Mozilla - CA Program

Case Information

Case Number	00000065	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	HydrantID	**Request Status**	Need Information from CA

Additional Case Information

Subject	Include HydrantID root certificates	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1173547

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	www.hydrantid.com	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	USA	**Verified?**	Verified
Primary Market / Customer Base	Avalanche Cloud Corporation doing business as (dba) HydrantID issues certificates to public customers worldwide, primarily Enterprise class businesses.	**Verified?**	Verified
Impact to Mozilla Users	New CA with current applications also with Microsoft and Apple. Avalanche Cloud Corporation is an organization in the internet access companies industry, located in the USA	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	* HydrantID discourages requests by Natural Persons to issue SLL certificates. * 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	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	* HydrantID does not issue DV SSL certificates. HydrantID issues OV and EV SSL certificates. * Wildcard SSL certs are OV. * HydrantID trusted personnel perform all validation * HydrantID does not issue certificates with internationalized domain names (IDNs) * HydrantID revokes certificates within 24 hours in accordance with CA/B Forum BR requirement 4.9.1 * 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. * HydrantID operates its own subCAs and does not utilize external entities for such operations. * HydrantID does not issue certificates referencing hostnames or private IP addresses * HydrantID does not issue trusted certificates to internal domain names or unroutable IP addresses	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	HydrantID Root CA 1	**Root Case No**	R00000088
Request Status	Need Information from CA	**Case Number**	00000065

Additional Root Case Information

Subject	Include HydrantID Root CA 1

Technical Information about Root Certificate

O From Issuer Field	HydrantID (Avalanche Cloud Corporation)	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This SHA-256 root cert signs internally-operated intermediate certs that sign end-entity certs.	**Verified?**	Verified
Root Certificate Download URL	http://crl.hydrantid.com/SSLICA1A/HIDROOT1.crt	**Verified?**	Verified
Valid From	2015 May 21	**Verified?**	Verified
Valid To	2039 May 21	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified

			Verified?	Verified
Signing Key Parameters	4096		**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://root1-ev-v.hydrantid.com		**Verified?**	Verified
CRL URL(s)	http://crl.hydrantid.com/SSLICA1A/HIDROOT1.crl http://crl.hydrantid.com/SSLICA1A/SSLICA1A.crl NextUpdate for CRLs of end-entity certs, CP/CPS: "(UTC format – thisUpdate plus 7 days)"		**Verified?**	Verified
OCSP URL(s)	http://ocsp1.hydrantid.com OCSP Stapling is supported		**Verified?**	Verified
Revocation Tested	http://certificate.revocationcheck.com/root1-ev-v.hydrantid.com results in no Errors		**Verified?**	Verified
Trust Bits	Email; Websites		**Verified?**	Verified
SSL Validation Type	OV; EV		**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.44058.0.1.1		**Verified?**	Verified
EV Tested	// CN=HydrantID Root CA 1,O=HydrantID (Avalanche Cloud Corporation),C=US "1.3.6.1.4.1.44058.0.1.1", "HydrantID EV OID", SEC_OID_UNKNOWN, { 0x69, 0x92, 0x75, 0x50, 0xE9, 0x19, 0x62, 0x5F, 0xAF, 0x24, 0x99, 0x2A, 0xFE, 0x77, 0xF3, 0x9D, 0x61, 0xFF, 0xAA, 0x3E, 0x78, 0xD4, 0x7C, 0x4A, 0x3E, 0xEE, 0x22, 0x28, 0xB8, 0x15, 0x2C, 0x15 }, "MF0xCzAJBgNVBAYTAlVTMTAwLgYDVQQKEydIeWRyYW50SUQgKEF2YWxhbmNoZSBD" "bG91ZCBDb3Jwb3JhdGlvbikxHDAaBgNVBAMTE0h5ZHJhbnRJRCBSb290IENBIDE=" "", "J9Kxy7NhhpFEVZruMPhNpQ==", Success!		**Verified?**	Verified
Root Stores Included In			**Verified?**	Verified
Mozilla Applied Constraints	None		**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	A0:4E:BE:E6:24:4F:4C:77:7C:BC:8C:3A:2C:3A:E2:76:F8:25:BC:E3		**Verified?**	Verified
SHA-256 Fingerprint	69:92:75:50:E9:19:62:5F:AF:24:99:2A:FE:77:F3:9D:61:FF:AA:3E:78:D4:7C:4A:3E:EE:22:28:B8:15:2C:15		**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The "HydrantID Root CA 1" root cert currently has two internally-operated intermediate certs: - HydrantID SSL ICA 1A -- issues OV and EV SSL certs - HydrantID Client ICA 1A -- issues Digital Signature and Code Signing certificates	**Verified?**	Verified	
Externally Operated SubCAs	None. None planned	**Verified?**	Verified	
Cross Signing	None. None planned.	**Verified?**	Verified	
Technical Constraint on 3rd party Issuer	No externally-operated subCAs. CPS section 1.2.2. Registration	**Verified?**	Verified	

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.

Verification Policies and Practices

Policy Documentation	HydrantID documents are available in English on their website.	**Verified?**	Verified
CA Document Repository	https://www.hydrantid.com/support/repository/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.hydrantid.com/wp-content/uploads/2015/06/HydrantID-Certificate-Policy-and-Certificate-Practices-Statement-v1-.0-6-9-2015.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.hydrantid.com/wp-content/uploads/2015/06/HydrantID-Certificate-Policy-and-Certificate-Practices-Statement-v1-.0-6-9-2015.pdf	**Verified?**	Verified
Other Relevant Documents	HydrantID Certificate Holder Agreement: https://www.hydrantid.com/wp-content/uploads/2013/07/HydrantID_Cert_Holder_Agreement-v2_7_8_13.pdf	**Verified?**	Verified
Auditor Name	BDO (Stone-Carlie)	**Verified?**	Verified
Auditor Website	https://www.bdo.com/ https://www.bdo.com/expansions/stone-carlie	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	NEED: URL to public-facing audit statement as per item #2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: URL to public-facing BR audit statement as per item #2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Please carefully review with your auditor: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type	WebTrust	**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	NEED: URL to public-facing EV audit statement as per item #2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
EV Audit Type	WebTrust	**Verified?**	Need Response From CA

EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	CPS section 1	**Verified?**	Verified
SSL Verification Procedures	NEED: the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber, as per item 3 of https://wiki.mozilla.org /CA:Information_checklist#Verification_Policies_and_Practices and https://wiki.mozilla.org /CA:BaselineRequirements#CA_Conformance_to_the_BRs "It is not sufficient to simply reference section 11 of the CA/Browser Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate."	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: I did not find the EV information in the CPS regarding what steps are taken to verify the organization, and identity and authority of the person acting on the organization's behalf.	**Verified?**	Need Response From CA
Organization Verification Procedures	NEED: I did not find in the CPS what steps are taken to verify the organization, and identity and authority of the person acting on the organization's behalf.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED: the sections of the CP/CPS documents that describe the procedures for verifying that the email address to be included in the certificate is owned/controlled by the certificate subscriber, as per item 4 of https://wiki.mozilla.org /CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Not requesting the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	HydrantID 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. CPS section 5.2.4 and 6.5	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.hydrantid.com/support /repository/	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	HydrantID Root CA 2	**Root Case No**	R00000089
Request Status	Need Information from CA	**Case Number**	00000065

Additional Root Case Information

	Subject	Include HydrantID Root CA 2		

Technical Information about Root Certificate

O From Issuer Field	HydrantID (Avalanche Cloud Corporation)	**Verified?**	Verified	
OU From Issuer Field		**Verified?**	Verified	
Certificate Summary	This SHA-512 root cert signs internally-operated intermediate certs that sign end-entity certs.	**Verified?**	Verified	
Root Certificate Download URL	http://crl.hydrantid.com/SSLICA2A/HIDROOT2.crt	**Verified?**	Verified	
Valid From	2015 May 21	**Verified?**	Verified	
Valid To	2039 May 21	**Verified?**	Verified	
Certificate Version	3	**Verified?**	Verified	
Certificate Signature Algorithm	SHA-512	**Verified?**	Verified	
Signing Key Parameters	4096	**Verified?**	Verified	
Test Website URL (SSL) or Example Cert	https://root2-ev-v.hydrantid.com/	**Verified?**	Verified	
CRL URL(s)	http://crl.hydrantid.com/SSLICA2A/HIDROOT2.crl http://crl.hydrantid.com/SSLICA2A/SSLICA2A.crl NextUpdate for CRLs of end-entity certs, CP/CPS: "(UTC format – thisUpdate plus 7 days)"	**Verified?**	Verified	
OCSP URL(s)	http://ocsp2.hydrantid.com OCSP Stapling is supported	**Verified?**	Verified	
Revocation Tested	http://certificate.revocationcheck.com/root2-ev-v.hydrantid.com results in no Errors	**Verified?**	Verified	
Trust Bits	Email; Websites	**Verified?**	Verified	
SSL Validation Type	OV; EV	**Verified?**	Verified	
EV Policy OID(s)	1.3.6.1.4.1.44058.0.1.1	**Verified?**	Verified	
EV Tested	// CN=HydrantID Root CA 2,O=HydrantID (Avalanche Cloud Corporation),C=US "1.3.6.1.4.1.44058.0.1.1", "HydrantID EV OID", SEC_OID_UNKNOWN, { 0x47, 0xD0, 0xA0, 0x78, 0x63, 0x62, 0x3C, 0x7D, 0xB9, 0x9C, 0x13, 0xA7, 0x36, 0x13, 0x4E, 0xC3, 0xE7, 0xC4, 0xBD, 0x93, 0x2D, 0xED, 0x87, 0xC9, 0x1A, 0xDA, 0x3D, 0x69, 0x49, 0x9D, 0xF2, 0x77 }, "MF0xCzAJBgNVBAYTAlVTMTAwLgYDVQQKEydIeWRyYW50SUQgKEF2YWxhbmNoZSBD" "bG91ZCBDb3Jwb3JhdGlvbikxHDAaBgNVBAMTE0h5ZHJhbnRJRCBSb290IENBIDI=" "", "I253pzQ1+6JD+2DJ3xXbBQ==", Success!	**Verified?**	Verified	
Root Stores Included In		**Verified?**	Verified	
Mozilla Applied Constraints	None	**Verified?**	Verified	

Digital Fingerprint Information

SHA-1 Fingerprint	F4:CC:B2:74:81:38:0E:6A:8C:43:50:41:80:9C:69:85:25:33:F4:F5	**Verified?**	Verified
SHA-256 Fingerprint	47:D0:A0:78:63:62:3C:7D:B9:9C:13:A7:36:13:4E:C3:E7:C4:BD:93:2D:ED:87:C9:1A:DA:3D:69:49:9D:F2:77	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The "HydrantID Root CA 2" root cert currently has one internally-operated intermediate cert: - HydrantID SSL ICA 2A -- issues OV and EV SSL certs	**Verified?**	Verified
Externally Operated SubCAs	None. None planned	**Verified?**	Verified
Cross Signing	None. None planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No externally-operated subCAs. CPS section 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.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	HydrantID documents are available in English on their website.	**Verified?**	Verified
CA Document Repository	https://www.hydrantid.com/support/repository/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.hydrantid.com/wp-content/uploads/2015/06/HydrantID-Certificate-Policy-and-Certificate-Practices-Statement-v1-.0-6-9-2015.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.hydrantid.com/wp-content/uploads/2015/06/HydrantID-Certificate-Policy-and-Certificate-Practices-Statement-v1-.0-6-9-2015.pdf	**Verified?**	Verified
Other Relevant Documents	HydrantID Certificate Holder Agreement: https://www.hydrantid.com/wp-content/uploads/2013/07/HydrantID_Cert_Holder_Agreement-v2_7_8_13.pdf	**Verified?**	Verified
Auditor Name	BDO (Stone-Carlie)	**Verified?**	Verified
Auditor Website	https://www.bdo.com/ https://www.bdo.com/expansions/stone-carlie	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified

Standard Audit	NEED: URL to public-facing audit statement as per item #2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: URL to public-facing BR audit statement as per item #2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Please carefully review with your auditor: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type	WebTrust	**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	NEED: URL to public-facing EV audit statement as per item #2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
EV Audit Type	WebTrust	**Verified?**	Need Response From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	CPS section 1	**Verified?**	Verified
SSL Verification Procedures	NEED: the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber, as per item 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices and https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs "It is not sufficient to simply reference section 11 of the CA/Browser Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate."	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: I did not find the EV information in the CPS regarding what steps are taken to verify the organization, and identity and authority of the person acting on the organization's behalf.	**Verified?**	Need Response From CA
Organization Verification Procedures	NEED: I did not find in the CPS what steps are taken to verify the organization, and identity and authority of the person acting on the organization's behalf.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED: the sections of the CP/CPS documents that describe the procedures for verifying that the email address to be included in the certificate is owned/controlled by the certificate subscriber, as per item 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Not requesting the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	HydrantID 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. CPS section 5.2.4 and 6.5	**Verified?**	Verified

| Network Security | CPS section 6.7 | | **Verified?** | Verified |

Link to Publicly Disclosed and Audited subordinate CA Certificates

| Publicly Disclosed & Audited subCAs | https://www.hydrantid.com/support /repository/ | **Verified?** | Verified |

Root Case Record # 3

Root Case Information

Root Certificate Name	HydrantID Root CA 3	Root Case No	R00000090
Request Status	Need Information from CA	Case Number	00000065

Additional Root Case Information

| Subject | Include HydrantID Root CA 3 |

Technical Information about Root Certificate

O From Issuer Field	HydrantID (Avalanche Cloud Corporation)	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This ECC root cert signs internally-operated intermediate certs that sign end-entity certs.	**Verified?**	Verified
Root Certificate Download URL	http://crl.hydrantid.com/SSLICA3A /HIDROOT3.crt	**Verified?**	Verified
Valid From	2015 May 21	**Verified?**	Verified
Valid To	2039 May 21	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	ECC	**Verified?**	Verified
Signing Key Parameters	ECC P-384	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://root3-ev-v.hydrantid.com	**Verified?**	Verified
CRL URL(s)	http://crl.hydrantid.com/SSLICA3A /HIDROOT3.crl http://crl.hydrantid.com/SSLICA3A /SSLICA3A.crl NextUpdate for CRLs of end-entity certs, CP/CPS: "(UTC format – thisUpdate plus 7 days)"	**Verified?**	Verified
OCSP URL(s)	OCSP: URI: http://ocsp3.hydrantid.com OCSP Stapling is supported	**Verified?**	Verified
Revocation Tested	http://certificate.revocationcheck.com /root3-ev-v.hydrantid.com results in no Errors	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.44058.0.1.1	**Verified?**	Verified

EV Tested	NEED: Successful output from https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version using the https://root3-ev-v.hydrantid.com test site.	**Verified?**	Need Response From CA
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	B7:69:02:A8:D2:A9:8C:44:FA:A6:55:19:E5:2C:CF:5A:BE:C1:DB:95	**Verified?**	Verified
SHA-256 Fingerprint	FB:63:29:F0:32:C1:3A:12:28:48:43:10:8C:B3:A8:72:17:23:18:E4:33:E9:68:24:B9:EF:0E:00:97:64:16:45	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The "HydrantID Root CA 3" root cert currently has one internally-operated intermediate cert: - HydrantID SSL ICA 3A -- issues OV and EV SSL certs	**Verified?**	Verified
Externally Operated SubCAs	None. None planned	**Verified?**	Verified
Cross Signing	None. None planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No externally-operated subCAs. CPS section 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.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	HydrantID documents are available in English on their website.	**Verified?**	Verified
CA Document Repository	https://www.hydrantid.com/support/repository/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.hydrantid.com/wp-content/uploads/2015/06/HydrantID-Certificate-Policy-and-Certificate-Practices-Statement-v1-.0-6-9-2015.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.hydrantid.com/wp-content/uploads/2015/06/HydrantID-Certificate-Policy-and-Certificate-Practices-Statement-v1-.0-6-9-2015.pdf	**Verified?**	Verified

Other Relevant Documents	HydrantID Certificate Holder Agreement: https://www.hydrantid.com/wp-content/uploads/2013/07/HydrantID_Cert_Holder_Agreement-v2_7_8_13.pdf	**Verified?**	Verified
Auditor Name	BDO (Stone-Carlie)	**Verified?**	Verified
Auditor Website	https://www.bdo.com/ https://www.bdo.com/expansions/stone-carlie	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	NEED: URL to public-facing audit statement as per item #2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: URL to public-facing BR audit statement as per item #2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Please carefully review with your auditor: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type	WebTrust	**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	NEED: URL to public-facing EV audit statement as per item #2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
EV Audit Type	WebTrust	**Verified?**	Need Response From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	CPS section 1	**Verified?**	Verified
SSL Verification Procedures	NEED: the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber, as per item 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices and https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs "It is not sufficient to simply reference section 11 of the CA/Browser Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate."	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: I did not find the EV information in the CPS regarding what steps are taken to verify the organization, and identity and authority of the person acting on the organization's behalf.	**Verified?**	Need Response From CA
Organization Verification Procedures	NEED: I did not find in the CPS what steps are taken to verify the organization, and identity and authority of the person acting on the organization's behalf.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED: the sections of the CP/CPS documents that describe the procedures for verifying that the email address to be included in the certificate is owned/controlled by the certificate	**Verified?**	Need Response From CA

	subscriber, as per item 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices		
Code Signing Subscriber Verification Pro	Not requesting the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	HydrantID 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. CPS section 5.2.4 and 6.5	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.hydrantid.com/support/repository/	**Verified?**	Verified