Mozilla - CA Program

Case Information

Case Number	00000063	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Amazon	**Request Status**	Need Information from CA

Additional Case Information

Subject	Include Amazon Root Certificates	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1172401

General information about CA's associated organization

CA Email Alias 1	aws-tsp-requests@amazon.com		
CA Email Alias 2			
Company Website	https://www.amazontrust.com/	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Global	**Verified?**	Verified
Primary Market / Customer Base	The Amazon PKI is run by Amazon Trust Services ("Amazon"). Customers of the Amazon PKI are the general public. We do not require that customers have a domain registration with Amazon, use domain suffixes where Amazon is the registrant, or have other services from Amazon.	**Verified?**	Verified
Impact to Mozilla Users	This application includes four new root CAs. It also includes one additional root CA already in the Mozilla program which we wish to have enabled for EV certificate issuance.	**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	Comment #9: We have reviewed the "Potentially problematic CA practices". We fully comply with the Mozilla CA program requirements, including complying with the CA/Browser Forum Guidelines.	**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	Comment #9: * Amazon allows externally operated subordinate CAs as documented in section 4.2.2 of the ATS CPS. * Third parties cannot directly cause the issuance of certificates from Amazon operated CAs.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Amazon Root CA 1	**Root Case No**	R00000083
Request Status	Need Information from CA	**Case Number**	00000063

Additional Root Case Information

Subject	Include Amazon Root CA 1 -- SHA-256

Technical Information about Root Certificate

O From Issuer Field	Amazon	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	The Amazon Root CAs will have internally-operated subordinate CAs that will issue certs for SSL, Code Signing, Email, etc. There will be separate subCAs for EV certificate issuance. Externally-operated subCAs are permitted according to the CPS.	**Verified?**	Verified
Root Certificate Download URL	https://www.amazontrust.com/repository/AmazonRootCA1.cer	**Verified?**	Verified
Valid From	2015 May 26	**Verified?**	Verified
Valid To	2038 Jan 17	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://good.sca1a.amazontrust.com/	**Verified?**	Verified
CRL URL(s)	http://crl.rootca1.amazontrust.com/rootca1.crl CP section 4.9.7: CRL issuing frequency for subscriber certificates is at least once every seven days	**Verified?**	Verified

OCSP URL(s)	http://ocsp.rootca1.amazontrust.com/ http://ocsp.sca1a.amazontrust.com CP section 4.9.10: OCSP responses from this service MUST have a maximum expiration time of ten days	**Verified?**	Verified
Revocation Tested	NEED: Resolve all errors listed here https://certificate.revocationcheck.com/good.sca1a.amazontrust.com (I'm getting timeout errors)	**Verified?**	Need Response From CA
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
EV Tested	// CN=Amazon Root CA 1,O=Amazon,C=US "2.23.140.1.1", "Amazon EV OID", SEC_OID_UNKNOWN, { 0x8E, 0xCD, 0xE6, 0x88, 0x4F, 0x3D, 0x87, 0xB1, 0x12, 0x5B, 0xA3, 0x1A, 0xC3, 0xFC, 0xB1, 0x3D, 0x70, 0x16, 0xDE, 0x7F, 0x57, 0xCC, 0x90, 0x4F, 0xE1, 0xCB, 0x97, 0xC6, 0xAE, 0x98, 0x19, 0x6E }, "MDkxCzAJBgNVBAYTAlVTMQ8wDQYDVQQKEwZBbWF6b24xGTAXBgNVBAMTEEFtYXpv" "biBSb290IENBIDE=", "Bmyfz5m/jAo54vB4ikPmljZbyg==", Success!	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	8D:A7:F9:65:EC:5E:FC:37:91:0F:1C:6E:59:FD:C1:CC:6A:6E:DE:16	**Verified?**	Verified
SHA-256 Fingerprint	8E:CD:E6:88:4F:3D:87:B1:12:5B:A3:1A:C3:FC:B1:3D:70:16:DE:7F:57:CC:90:4F:E1:CB:97:C6:AE:98:19:6E	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	We will have separate subordinate CAs to issue the following types of certificates: - Extended Validation Server Authentication - Code Signing - Other types of certificates as covered by our CP and CPS (including Server Authentication and Email Protection) We will not issue EV certificates from subordinates used to issue non-EV certificates and we will not issue code signing certificates from subordinates used to issue non-code signing certificates.	**Verified?**	Verified
Externally Operated SubCAs	Amazon allows externally operated subordinate CAs. CPS section 4.2.2: For Applications for a Subordinate CA where the Subordinate CA will not be controlled by Amazon, Amazon ensures that all the following are true: • The APPMA has approved the Subordinate CA	**Verified?**	Verified

	• There is a contract in place requiring the Subordinate CA to comply with CA/Browser Forum guidelines • The CA generated and stores its keys on a HSM that meets the requirements in the CP • The CA had the key generation audited by a qualified auditor. This is not required to be a WebTrust licensed auditor, but the auditor must meet items 1, 3, 6, and 7 of section 8.2 of the CP. • If the Subordinate CA certificate is not technically constrained, then the contract requires the Subordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application...		
Cross Signing	Yes. Starfield Services Root Certificate Authority - G2 issued a cross certificate with this root as the subject.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Third parties cannot directly cause the issuance of certificates from Amazon operated CAs. CPS section 4.2.2 regarding externally-operated subCAs: If the Subordinate CA certificate is not technically constrained, then the contract requires theSubordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application. Additionally, the CA must have WebTrust audits covering periods no longer than one year in duration where each audit period must immediately start after the previous period end with no gaps. Amazon will post links to Subordinate CA certificates, CP, CPS, and audit options (if applicable) in its repository.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation		**Verified?**	Verified
CA Document Repository	https://www.amazontrust.com/	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.amazontrust.com/repository/cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.amazontrust.com/repository/cps.pdf	**Verified?**	Verified
Other Relevant Documents	Subscriber Agreement: https://www.amazontrust.com/repository/sa-1.1.pdf	**Verified?**	Verified
Auditor Name	EY	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified

Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://www.amazontrust.com/repository/AWS_WebTrustforCA.pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/3/2015	**Verified?**	Verified
BR Audit	https://www.amazontrust.com/repository/AWS_WebTrustforBR.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/3/2015	**Verified?**	Verified
EV Audit	https://www.amazontrust.com/repository/AWS_WebTrustforEV.pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	6/3/2015	**Verified?**	Verified
BR Commitment to Comply	CP section 1.1.1, CPS section 1.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2 and CP section 3.2.2.4: Amazon uses the following methods to confirm that the Applicant has control of or right to use Domain Names: 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; or 2. Confirming authorization of the Certificate's issuance directly with the Domain Name Registrant using a Reliable Method of Communication verified by either (i) communication with the Domain Name Registrar or (ii) being listed as the contact information for "registrant", "technical", or "administrative" contacts listed in the WHOIS record for the Base Domain; or 3. Confirming authorization for the Certificate's issuance through an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; or 4. Relying upon a Domain Authorization Document that meets the requirements listed below; or 5. Having the Applicant demonstrate control over the FQDN or Base Domain by making an agreed-upon change ...	**Verified?**	Verified
EV SSL Verification Procedures	CP section 3.2	**Verified?**	Verified
Organization Verification Procedures	CP section 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2: Amazon uses the following methods to confirm the Applicant has control of or right to use Email Addresses:	**Verified?**	Verified

	1. Confirming authorization of the Certificate's issuance by contacting the requested email address, or 2. Confirming control of the FQDN in the Domain portion of the Email address using methods 1, 2, 5, 7, or 8 above.		
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit, because we plan to remove the Code Signing trust bit in the next version of Mozilla's CA Certificate Policy.	**Verified?**	Not Applicable
Multi-Factor Authentication	CP section 5.3.7 and 6.5.1.1	**Verified?**	Verified
Network Security	CP section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

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

Root Case Record # 2

Root Case Information

Root Certificate Name	Amazon Root CA 3	**Root Case No**	R00000084
Request Status	Need Information from CA	**Case Number**	00000063

Additional Root Case Information

Subject	Include Amazon Root CA 3 -- ECC P-256

Technical Information about Root Certificate

O From Issuer Field	Amazon	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	New root certificate that will sign intermediate certificates that will issue certs for SSL, Code Signing, Email, etc.	**Verified?**	Verified
Root Certificate Download URL	http://www.amazontrust.com/repository/AmazonRootCA3.cer	**Verified?**	Verified
Valid From	2015 May 26	**Verified?**	Verified
Valid To	2040 May 26	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	ECC	**Verified?**	Verified
Signing Key Parameters	ECC P-256	**Verified?**	Verified
Test Website URL (SSL) or Example	https://good.sca3a.amazontrust.com/	**Verified?**	Verified

Cert			
CRL URL(s)	http://crl.rootca3.amazontrust.com/rootca3.crl CP section 4.9.7: CRL issuing frequency for subscriber certificates is at least once every seven days	**Verified?**	Verified
OCSP URL(s)	http://ocsp.rootca3.amazontrust.com/ http://ocsp.sca3a.amazontrust.com CP section 4.9.10: OCSP responses from this service MUST have a maximum expiration time of ten days	**Verified?**	Verified
Revocation Tested	NEED: Resolve all errors listed here: https://certificate.revocationcheck.com/good.sca3a.amazontrust.com	**Verified?**	Need Response From CA
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
EV Tested	// CN=Amazon Root CA 3,O=Amazon,C=US "2.23.140.1.1", "Amazon EV OID", SEC_OID_UNKNOWN, { 0x18, 0xCE, 0x6C, 0xFE, 0x7B, 0xF1, 0x4E, 0x60, 0xB2, 0xE3, 0x47, 0xB8, 0xDF, 0xE8, 0x68, 0xCB, 0x31, 0xD0, 0x2E, 0xBB, 0x3A, 0xDA, 0x27, 0x15, 0x69, 0xF5, 0x03, 0x43, 0xB4, 0x6D, 0xB3, 0xA4 }, "MDkxCzAJBgNVBAYTAlVTMQ8wDQYDVQQKEwZBbWF6b24xGTAXBgNVBAMTEEFtYXpv" "biBSb290IENBIDM=", "Bmyf1XSXNmY/Owua2eiedgPySg==", Success!	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	0D:44:DD:8C:3C:8C:1A:1A:58:75:64:81:E9:0F:2E:2A:FF:B3:D2:6E	**Verified?**	Verified
SHA-256 Fingerprint	18:CE:6C:FE:7B:F1:4E:60:B2:E3:47:B8:DF:E8:68:CB:31:D0:2E:BB:3A:DA:27:15:69:F5:03:43:B4:6D:B3:A4	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	We will have separate subordinate CAs to issue the following types of certificates: - Extended Validation Server Authentication - Code Signing - Other types of certificates as covered by our CP and CPS (including Server Authentication and Email Protection) We will not issue EV certificates from subordinates used to issue non-EV certificates and we will not issue code signing certificates from subordinates used to issue non-code signing certificates.	**Verified?**	Verified
Externally Operated SubCAs	Amazon allows externally operated subordinate CAs. CPS section 4.2.2: For Applications for a	**Verified?**	Verified

	Subordinate CA where the Subordinate CA will not be controlled by Amazon, Amazon ensures that all the following are true: • The APPMA has approved the Subordinate CA • There is a contract in place requiring the Subordinate CA to comply with CA/Browser Forum guidelines • The CA generated and stores its keys on a HSM that meets the requirements in the CP • The CA had the key generation audited by a qualified auditor. This is not required to be a WebTrust licensed auditor, but the auditor must meet items 1, 3, 6, and 7 of section 8.2 of the CP. • If the Subordinate CA certificate is not technically constrained, then the contract requires the Subordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application...		
Cross Signing	Yes. Starfield Services Root Certificate Authority - G2 issued a cross certificate with this root as the subject.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Third parties cannot directly cause the issuance of certificates from Amazon operated CAs. CPS section 4.2.2 regarding externally-operated subCAs: If the Subordinate CA certificate is not technically constrained, then the contract requires theSubordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application. Additionally, the CA must have WebTrust audits covering periods no longer than one year in duration where each audit period must immediately start after the previous period end with no gaps. Amazon will post links to Subordinate CA certificates, CP, CPS, and audit options (if applicable) in its repository.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation		**Verified?**	Verified
CA Document Repository	https://www.amazontrust.com/	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.amazontrust.com/repository/cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.amazontrust.com/repository/cps.pdf	**Verified?**	Verified
Other Relevant Documents	Subscriber Agreement: https://www.amazontrust.com/repository/sa-1.1.pdf	**Verified?**	Verified

Auditor Name	EY	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://www.amazontrust.com/repository/AWS_WebTrustforCA.pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/3/2015	**Verified?**	Verified
BR Audit	https://www.amazontrust.com/repository/AWS_WebTrustforBR.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/3/2015	**Verified?**	Verified
EV Audit	https://www.amazontrust.com/repository/AWS_WebTrustforEV.pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	6/3/2015	**Verified?**	Verified
BR Commitment to Comply	CP section 1.1.1, CPS section 1.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2 and CP section 3.2.2.4: Amazon uses the following methods to confirm that the Applicant has control of or right to use Domain Names: 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; or 2. Confirming authorization of the Certificate's issuance directly with the Domain Name Registrant using a Reliable Method of Communication verified by either (i) communication with the Domain Name Registrar or (ii) being listed as the contact information for "registrant", "technical", or "administrative" contacts listed in the WHOIS record for the Base Domain; or 3. Confirming authorization for the Certificate's issuance through an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; or 4. Relying upon a Domain Authorization Document that meets the requirements listed below; or 5. Having the Applicant demonstrate control over the FQDN or Base Domain by making an agreed-upon change ...	**Verified?**	Verified
EV SSL Verification Procedures	CP section 3.2	**Verified?**	Verified
Organization Verification Procedures	CP section 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2: Amazon uses the following methods to confirm the Applicant has control of or right to use Email Addresses: 1. Confirming authorization of the Certificate's issuance by contacting the requested email address, or 2. Confirming control of the FQDN in the Domain portion of the Email address using methods 1, 2, 5, 7, or 8 above. Item 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Verified

Code Signing Subscriber Verification Pro	EV Code Signing Certs: CP section 3.2	**Verified?**	Not Applicable
Multi-Factor Authentication	CP section 5.3.7 and 6.5.1.1	**Verified?**	Verified
Network Security	CP section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

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

Root Case Record # 3

Root Case Information

Root Certificate Name	Amazon Root CA 2	**Root Case No**	R00000085
Request Status	Need Information from CA	**Case Number**	00000063

Additional Root Case Information

Subject	Include Amazon Root CA 2 -- SHA-384

Technical Information about Root Certificate

O From Issuer Field	Amazon	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	The Amazon Root CAs will have internally-operated subordinate CAs that will issue certs for SSL, Code Signing, Email, etc. There will be separate subCAs for EV certificate issuance. Externally-operated subCAs are permitted according to the CPS.	**Verified?**	Verified
Root Certificate Download URL	http://www.amazontrust.com/repository/AmazonRootCA2.cer	**Verified?**	Verified
Valid From	2015 May 26	**Verified?**	Verified
Valid To	2040 May 26	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-384	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://good.sca2a.amazontrust.com/	**Verified?**	Verified
CRL URL(s)	http://crl.rootca2.amazontrust.com/rootca2.crl CP section 4.9.7: CRL issuing frequency for subscriber certificates is at least once every seven days	**Verified?**	Verified

OCSP URL(s)	http://ocsp.rootca2.amazontrust.com/ http://ocsp.sca2a.amazontrust.com CP section 4.9.10: OCSP responses from this service MUST have a maximum expiration time of ten days	**Verified?**	Verified
Revocation Tested	NEED: Resolve all errors listed here: https://certificate.revocationcheck.com/good.sca2a.amazontrust.com	**Verified?**	Need Response From CA
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
EV Tested	// CN=Amazon Root CA 2,O=Amazon,C=US "2.23.140.1.1", "Amazon EV OID", SEC_OID_UNKNOWN, { 0x1B, 0xA5, 0xB2, 0xAA, 0x8C, 0x65, 0x40, 0x1A, 0x82, 0x96, 0x01, 0x18, 0xF8, 0x0B, 0xEC, 0x4F, 0x62, 0x30, 0x4D, 0x83, 0xCE, 0xC4, 0x71, 0x3A, 0x19, 0xC3, 0x9C, 0x01, 0x1E, 0xA4, 0x6D, 0xB4 }, "MDkxCzAJBgNVBAYTAlVTMQ8wDQYDVQQKEwZBbWF6b24xGTAXBgNVBAMTEEFtYXpv" "biBSb290IENBIDI=", "Bmyf0pY1hp8KD+WGePhbJruKNw==", Success!	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	5A:8C:EF:45:D7:A6:98:59:76:7A:8C:8B:44:96:B5:78:CF:47:4B:1A	**Verified?**	Verified
SHA-256 Fingerprint	1B:A5:B2:AA:8C:65:40:1A:82:96:01:18:F8:0B:EC:4F:62:30:4D:83:CE:C4:71:3A:19:C3:9C:01:1E:A4:6D:B4	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	We will have separate subordinate CAs to issue the following types of certificates: - Extended Validation Server Authentication - Code Signing - Other types of certificates as covered by our CP and CPS (including Server Authentication and Email Protection) We will not issue EV certificates from subordinates used to issue non-EV certificates and we will not issue code signing certificates from subordinates used to issue non-code signing certificates.	**Verified?**	Verified
Externally Operated SubCAs	Amazon allows externally operated subordinate CAs. CPS section 4.2.2: For Applications for a Subordinate CA where the Subordinate CA will not be controlled by Amazon, Amazon ensures that all the following are true: • The APPMA has approved the Subordinate CA	**Verified?**	Verified

	• There is a contract in place requiring the Subordinate CA to comply with CA/Browser Forum guidelines • The CA generated and stores its keys on a HSM that meets the requirements in the CP • The CA had the key generation audited by a qualified auditor. This is not required to be a WebTrust licensed auditor, but the auditor must meet items 1, 3, 6, and 7 of section 8.2 of the CP. • If the Subordinate CA certificate is not technically constrained, then the contract requires the Subordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application...		
Cross Signing	Yes. Starfield Services Root Certificate Authority - G2 issued a cross certificate with this root as the subject.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Third parties cannot directly cause the issuance of certificates from Amazon operated CAs. CPS section 4.2.2 regarding externally-operated subCAs: If the Subordinate CA certificate is not technically constrained, then the contract requires theSubordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application. Additionally, the CA must have WebTrust audits covering periods no longer than one year in duration where each audit period must immediately start after the previous period end with no gaps. Amazon will post links to Subordinate CA certificates, CP, CPS, and audit options (if applicable) in its repository.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation		**Verified?**	Verified
CA Document Repository	https://www.amazontrust.com/	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.amazontrust.com/repository/cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.amazontrust.com/repository/cps.pdf	**Verified?**	Verified
Other Relevant Documents	Subscriber Agreement: https://www.amazontrust.com/repository/sa-1.1.pdf	**Verified?**	Verified
Auditor Name	EY	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified

Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://www.amazontrust.com/repository/AWS_WebTrustforCA.pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/3/2015	**Verified?**	Verified
BR Audit	https://www.amazontrust.com/repository/AWS_WebTrustforBR.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/3/2015	**Verified?**	Verified
EV Audit	https://www.amazontrust.com/repository/AWS_WebTrustforEV.pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	6/3/2015	**Verified?**	Verified
BR Commitment to Comply	CP section 1.1.1, CPS section 1.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2 and CP section 3.2.2.4: Amazon uses the following methods to confirm that the Applicant has control of or right to use Domain Names: 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; or 2. Confirming authorization of the Certificate's issuance directly with the Domain Name Registrant using a Reliable Method of Communication verified by either (i) communication with the Domain Name Registrar or (ii) being listed as the contact information for "registrant", "technical", or "administrative" contacts listed in the WHOIS record for the Base Domain; or 3. Confirming authorization for the Certificate's issuance through an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; or 4. Relying upon a Domain Authorization Document that meets the requirements listed below; or 5. Having the Applicant demonstrate control over the FQDN or Base Domain by making an agreed-upon change ...	**Verified?**	Verified
EV SSL Verification Procedures	CP section 3.2	**Verified?**	Verified
Organization Verification Procedures	CP section 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2: Amazon uses the following methods to confirm the Applicant has control of or right to use Email Addresses:	**Verified?**	Verified

	1. Confirming authorization of the Certificate's issuance by contacting the requested email address, or 2. Confirming control of the FQDN in the Domain portion of the Email address using methods 1, 2, 5, 7, or 8 above.		
Code Signing Subscriber Verification Pro		**Verified?**	Not Applicable
Multi-Factor Authentication	CP section 5.3.7 and 6.5.1.1	**Verified?**	Verified
Network Security	CP section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

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

Root Case Record # 4

Root Case Information

Root Certificate Name	Amazon Root CA 4	**Root Case No**	R00000086
Request Status	Need Information from CA	**Case Number**	00000063

Additional Root Case Information

Subject	Include Amazon Root CA 4 -- ECC P-384

Technical Information about Root Certificate

O From Issuer Field	Amazon	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	The Amazon Root CAs will have internally-operated subordinate CAs that will issue certs for SSL, Code Signing, Email, etc. There will be separate subCAs for EV certificate issuance. Externally-operated subCAs are permitted according to the CPS.	**Verified?**	Verified
Root Certificate Download URL	http://www.amazontrust.com/repository/AmazonRootCA4.cer	**Verified?**	Verified
Valid From	2015 May 26	**Verified?**	Verified
Valid To	2040 May 26	**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://good.sca4a.amazontrust.com/	**Verified?**	Verified

CRL URL(s)	http://crl.rootca4.amazontrust.com/rootca4.crl CP section 4.9.7: CRL issuing frequency for subscriber certificates is at least once every seven days	**Verified?**	Verified
OCSP URL(s)	http://ocsp.rootca4.amazontrust.com/ http://ocsp.sca4a.amazontrust.com CP section 4.9.10: OCSP responses from this service MUST have a maximum expiration time of ten days	**Verified?**	Verified
Revocation Tested	NEED: Resolve all errors list here: https://certificate.revocationcheck.com/good.sca4a.amazontrust.com	**Verified?**	Need Response From CA
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
EV Tested	// CN=Amazon Root CA 4,O=Amazon,C=US "2.23.140.1.1", "Amazon EV OID", SEC_OID_UNKNOWN, { 0xE3, 0x5D, 0x28, 0x41, 0x9E, 0xD0, 0x20, 0x25, 0xCF, 0xA6, 0x90, 0x38, 0xCD, 0x62, 0x39, 0x62, 0x45, 0x8D, 0xA5, 0xC6, 0x95, 0xFB, 0xDE, 0xA3, 0xC2, 0x2B, 0x0B, 0xFB, 0x25, 0x89, 0x70, 0x92 }, "MDkxCzAJBgNVBAYTAlVTMQ8wDQYDVQQKEwZBbWF6b24xGTAXBgNVBAMTEEFtYXpv" "biBSb290IENBIDQ=", "Bmyf18G7EEwpQ+Vxe3ssyBrBDg==", Success!	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	F6:10:84:07:D6:F8:BB:67:98:0C:C2:E2:44:C2:EB:AE:1C:EF:63:BE	**Verified?**	Verified
SHA-256 Fingerprint	E3:5D:28:41:9E:D0:20:25:CF:A6:90:38:CD:62:39:62:45:8D:A5:C6:95:FB:DE:A3:C2:2B:0B:FB:25:89:70:92	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	We will have separate subordinate CAs to issue the following types of certificates: - Extended Validation Server Authentication - Code Signing - Other types of certificates as covered by our CP and CPS (including Server Authentication and Email Protection) We will not issue EV certificates from subordinates used to issue non-EV certificates and we will not issue code signing certificates from subordinates used to issue non-code signing certificates.	**Verified?**	Verified
Externally Operated SubCAs	Amazon allows externally operated subordinate CAs. CPS section 4.2.2: For Applications for a Subordinate CA where the Subordinate CA will not be controlled by Amazon,	**Verified?**	Verified

	Amazon ensures that all the following are true: • The APPMA has approved the Subordinate CA • There is a contract in place requiring the Subordinate CA to comply with CA/Browser Forum guidelines • The CA generated and stores its keys on a HSM that meets the requirements in the CP • The CA had the key generation audited by a qualified auditor. This is not required to be a WebTrust licensed auditor, but the auditor must meet items 1, 3, 6, and 7 of section 8.2 of the CP. • If the Subordinate CA certificate is not technically constrained, then the contract requires the Subordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application...		
Cross Signing	Yes. Starfield Services Root Certificate Authority - G2 issued a cross certificate with this root as the subject.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Third parties cannot directly cause the issuance of certificates from Amazon operated CAs. CPS section 4.2.2 regarding externally-operated subCAs: If the Subordinate CA certificate is not technically constrained, then the contract requires theSubordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application. Additionally, the CA must have WebTrust audits covering periods no longer than one year in duration where each audit period must immediately start after the previous period end with no gaps. Amazon will post links to Subordinate CA certificates, CP, CPS, and audit options (if applicable) in its repository.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation		**Verified?**	Verified
CA Document Repository	https://www.amazontrust.com/	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.amazontrust.com/repository/cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.amazontrust.com/repository/cps.pdf	**Verified?**	Verified
Other Relevant Documents	Subscriber Agreement: https://www.amazontrust.com/repository/sa-1.1.pdf	**Verified?**	Verified
Auditor Name	EY	**Verified?**	Verified

Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://www.amazontrust.com/repository/AWS_WebTrustforCA.pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/3/2015	**Verified?**	Verified
BR Audit	https://www.amazontrust.com/repository/AWS_WebTrustforBR.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/3/2015	**Verified?**	Verified
EV Audit	https://www.amazontrust.com/repository/AWS_WebTrustforEV.pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	6/3/2015	**Verified?**	Verified
BR Commitment to Comply	CP section 1.1.1, CPS section 1.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2 and CP section 3.2.2.4: Amazon uses the following methods to confirm that the Applicant has control of or right to use Domain Names: 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; or 2. Confirming authorization of the Certificate's issuance directly with the Domain Name Registrant using a Reliable Method of Communication verified by either (i) communication with the Domain Name Registrar or (ii) being listed as the contact information for "registrant", "technical", or "administrative" contacts listed in the WHOIS record for the Base Domain; or 3. Confirming authorization for the Certificate's issuance through an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; or 4. Relying upon a Domain Authorization Document that meets the requirements listed below; or 5. Having the Applicant demonstrate control over the FQDN or Base Domain by making an agreed-upon change ...	**Verified?**	Verified
EV SSL Verification Procedures	CP section 3.2	**Verified?**	Verified
Organization Verification Procedures	CP section 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2: Amazon uses the following methods to confirm the Applicant has control of or right to use Email Addresses: 1. Confirming authorization of the Certificate's issuance by contacting the requested email address, or 2. Confirming control of the FQDN in the Domain portion of the Email address using methods 1, 2, 5, 7, or 8 above. Item 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Verified

Code Signing Subscriber Verification Pro		**Verified?**	Not Applicable
Multi-Factor Authentication	CP section 5.3.7 and 6.5.1.1	**Verified?**	Verified
Network Security	CP section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

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

Root Case Record # 5

Root Case Information

Root Certificate Name	Starfield Services Root Certificate Authority - G2	**Root Case No**	R00000105
Request Status	Need Information from CA	**Case Number**	00000063

Additional Root Case Information

Subject	Enable EV for Starfield Services Root Certificate Authority - G2

Technical Information about Root Certificate

O From Issuer Field	Starfield Technologies, Inc.	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	Enable EV treatment for the "Starfield Services Root Certificate Authority - G2" certificate that was included via Bugzilla Bug #527056 when owned by GoDaddy. Ownership of this root changed in June 2015, and was witnessed and documented by auditors.	**Verified?**	Verified
Root Certificate Download URL	https://www.amazontrust.com/repository/SFSRootCAG2.cer	**Verified?**	Verified
Valid From	2009 Sep 01	**Verified?**	Verified
Valid To	2037 Dec 31	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://good.sca0a.amazontrust.com/	**Verified?**	Verified

CRL URL(s)	http://crl.rootg2.amazontrust.com/rootg2.crl CP section 4.9.7: CRL issuing frequency for subscriber certificates is at least once every seven days	**Verified?**	Verified
OCSP URL(s)	http://ocsp.rootg2.amazontrust.com http://ocsp.sca0a.amazontrust.com CP section 4.9.10: OCSP responses from this service MUST have a maximum expiration time of ten days	**Verified?**	Verified
Revocation Tested	NEED: Resolve all errors listed here: https://certificate.revocationcheck.com/good.sca0a.amazontrust.com	**Verified?**	Need Response From CA
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
EV Tested	// CN=Starfield Services Root Certificate Authority - G2,O="Starfield Technologies, Inc.",L=Scottsdale,ST=Arizona,C=US "2.23.140.1.1", "Amazon EV OID", SEC_OID_UNKNOWN, { 0x56, 0x8D, 0x69, 0x05, 0xA2, 0xC8, 0x87, 0x08, 0xA4, 0xB3, 0x02, 0x51, 0x90, 0xED, 0xCF, 0xED, 0xB1, 0x97, 0x4A, 0x60, 0x6A, 0x13, 0xC6, 0xE5, 0x29, 0x0F, 0xCB, 0x2A, 0xE6, 0x3E, 0xDA, 0xB5 }, "MIGYMQswCQYDVQQGEwJVUzEQMA4GA1UECBMHQXJpem9uYTETMBEGA1UEBxMKU2Nv" "dHRzZGFsZTElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLjE7" "MDkGA1UEAxMyU3RhcmZpZWxkIFNlcnZpY2VzIFJvb3QgQ2VydGlmaWNhdGUgQXV0" "aG9yaXR5IC0gRzI=", "AA==", Success!	**Verified?**	Verified
Root Stores Included In	Apple; Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	92:5A:8F:8D:2C:6D:04:E0:66:5F:59:6A:FF:22:D8:63:E8:25:6F:3F	**Verified?**	Verified
SHA-256 Fingerprint	56:8D:69:05:A2:C8:87:08:A4:B3:02:51:90:ED:CF:ED:B1:97:4A:60:6A:13:C6:E5:29:0F:CB:2A:E6:3E:DA:B5	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	We will have separate subordinate CAs to issue the following types of certificates: - Extended Validation Server Authentication - Code Signing - Other types of certificates as covered by our CP and CPS (including Server Authentication and Email Protection) We will not issue EV certificates from subordinates used to issue non-EV certificates and we will not issue code signing certificates from subordinates used to issue non-code signing certificates.	**Verified?**	Verified

Externally Operated SubCAs	Amazon allows externally operated subordinate CAs. CPS section 4.2.2: For Applications for a Subordinate CA where the Subordinate CA will not be controlled by Amazon, Amazon ensures that all the following are true: • The APPMA has approved the Subordinate CA • There is a contract in place requiring the Subordinate CA to comply with CA/Browser Forum guidelines • The CA generated and stores its keys on a HSM that meets the requirements in the CP • The CA had the key generation audited by a qualified auditor. This is not required to be a WebTrust licensed auditor, but the auditor must meet items 1, 3, 6, and 7 of section 8.2 of the CP. • If the Subordinate CA certificate is not technically constrained, then the contract requires the Subordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application...	**Verified?**	Verified
Cross Signing	Yes. Starfield Services Root Certificate Authority - G2 issued cross certificates with: - Amazon Root CA 1 (RSA key with a 2048 bit long modulus) - Amazon Root CA 2 (RSA key with a 4096 bit long modulus) - Amazon Root CA 3 (EC key on the NIST P-256 curve) - Amazon Root CA 4 (EC key on the NIST P-384 curve)	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Third parties cannot directly cause the issuance of certificates from Amazon operated CAs. CPS section 4.2.2 regarding externally-operated subCAs: If the Subordinate CA certificate is not technically constrained, then the contract requires theSubordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application. Additionally, the CA must have WebTrust audits covering periods no longer than one year in duration where each audit period must immediately start after the previous period end with no gaps. Amazon will post links to Subordinate CA certificates, CP, CPS, and audit options (if applicable) in its repository.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation		**Verified?**	Verified

CA Document Repository	https://www.amazontrust.com/	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.amazontrust.com/repository/cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.amazontrust.com/repository/cps.pdf	**Verified?**	Verified
Other Relevant Documents	Subscriber Agreement: https://www.amazontrust.com/repository/sa-1.1.pdf	**Verified?**	Verified
Auditor Name	EY	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://www.amazontrust.com/repository/SFSG2_WebTrustforCA.pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	8/28/2015	**Verified?**	Verified
BR Audit	https://www.amazontrust.com/repository/SFSG2_WebTrustforBR.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	8/28/2015	**Verified?**	Verified
EV Audit	https://www.amazontrust.com/repository/SFSG2_WebTrustforEV.pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	8/28/2015	**Verified?**	Verified
BR Commitment to Comply	CP section 1.1.1, CPS section 1.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2 and CP section 3.2.2.4: Amazon uses the following methods to confirm that the Applicant has control of or right to use Domain Names: 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; or 2. Confirming authorization of the Certificate's issuance directly with the Domain Name Registrant using a Reliable Method of Communication verified by either (i) communication with the Domain Name Registrar or (ii) being listed as the contact information for "registrant", "technical", or "administrative" contacts listed in the WHOIS record for the Base Domain; or 3. Confirming authorization for the Certificate's issuance through an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from	**Verified?**	Verified

	the requested FQDN; or 4. Relying upon a Domain Authorization Document that meets the requirements listed below; or 5. Having the Applicant demonstrate control over the FQDN or Base Domain by making an agreed-upon change ...		
EV SSL Verification Procedures	CP section 3.2	**Verified?**	Verified
Organization Verification Procedures	CP section 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2: Amazon uses the following methods to confirm the Applicant has control of or right to use Email Addresses: 1. Confirming authorization of the Certificate's issuance by contacting the requested email address, or 2. Confirming control of the FQDN in the Domain portion of the Email address using methods 1, 2, 5, 7, or 8 above.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit, because we plan to remove the Code Signing trust bit in the next version of Mozilla's CA Certificate Policy.	**Verified?**	Verified
Multi-Factor Authentication	CP section 5.3.7 and 6.5.1.1	**Verified?**	Verified
Network Security	CP section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

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