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 An email alias is requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. CA Phone Number: 480-505-8800 A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA. Title / Department: PKI operations If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?

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	Is the "Go Daddy Class 2 CA" root cert that is currently included in Mozilla/NSS the old version of this root?	Is the "Starfield Class 2 CA" root cert that is currently included in Mozilla/NSS the old version of this root?	The old version of this root was not included in Mozilla/NSS. Correct?

The root CA certificate URL	Please either attach the root certs to the bug, or provide the urls to them.		
SHA-1 fingerprint			
Valid from			
Valid to			
Cert Version			
Modulus length / key length			
Test Website	For each root: For testing purposes, please provide a URL to a website whose SSL cert chains up to this root. Note that this can be a test site.		
CRL URL	CRL URL?	CRL URL?	CRL URL?
CRL Issuance Frequency	CPS section 4.4.9 CRL Issuance Frequency: Issuing CAs -- Every 7 days or less		
OCSP Responder URL	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	For each root: Please provide a diagram and/or description of the CA hierarchy under this root. (or what it will be based on assumption of transition from old root to new root)		
Sub-CAs operated by 3rd parties	For each root: Does this root have any subordinate CAs that are operated by external third parties? For the subordinate CAs that are operated by third parties, please provide a general description and explain how the CP/CPS and audits ensure the third parties are in compliance. Also, see https://wiki.mozilla.org/CA:SubordinateCA_checklist Are any of the sub-CAs that are operated by third-parties are or will be EV enabled? If the answer is yes, then please refer to http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf section 7.b.1 and section 37b.		
cross-signing	For each root: List any other root CAs that have issued cross-signing certificates for this root CA		
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) ? Code Signing	Websites (SSL/TLS) Email (S/MIME) ? Code Signing	Websites (SSL/TLS) Email (S/MIME) ? Code Signing
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	?
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	These new roots are not referenced in the 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.
Organization Identity Verification	CP/CPS 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	Section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; If you intend to request enablement of the email trust bit for these roots: Please provide the specific document(s) and section or page numbers where the procedures are described for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber.
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	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information.
	• Long-lived DV certificates
	  o **CPS section 7.1.4: One to ten years after Certificate issuance (depending on SSL certificate type).**
	• 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)
	• Delegation of Domain / Email validation to third parties
	  o ?
	• Issuing end entity certificates directly from roots
	  o ?
	• Allowing external entities to operate unconstrained subordinate CAs
	  o ?
	• Distributing generated private keys in PKCS#12 files
	  o ?
	• Certificates referencing hostnames or private IP addresses
	  o **Yes for Medium and High assurance certs**
	  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 ?
	• CRL with critical CIDP Extension
	  o ?
	• Generic names for CAs
	  o No