking plans:  - OCSP is (and will continue to be) required for end-entity certs. OCSP stapling is preferred.  - For revocation checking of intermediate certs we will be moving towards a CRL push mechanism, so Mozilla will not be requiring OCSP for intermediate certs. |
| Requested Trust Bits | ✓ Websites (SSL/TLS)  ✓ Email (S/MIME) |
| SSL Validation Type | Extended Validation |
| EV Policy OID(s) | 1.3.6.1.4.1.44058.0.1.1.1 |
| Non-sequential serial numbers and entropy in cert | http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html  “9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: …  - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number).”  The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration.  This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn’t an acceptable hash algorithm for certificates in this hierarchy.  HydrantID attests that our PKI issuing infrastructure complies |
| Response to Recent CA Communication(s) | https://wiki.mozilla.org/CA:Communications  HydrantID attests that we have reviewed and are compliant |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | List, description, and/or diagram of all intermediate CAs signed by this root.    See detailed exhibits appended below. |
| Externally Operated SubCAs | If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA\_checklist  If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.  HydrantID operates its own subCAs |
| Cross-Signing | List all other root certificates for which this root certificate has issued cross-signing certificates.  List all other root certificates that have issued cross-signing certificates for this root certificate.  If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.  HydrantID: None |
| Technical Constraints on Third-party Issuers | Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of  https://wiki.mozilla.org/CA:Information\_checklist#CA\_Hierarchy\_information\_for\_each\_root\_certificate  HydrantID is currently undergoing a WebTrust for CAs and Extended Validation audit and has implemented a “m of n” multi-factor authentication process that requires the approval of two HydrantID personnel acting in trusted roles to issue an end-entity certificate. (Three or more are required to issue from the Root CA) |

**HydrantID Root CA 2**

|  |  |
| --- | --- |
| Certificate Name | HydrantID Root CA 2 |
| Certificate Issuer Field | CN=HydrantID Root CA 2  O=HydrantID (Avalanche Cloud Corporation)  C=US |
| Certificate Summary | The HydrantID Roots are used to issue trusted SSL (OV and EV only) certificates and Secure Multipurpose Internet Mail Extensions (S/MIME) identity certiicates |
| Mozilla Applied Constraints | None. |
| Root Cert URL | [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository) |
| SHA1 Fingerprint | ‎f4 cc b2 74 81 38 0e 6a 8c 43 50 41 80 9c 69 85 25 33 f4 f5 |
| Valid From | ‎May ‎21, ‎2015 1:42:53 PM |
| Valid To | May ‎21, ‎2039 1:42:53 PM |
| Certificate Version | V3 |
| Certificate Signature Algorithm | RSA 4,096 |
| Signing key parameters | RSA modulus length: 4,096 bits |
| Test Website URL (SSL)  Example Certificate (non-SSL) | [https://root2-ssl-v.hydrantid.com](https://root2-ssl-v.hydrantid.com/) (valid OV SSL)  <https://root2-ssl-r.hydrantid.com/> (revoked OV SSL)  <https://root2-ssl-e.hydrantid.com/> (expired OV SSL)  <https://root2-ev-v.hydrantid.com/> (valid EV SSL)  <https://root2-ev-r.hydrantid.com/> (revoked EV SSL)  <https://root2-ev-e.hydrantid.com/> (expired EV SSL) |
| CRL URL | URL=http://crl.hydrantid.com/SSLICA2A/SSLICA2A.crl  what’s documented in CP/CPS: “(UTC format – thisUpdate plus 7 days)” |
| OCSP URL (Required now for end-­entity certs) | OCSP URI in the AIA of end-entity certs  URL=http://ocsp2.hydrantid.com  OCSP Stapling is supported  Maximum expiration time of OCSP responses  Testing results   1. Browsing to test website with OCSP enforced in Firefox browser 2. If requesting EV: https://wiki.mozilla.org/PSM:EV\_Testing\_Easy\_Version   Regarding Mozilla’s revocation checking plans:  - OCSP is (and will continue to be) required for end-entity certs. OCSP stapling is preferred.  - For revocation checking of intermediate certs we will be moving towards a CRL push mechanism, so Mozilla will not be requiring OCSP for intermediate certs. |
| Requested Trust Bits | ✓ Websites (SSL/TLS)  ✓ Email (S/MIME) |
| SSL Validation Type | Extended Validation |
| EV Policy OID(s) | 1.3.6.1.4.1.44058.0.1.1.1 |
| Non-sequential serial numbers and entropy in cert | http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html  “9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: …  - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number).”  The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration.  This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn’t an acceptable hash algorithm for certificates in this hierarchy.  HydrantID attests that we have reviewed and our PKI issuing infrastructure complies |
| Response to Recent CA Communication(s) | https://wiki.mozilla.org/CA:Communications  HydrantID attests that we have reviewed and our PKI issuing infrastructure complies |

**CA Hierarchy information for each root certificate**

**HydrantID Root CA 2**

|  |  |
| --- | --- |
| CA Hierarchy | List, description, and/or diagram of all intermediate CAs signed by this root.    See detailed exhibits appended below. |
| Externally Operated SubCAs | If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA\_checklist  If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.  HydrantID operates its own subCAs |
| Cross-Signing | List all other root certificates for which this root certificate has issued cross-signing certificates.  List all other root certificates that have issued cross-signing certificates for this root certificate.  If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.  HydrantID: None |
| Technical Constraints on Third-party Issuers | Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of  https://wiki.mozilla.org/CA:Information\_checklist#CA\_Hierarchy\_information\_for\_each\_root\_certificate  HydrantID is currently undergoing a WebTrust for CAs and Extended Validation audit and has implemented a “m of n” multi-factor authentication process that requires the approval of two HydrantID personnel acting in trusted roles to issue an end-entity certificate. (Three or more are required to issue from the Root CA) |

**HydrantID Root CA 3**

|  |  |
| --- | --- |
| Certificate Name | HydrantID Root CA 3 |
| Certificate Issuer Field | CN=HydrantID Root CA 3  O=HydrantID (Avalanche Cloud Corporation)  C=US |
| Certificate Summary | The HydrantID Roots are used to issue trusted SSL (OV and EV only) certificates and Secure Multipurpose Internet Mail Extensions (S/MIME) identity certificates |
| Mozilla Applied Constraints | None. |
| Root Cert URL | [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository) |
| SHA1 Fingerprint | ‎b7 69 02 a8 d2 a9 8c 44 fa a6 55 19 e5 2c cf 5a be c1 db 95 |
| Valid From | May 21 2015 20:57:08 UTC |
| Valid To | May 21 2039 20:57:33 UTC |
| Certificate Version | V3 |
| Certificate Signature Algorithm | sha384ECDSA |
| Signing key parameters | ECDSA\_P384 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | [https://root3-ssl-v.hydrantid.com](https://root3-ssl-v.hydrantid.com/) (valid OV SSL)  [https://root3-ssl-r.hydrantid.com](https://root3-ssl-r.hydrantid.com/) (revoked OV SSL)  [https://root3-ssl-e.hydrantid.com](https://root3-ssl-e.hydrantid.com/) (expired OV SSL)  [https://root3-ev-v.hydrantid.com](https://root3-ev-v.hydrantid.com/) (valid EV SSL)  [https://root3-ev-r.hydrantid.com](https://root3-ev-r.hydrantid.com/) (revoked EV SSL)  [https://root3-ev-e.hydrantid.com](https://root3-ev-e.hydrantid.com/) (expired EV SSL) |
| CRL URL | URL=http://crl.hydrantid.com/SSLICA3A/SSLICA3A.crl  what’s documented in CP/CPS: “(UTC format – thisUpdate plus 7 days)” |
| OCSP URL (Required now for end-­entity certs) | OCSP URI in the AIA of end-entity certs  URL=http://ocsp3.hydrantid.com  OCSP Stapling is supported  Maximum expiration time of OCSP responses  Testing results   1. Browsing to test website with OCSP enforced in Firefox browser 2. If requesting EV: https://wiki.mozilla.org/PSM:EV\_Testing\_Easy\_Version   Regarding Mozilla’s revocation checking plans:  - OCSP is (and will continue to be) required for end-entity certs. OCSP stapling is preferred.  - For revocation checking of intermediate certs we will be moving towards a CRL push mechanism, so Mozilla will not be requiring OCSP for intermediate certs. |
| Requested Trust Bits | ✓ Websites (SSL/TLS)  ✓ Email (S/MIME) |
| SSL Validation Type | Extended Validation |
| EV Policy OID(s) | 1.3.6.1.4.1.44058.0.1.1.1 |
| Non-sequential serial numbers and entropy in cert | http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html  “9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: …  - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number).”  The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration.  This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn’t an acceptable hash algorithm for certificates in this hierarchy.  HydrantID attests that we have reviewed and our PKI issuing infrastructure complies |
| Response to Recent CA Communication(s) | https://wiki.mozilla.org/CA:Communications  HydrantID attests that we have reviewed and our PKI issuing infrastructure complies |

**CA Hierarchy information for each root certificate**

**HydrantID Root CA 2**

|  |  |
| --- | --- |
| CA Hierarchy | List, description, and/or diagram of all intermediate CAs signed by this root.    See detailed exhibits appended below. |
| Externally Operated SubCAs | If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA\_checklist  If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.  HydrantID operates its own subCAs |
| Cross-Signing | List all other root certificates for which this root certificate has issued cross-signing certificates.  List all other root certificates that have issued cross-signing certificates for this root certificate.  If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.  HydrantID: None |
| Technical Constraints on Third-party Issuers | Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of  https://wiki.mozilla.org/CA:Information\_checklist#CA\_Hierarchy\_information\_for\_each\_root\_certificate  HydrantID is currently undergoing a WebTrust for CAs and Extended Validation audit and has implemented a “m of n” multi-factor authentication process that requires the approval of two HydrantID personnel acting in trusted roles to issue an end-entity certificate. (Three or more are required to issue from the Root CA) |

**Verification Policies and Practices**

|  |  |
| --- | --- |
| Policy Documentation | Language(s) that the documents are in:  CP: U.S. English  CPS: U.S. English  Relying Party Agreement: U.S. English |
| Audits | Audit Type: WebTrust® Trust Service Principles and Criteria for Certification Authorities,  Baseline SSL with Network Security, and  Extended Validation SSL  Auditor: Stone-Carlie (now BDO, as of June 1, 2015)  Auditor Website: [www.stonecarlie.com](http://www.stonecarlie.com/) and [www.bdo.com](http://www.bdo.com/)  URL to Audit Report and Management’s Assertions:  [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository) |
| Baseline Requirements (SSL) | URL to BR audit statement:  This audit is in process and should be completed Q4 2015  Please carefully review: https://wiki.mozilla.org/CA:BaselineRequirements  (also have your auditor carefully review this wiki page)  [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository)  CP/CPS Section 1.1 Paragraph i  The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.  Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results.  https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Time\_Frames\_for\_included\_CAs\_to\_comply\_with\_the\_new\_policy  “Any Certificate Authority being considered for root inclusion after February 15, 2013 must comply with Version 2.1 or later of Mozilla's CA Certificate Policy. This includes having a Baseline Requirements audit performed if the websites trust bit is to be enabled. Note that the CA's first Baseline Requirements audit may be a Point in Time audit.” |
| SSL Verification Procedures | If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of  [https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices](https://wiki.mozilla.org/CA:Information_checklist" \l "Verification_Policies_and_Practices)  [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository)  CP/CPS Section 3 - IDENTIFICATION AND AUTHENTICATION |
| Organization Verification Procedures | [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository)  CP/CPS Section 3 - IDENTIFICATION AND AUTHENTICATION |
| Email Address Verification Procedures | If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of  [https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices](https://wiki.mozilla.org/CA:Information_checklist" \l "Verification_Policies_and_Practices)  [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository)  CP/CPS Section 3 - IDENTIFICATION AND AUTHENTICATION |
| Code Signing Subscriber Verification Procedures | If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of  https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices  HydrantID is not requesting code-signing |
| Multi-factor Authentication | Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices  HydrantID uses a multi-factor authentication system and also requires an “m of n” multi-person approval process. |
| Network Security | Confirm that you have performed the actions listed in #7 of  [https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices](https://wiki.mozilla.org/CA:Information_checklist" \l "Verification_Policies_and_Practices)  HydrantID confirms that we comply with this requirement, as to be evidenced by the current Baseline SSL with Network Security Audit which is underway. |

|  |  |
| --- | --- |
| Publicly Available CP and CPS | [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository) |
| CA Hierarchy | HydrantID utilizes online Issuing CAs, certificates for which are issued from a single off-line trusted Root CA. Multiple issuing CAs may chain back to a single root CA. |
| Audit Criteria | Audit Type: WebTrust® Trust Service Principles and Criteria for Certification Authorities,  Baseline SSL with Network Security, and  Extended Validation SSL  Auditor: Stone-Carlie (now BDO, as of June 1, 2015)  Auditor Website: [www.stonecarlie.com](http://www.stonecarlie.com/) and [www.bdo.com](http://www.bdo.com/)  URL to Audit Report and Management’s Assertions:  [www.hydrantid.com/support/repository](http://www.hydrantid.com/support/repository) |
| Document Handling of IDNs in CP/CPS | HydrantID does not issue certificates with internationalized domain names (IDNs) |
| Revocation of Compromised Certificates | HydrantID revokes certificates within 24 hours in accordance with CA/B Forum BR requirement 4.9.1 |
| Verifying Domain Name Ownership | HydrantID contacts the registered WHOIS contact for each domain either by email or telephone. In cases where that cannot be done, HydrantID utilizes one of the alternate methods specified in CA/B Forum BR 3.2.2.4, primarily emailing “hostmaster@” or having the applicant make a change to the DNS to demonstrate domain control. |
| Verifying Email Address Control | HydrantID verifies control of email addresses by sending an email to the requested address containing a link to which the applicant must click in a limited amount of time or respond via reply email, which confirms the email address. |
| Verifying Identity of Code Signing Certificate Subscriber | HydrantID will not be issuing code signing certificates from this root or its issuing sub-CAs |
| DNS names go in SAN | HydrantID complies with the CA/B Forum BR in populating SAN fields. HydrantID populates the Subject Common Name Field with a Fully Qualified Domain Name. |

**Response to Mozilla's CA Recommended Practices** (https://wiki.mozilla.org/CA:Recommended\_Practices)

|  |  |
| --- | --- |
| Domain owned by a Natural Person | HydrantID discourages requests by Natural Persons to issue SLL certificates. |
| OCSP | HydrantID’s OSCP responders include OCSP stapling in the response and are available on HTTP: port 80 and have been tested and verified to work with Mozilla Firefox |

**Response to Mozilla's list of Potentially Problematic Practices** (https://wiki.mozilla.org/CA:Problematic\_Practices)

|  |  |
| --- | --- |
| Long-lived DV certificates | HydrantID does not issue DV SSL certificates. HydrantID only issues OV and EV SSL certificates. |
| Wildcard DV SSL certificates | HydrantID does not issue DV SSL certificates. HydrantID only issues OV and EV SSL certificates. |
| Email Address Prefixes for DV Certs | HydrantID does not issue DV SSL certificates. HydrantID only issues OV and EV SSL certificates. |
| Delegation of Domain / Email validation to third parties | HydrantID trusted personnel perform all validation |
| Issuing end entity certificates directly from roots | HydrantID does not issue end-entity certificates directly from roots |
| Allowing external entities to operate subordinate CAs | HydrantID operates its own subCAs and does not utilize external entities for such operations. |
| Distributing generated private keys in PKCS#12 files | HydrantID does not distribute private keys in PKCS#12 files |
| Certificates referencing hostnames or private IP addresses | HydrantID does not issue certificates referencing hostnames or private IP addresses |
| Issuing SSL Certificates for Internal Domains | HydrantID does not issue trusted certificates to internal domain names or unroutable IP addresses |
| OCSP Responses signed by a certificate under a different root | Each HydrantID OCSP responder is signed by a certificate issued by the root for which it is the responder. HydrantID operates its OCSP Responders in accordance with RFC 2560. |
| SHA-1 Certificates | HydrantID does not issue SHA1 certificates |
| Generic names for CAs | HydrantID uses descriptive names for its roots and issuing CAs, all off which begin with “HydrantID” |
| Lack of Communication With End Users | HydrantID publishes email, telephone, web and chat based methods of contacting our support group. |
| Backdating the notBefore date | HydrantID does not backdate the notBefore date |

**HydrantID Test sites with sample SSL certificates**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **URL** | **Root CA** | **Intermediate CA** | **Cert Status** | **Cert Type** |
| [https://root1-ssl-v.hydrantid.com](https://root1-ssl-v.hydrantid.com/) | HydrantID Root CA 1 | HydrantID SSL ICA 1A | Valid | OV SSL |
| [https://root1-ssl-r.hydrantid.com](https://root1-ssl-r.hydrantid.com/) | HydrantID Root CA 1 | HydrantID SSL ICA 1A | Revoked | OV SSL |
| [https://root1-ssl-e.hydrantid.com](https://root1-ssl-e.hydrantid.com/) | HydrantID Root CA 1 | HydrantID SSL ICA 1A | Expired | OV SSL |
| [https://root2-ssl-v.hydrantid.com](https://root2-ssl-v.hydrantid.com/) | HydrantID Root CA 2 | HydrantID SSL ICA 2A | Valid | OV SSL |
| [https://root2-ssl-r.hydrantid.com](https://root2-ssl-r.hydrantid.com/) | HydrantID Root CA 2 | HydrantID SSL ICA 2A | Revoked | OV SSL |
| [https://root2-ssl-e.hydrantid.com](https://root2-ssl-e.hydrantid.com/) | HydrantID Root CA 2 | HydrantID SSL ICA 2A | Expired | OV SSL |
| [https://root3-ssl-v.hydrantid.com](https://root3-ssl-v.hydrantid.com/) | HydrantID Root CA 3 | HydrantID SSL ICA 3A | Valid | OV SSL |
| [https://root3-ssl-r.hydrantid.com](https://root3-ssl-r.hydrantid.com/) | HydrantID Root CA 3 | HydrantID SSL ICA 3A | Revoked | OV SSL |
| [https://root3-ssl-e.hydrantid.com](https://root3-ssl-e.hydrantid.com/) | HydrantID Root CA 3 | HydrantID SSL ICA 3A | Expired | OV SSL |
| [https://root1-ev-v.hydrantid.com](https://root1-ev-v.hydrantid.com/) | HydrantID Root CA 1 | HydrantID SSL ICA 1A | Valid | EV SSL |
| [https://root1-ev-r.hydrantid.com](https://root1-ev-r.hydrantid.com/) | HydrantID Root CA 1 | HydrantID SSL ICA 1A | Revoked | EV SSL |
| [https://root1-ev-e.hydrantid.com](https://root1-ev-e.hydrantid.com/) | HydrantID Root CA 1 | HydrantID SSL ICA 1A | Expired | EV SSL |
| [https://root2-ev-v.hydrantid.com](https://root2-ev-v.hydrantid.com/) | HydrantID Root CA 2 | HydrantID SSL ICA 2A | Valid | EV SSL |
| [https://root2-ev-r.hydrantid.com](https://root2-ev-r.hydrantid.com/) | HydrantID Root CA 2 | HydrantID SSL ICA 2A | Revoked | EV SSL |
| [https://root2-ev-e.hydrantid.com](https://root2-ev-e.hydrantid.com/) | HydrantID Root CA 2 | HydrantID SSL ICA 2A | Expired | EV SSL |
| [https://root3-ev-v.hydrantid.com](https://root3-ev-v.hydrantid.com/) | HydrantID Root CA 3 | HydrantID SSL ICA 3A | Valid | EV SSL |
| [https://root3-ev-r.hydrantid.com](https://root3-ev-r.hydrantid.com/) | HydrantID Root CA 3 | HydrantID SSL ICA 3A | Revoked | EV SSL |
| [https://root3-ev-e.hydrantid.com](https://root3-ev-e.hydrantid.com/) | HydrantID Root CA 3 | HydrantID SSL ICA 3A | Expired | EV SSL |







