Bugzilla ID: 527056
Bugzilla Summary: Add Go Daddy CA Certs to root store
CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	Go Daddy Group, Inc.
Website URL	http://www.godaddy.com/
Organizational type	Commercial CA
Primary market / customer base	The Go Daddy Group is an ICANN-accredited domain registrar. They also provide hosting solutions, Web site creation tools, Secure SSL certificates, personalized email with spam and anti-phishing filtering, and e-commerce tools. The Go Daddy Group of companies also includes Wild West Domains, Inc., a reseller of domains and domain-related products and services; Domains By Proxy, a private registration service; Starfield Technologies, a research and development affiliate; and Blue Razor Domains, a membership-based discount registrar. Note: Starfield acquired the ValiCert Class 2 Policy Validation Authority from ValiCert, Inc. in June 2003.
CA Contact Information	CA Email Alias: practices@starfieldtech.com CA Phone Number: 480-505-8800 Title / Department: PKI operations

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**	**Data**	**Data**
Certificate Name	Go Daddy Root Certificate Authority - G2	Starfield Root Certificate Authority - G2	Starfield Services Root Certificate Authority - G2
Cert summary / comments	This new root will eventually replace the "Go Daddy Class 2 CA" root cert that is currently included in NSS. CPS: Second Generation (G2) Go Daddy Root CA. Serves as the "trust anchor" for the future Starfield PKI hierarchy for any certificates sold under the Go Daddy brand. Issues any future CAs for different types of PKI services sold under the Go Daddy rand.	This new root will eventually replace the "Starfield Class 2 CA" root cert that is currently included in NSS. CPS: Second Generation (G2) Starfield Root CA. Serves as the "trust anchor" for the future Starfield PKI hierarchy for any certificates other than those sold under the Go Daddy brand. Issues any future CAs for different types of PKI services except those used with the Go Daddy brand. Serves as a trusted root for time stamping certificates.	CPS: Reserved for future use. Comment #17: Regarding the future use, we may use this root to anchor new services such as S/MIME certificates, or services that are required by laws or standards to run under a distinct trust anchor.

Root Cert URL	https://certificates.godaddy.com/repository/gdroot-g2.crt	https://certificates.starfieldtech.com/repository/sfroot-g2.crt	https://certificates.starfieldtech.com/repository/sfsroot-g2.crt
SHA-1 fingerprint	47:BE:AB:C9:22:EA:E8:0E:78:78:34:62:A7:9F:45:C2:54:FD:E6:8B	B5:1C:06:7C:EE:2B:0C:3D:F8:55:AB:2D:92:F4:FE:39:D4:E7:0F:0E	92:5A:8F:8D:2C:6D:04:E0:66:5F:59:6A:FF:22:D8:63:E8:25:6F:3F
Valid from	2009-08-31	2009-08-31	2009-08-31
Valid to	2037-12-31	2037-12-31	2037-12-31
Cert Version	3	3	3
Modulus length	2048 (SHA-256)	2048 (SHA-256)	2048 (SHA-256)
Test Website	https://gdg2roottest.godaddy.com/	https://sfg2roottest.starfieldtech.com/	https://sfsg2roottest.starfieldtech.com/
	Note: No sub-CAs have yet been created for these roots, so the test certs are signed directly by the roots.		
CRL URL	http://crl.godaddy.com/gdroot-g2.crl	http://crl.starfieldtech.com/sfroot-g2.crl	http://crl.starfieldtech.com/sfsroot-g2.crl
CRL Issuance Frequency	CRLs for end-entity certs haven't been created yet because no sub-CA has been created. CPS section 4.4.9 CRL Issuance Frequency: Issuing CAs -- Every 7 days or less Comment #14: CRLs issued by subCAs that will generally contain entries for end-entity certificates are typically issued every 24 hours. This is the case with all of our currently operating subCAs. However we reserve the right to extend that up to a maximum of 7 days as specified in our CPS should it be required or desired in specific circumstances.		
OCSP Responder	http://ocsp.godaddy.com	http://ocsp.starfieldtech.com	http://ocsp.starfieldtech.com
OCSP Max Time	CPS section 4.4.11 Online Revocation/Status Checking Availability: Issuing CAs -- Every 4 days or less		
CA Hierarchy	Each root will sign at least one subordinate CA for issuing end-entity certificates. Comment #14: at this time we expect <the hierarchy under the new roots> will be very similar to the hierarchy of the current roots. At present, we do not expect to have any cross-certificates for the new roots. However, if we need or want to start making use of the newer root certificates before they have achieved a sufficient level of distribution amongst the installed base of various software products, we may elect to issue cross-certificates to the new roots from the existing Go Daddy and Starfield root CAs (but not the from the Valicert root). CA Hierarchy diagram of the roots currently included in NSS: https://bugzilla.mozilla.org/attachment.cgi?id=417535 (this diagram does NOT show the G2 roots; it shows the current CA hierarchy in operation today)		
3rd –Party Sub-CAs	None, and none planned.		
Cross-Signing	None, and none planned, unless needed for backwards compatibility.		
Requested Trust Bits	Websites (SSL/TLS) Code Signing	Websites (SSL/TLS) Code Signing	Websites (SSL/TLS) Code Signing
	Ideally we would request all trust bits. However, they make the point in the Email Address Ownership/Control section that we need to show documentation about our verification practices for email addresses. We do not currently have any such thing, as we have not been in the personal identity cert business(yet).		
SSL Validation Type DV, OV, and/or EV	Medium assurance certs: DV High assurance certs: OV Extended Validation certs: EV	Medium assurance certs: DV High assurance certs: OV Extended Validation certs: EV	Medium assurance certs: DV High assurance certs: OV

EV policy OID(s)	2.16.840.1.114413.1.7.23.3	2.16.840.1.114414.1.7.23.3	Not EV
CP/CPS	Repository of root and intermediate certs and policies: https://certificates.godaddy.com/repository CP and CPS: https://certs.starfieldtech.com/repository/StarfieldCP-CPS.pdf Relying Party Agreement: https://certs.starfieldtech.com/repository/StarfieldRelyingPartyAgreement.pdf Subscriber Agreement: https://certs.starfieldtech.com/repository/StarfieldSubscriberAgreement.pdf Premium EV Subscriber Agreement: https://certs.starfieldtech.com/repository/StarfieldEVSubscriberAgreement.pdf Code Signing Subscriber Agreement: https://certs.starfieldtech.com/repository/StarfieldCodeSigningCertificateSubscriberAgreement_1.0.pdf Extended Validation (EV) Certificate Documents Certified Public Account Letter: https://certs.starfieldtech.com/repository/AccountantLetterTemplate.pdf Verified Legal Opinion: https://certs.starfieldtech.com/repository/LegalOpinionTemplate.pdf Business Entity Attestation: https://certs.starfieldtech.com/repository/EV_Principal_Attestation_Starfield.pdf		
AUDIT	Audit Type: WebTrust CA and WebTrust EV Auditor: KPMG Auditor Website: www.kpmg.com Audit Report and Management's Assertions: https://cert.webtrust.org/SealFile?seal=355&file=pdf (2009.06.30) Both of these audit reports cover: Go Daddy Class 2 CA, Starfield Class 2 CA, and Starfield Services Root CA. The new, G2, version of these roots are not yet covered in an audit. Comment #12: Our annual audit cycle is roughly June to June. These new roots were created in September. They have not been covered under an official audit period. However, our WebTrust auditors were on site and present for the entirety of the root creation ceremony. We should be able to obtain some kind of letter/statement from KPMG attesting to the soundness of that procedure (if Mozilla requires such a thing).		
Organization Identity Verification	Comment #14: Medium (DV), High (OV) and EV assurance levels are all applicable CP/CPS section 3.1.8 Authentication of Organization Identity For High Assurance organizational Subscribers, Starfield verifies the following: • the organization name represents an organization currently registered with a government authority • the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application • the individual requesting the certificate is authorized to do so by the organization named in the certificate 3.1.9 Authentication of Individual Identity For High Assurance individual Subscribers, Starfield verifies the following: • the identity of the individual named in the certificate application • the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application In the case of a small business/sole proprietorship that is not registered with a government authority, Starfield will optionally include the entity's "doing business as" (DBA) name in an informational, unauthenticated "organizational unit" (OU) field.		

	3.1.10 Unified Communications Certificate Authentication The individual requesting the certificate is confirmed to have access to every fully qualified domain name included in the Subject Common Name or Subject Alternative Name fields of a UCC certificate. Only one Organization (as described in §3.1.8) or Individual (as described in §3.1.9) is authenticated for each High Assurance UCC certificate. 3.1.11 Medium Assurance Authentication For Medium Assurance Subscribers, Starfield verifies the following: • the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application 3.1.12 Authentication of Organization Identity for Extended Validation Certificates For Extended Validation Subscribers, Starfield verifies the following in accordance with the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates: • Legal Existence and Identity • Assumed Name (optional) • Physical Existence • Operational Existence (if records indicate that the organization is less than three years old) • Domain ownership or exclusive right to use • Name, title, and authority of contract signer, and certificate approver 3.1.14 Custom Certificate Authentication Starfield may issue certificates designed for use in a specific peer-to-peer application. These certificates are designed for use only in that application and steps are taken to ensure that they will not function for standard uses such as SSL or code signing.
Domain Name Ownership / Control	According to CPS sections 3.1.8, 3.1.9, and 3.1.11, for both Medium and High Assurance SSL certificates, Starfield verifies that the subscriber requesting the certificate has access to the domain name(s) that are specified in the certificate application. According to CPS section 3.1.12, for Extended Validation certificates, Starfield verifies “Domain ownership or exclusive right to use” in accordance with the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.
Email Address Ownership / Control	Not requesting the email trust bit at this time.
Identity of Code Signing Subscriber	CPS Section 9: Code Signing Certificate – a certificate issued to an organization for the purpose of digitally signing software CPS Section 3.1.13 Code Signing Certificate Authentication: For High Assurance Code Signing Subscribers, Starfield verifies the following: • the organization name represents an organization currently registered with a government Authority • the individual requesting the certificate is authorized to do so by the organization named in the certificate

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  o **Yes.** CPS section 7.1.4: One to ten years after Certificate issuance (depending on SSL certificate type).
	  o Comment #12: Our CPS permits up to 10 years. Indeed, we did issue 10 year DV certificates in the past. The CPS remains that way in order to cover those still-valid certificates. **We no longer issue 10-year certificates; the maximum lifetime we currently offer is 5 years.**
	• Wildcard DV SSL certificates
	  o **Yes for Medium assurance certs – Medium assurance certs are DV.**
	  o CPS section 7.1.4, medium assurance: CN = domain name of Subscriber's web site (may be fully qualified, wildcard, contain no periods, or IP address reserved for internal use)
	  o Comment #12: GoDaddy/Starfield do issue wildcard DV certificates.
	  o Comment #14: At present, there are no extra steps taken in the validation process of a wildcard DV certificate beyond that of a non-wildcard DV certificate. The debate over what level of risk actually exists from wildcard certificates is ongoing and certainly not decided. We believe that there are good measures that browsers can take, such as highlighting the actual domain portion in the address bar (highlighting "example.com" in the case of "paypal.example.com") that are very beneficial in helping end users determine which site they are actually visiting. We also do not believe that this is an issue unique to DV certificates.
	• Delegation of Domain / Email validation to third parties
	  o GoDaddy/Starfield does not delegate any validation duties. All vetting/verification/validation is performed by GoDaddy/Starfield.
	• Issuing end entity certificates directly from roots
	  o GoDaddy/Starfield does not issue subscriber certificates directly from root CAs. However, we do issue certificates directly from the roots for infrastructure purposes (OCSP responder certificates, timestamp authority certificates, and test certificates, such as the SSL test certificates used at the test URLs listed in this application).
	• Allowing external entities to operate unconstrained subordinate CAs
	  o GoDaddy/Starfield have not, and have no plans to, issue subordinate CA certificates to third parties.
	• Distributing generated private keys in PKCS#12 files
	  o As a policy, GoDaddy/Starfield do not ever generate or come into contact with subscriber private keys.
	• Certificates referencing hostnames or private IP addresses
	  o **Yes for Medium and High assurance certs**
	  o Comment #12: GoDaddy/Starfield currently do issue certificates to private IP addresses and non-fully-qualified hostnames if a subscriber so requests. All such requests are reviewed by a human RA prior to issuance.
	  o Comment #14: First, all requests (regardless of the name(s) being requested) are automatically screened through an extensive list of strings intended to flag any name that may be used in fraud, phishing, etc. In the case of non-TLD names, a human RA will further evaluate the name looking for any signs of homoglyph

	attacks or other visual issues with the name. For both non-TLD names and IP addresses, our process: 1) Verifies that the name or IP cannot be resolved/routed on the public Internet, and 2) Verifies that there are no signs of attempted fraud using both automated and manual methods. o CPS section 7.1.4, medium assurance: CN = domain name of Subscriber's web site (may be fully qualified, wildcard, contain no periods, or IP address reserved for internal use) o CPS section 7.1.4, high assurance: CN = domain name of Subscriber's web site (may be fully qualified, wildcard, contains no periods, or IP address reserved for internal use) o CPS section 7.1.4, EV: Certificates: CN = domain name of Subscriber's web site • OCSP Responses signed by a certificate under a different root o Test websites loaded without error into Firefox browser when OCSP enforced. AIA extension has OCSP. o Comment #12: All GoDaddy/Starfield CAs generate OCSP responses using a certificate that is issued directly by the CA for which responses are being generated. In other words, the "Go Daddy Root Certificate Authority - G2" directly issues an OCSP Response signing certificate, and that certificate is used in the OCSP responses for the "Go Daddy Root Certificate Authority - G2" (and likewise for our other CAs). • CRL with critical CIDP Extension o CRLs import into Firefox browser without error. • Generic names for CAs o The root cert names are not generic.