Starfield Technologies, LLC

Certificate Policy
and
Certification Practice Statement
(CP/CPS)

Version 4.3
June 5, 2020

Table of Contents

1 INTRODUCTION

Starfield Technologies is an innovator in the field of Internet foundation services, providing advanced software and Internet solutions critical to the building of online presence and e-commerce.

The Starfield Public Key Infrastructure ("Starfield PKI") has been established to provide a variety of digital certificate services.

1.1 Overview

This Certificate Policy and Certification Practice Statement (CP/CPS) describes the practices of the Starfield PKI and applies to all Certification Authorities (CAs) within the Starfield PKI hierarchy. This CP/CPS is applicable to all entities with relationships with the Starfield PKI, including Policy Authorities (PAs), Certification Authorities (CAs), Registration Authorities (RAs), Subscribers, and Relying Parties.

The Starfield PKI conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document. The following policy identifiers are managed in accordance with these requirements: 2.23.140.1.2.1, 2.23.140.1.2.2, 2.23.140.1.2.3, and 2.23.140.1.1

The Starfield PKI conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

The Starfield PKI conforms to the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr. If there is any inconsistency between this document and those requirements, those requirements take precedence over this document. The following policy identifier is managed in accordance with these requirements: 2.23.140.1.4.1.

1.2 Document Name and Identification

This document is formally referred to as the "Starfield Certificate Policy and Certification Practice Statement" (Starfield CP/CPS). Starfield CAs issue certificates in accordance with the policy and practice requirements of this document.

The OID-arcs associated with this document are 2.16.840.1.114413 and 2.16.840.1.114414.

1.2.1 Document History

Version	Effective Date	Change Summary
3.12	August 15, 2017	• Added this changelog • Updated 3.3.9 to state that Starfield now relies on 3rd party data sources to identify high risk requests

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

		• Updated section 4.1.1 to confirm that Starfield now processes CAA records
3.12.2	November 9, 2017	• Corrected the 3.1.8 section to reference valid subsections
3.13	September 18, 2018	• Reformat to RFC 3647 Part 1
4.0	September 27, 2018	• Reformat to RFC 3647 Part 2
4.1	May 14, 2019	• Added text to sections 1.4 and 1.4.1 • Updated section 9.8
4.2	March 11, 2020	• Updated to reflect Mozilla Root Store requirements • Updated section 3.2
4.3	May 26, 2020	• Updated section 7.2 to show both versions of CRL

1.3 PKI Participants

This CP/CPS is applicable to all certificates issued by Starfield CAs within the Starfield PKI. This document defines the specific communities for which a specific class or type of certificate is applicable, specific Starfield PKI practices and requirements for the issuance and management of such certificates, and the intended purposes and uses of such certificates.

1.3.1 Certification Authorities

Starfield Certification Authorities (CAs) perform the following general functions:

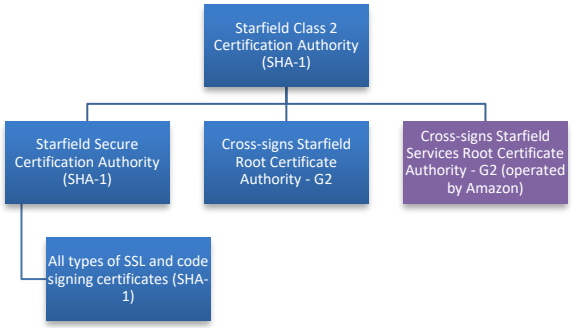
- Create and sign certificates
- Distribute certificates to the appropriate Subscribers and Relying Parties
- Revoke certificates
- Distribute certificate status information in the form of Certificate Revocation Lists (CRLs) or other mechanisms
- Provide a repository where certificates and certificate status information are stored and made available (if applicable).

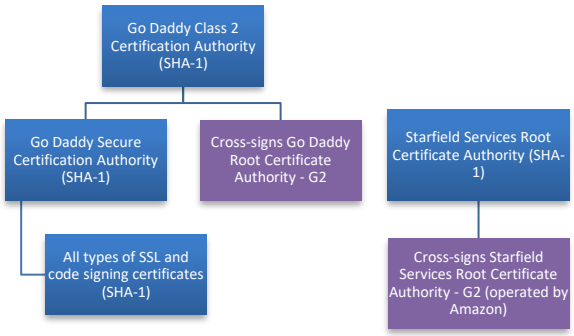
Obligations of the CAs within the Starfield PKI include:

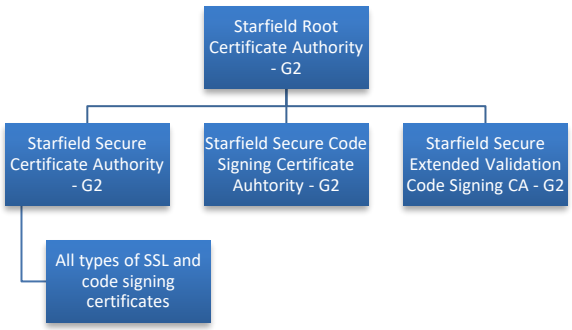
- Generating, issuing and distributing public key certificates
- Distributing CA certificates
- Generating and publishing certificate status information (such as CRLs)
- Maintaining the security, availability, and continuity of the certificate issuance and CRL signing functions
- Providing a means for Subscribers to request revocation
- Revoking public-key certificates
- Periodically demonstrating internal or external audited compliance with this CP/CPS.

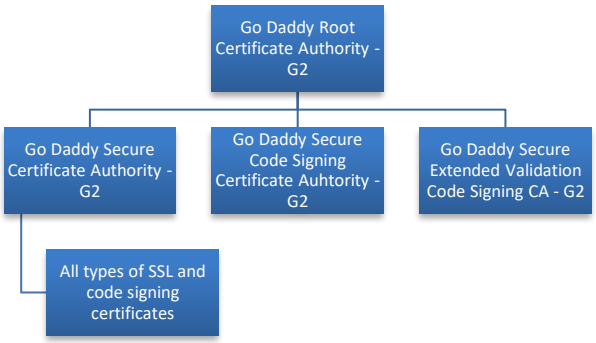
Within the Starfield PKI, there are two general types of CAs: Root and Issuing CAs. Currently, the Starfield PKI hierarchy consists of the CAs in the diagrams below. Relationships between these CA certificates are represented in the following diagrams:

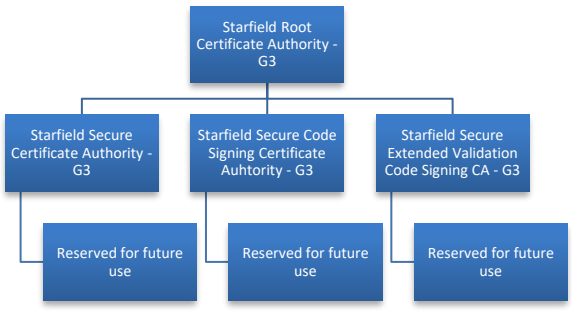
Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

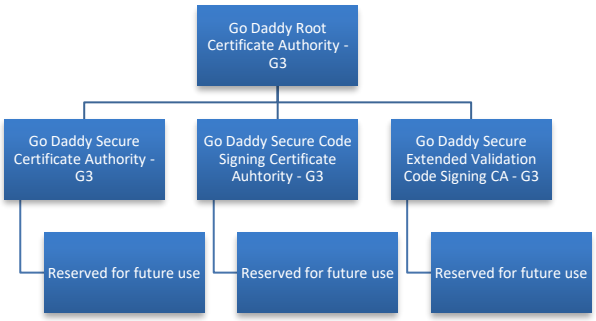




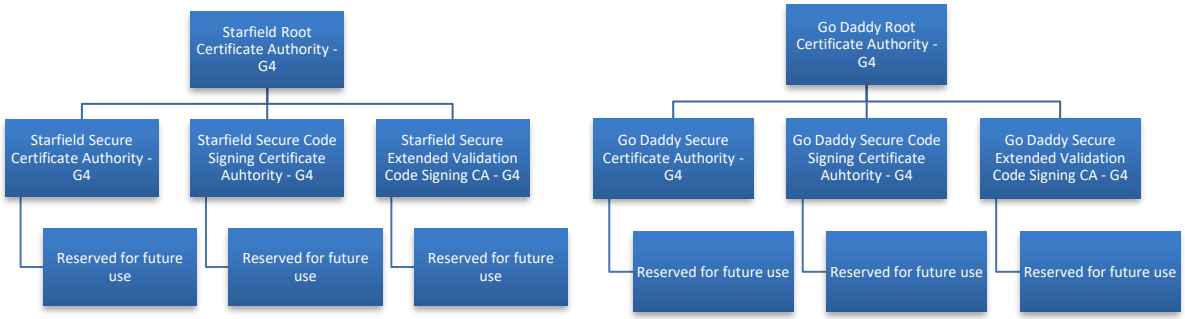








Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.



1.3.2 Registration Authorities

Registration Authorities (RAs) evaluate and either approve or reject Subscriber certificate management transactions (including certificate requests, renewal and re-key requests, and revocation requests). Starfield serves as the sole RA for the Starfield PKI.

Obligations of the Registration Authorities (RAs) within the Starfield PKI include:

- Obtaining a public-key from the Subscriber
- Identifying and authenticating Subscribers in accordance with this CP/CPS
- Verifying that the Subscriber possesses the asymmetric private key corresponding to the public-key submitted for certification
- Receiving, authenticating and processing certificate revocation requests
- Providing suitable training to personnel performing RA functions.

For the Starfield Root CAs the Subscribers are Subordinate CAs that are under the control of Starfield. Accordingly, the RA function for these CAs is performed manually by authorized Starfield PKI personnel.

For the Starfield Issuing CAs, the RA function is performed by Starfield using a combination of automated and manual processes.

1.3.3 Subscribers

For the Root CAs, the Subscribers include subordinate CAs. For Starfield Issuing CAs, Subscribers typically include organizations and individuals.

Obligations of Subscribers within the Starfield PKI include:

- Generating or causing to be generated one or more asymmetric key pairs
- Submitting public keys and credentials for registration

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- Providing information to the RA that is accurate and complete to the best of the Subscribers' knowledge and belief regarding information in their certificates and identification and authentication information
- Taking appropriate measures to protect their private keys from compromise
- Promptly reporting loss or compromise of private key(s) and inaccuracy of certificate information
- Using its key pair(s) in compliance with this CP/CPS.

1.3.4 Relying Parties

Relying Parties include any entity that may rely upon a Starfield certificate for purposes of determining the organizational or individual identity of an entity providing a web site, data encryption, digital signature verification, and user authentication.

Obligations of Relying Parties within the Starfield PKI include:

- Confirming the validity of Subscriber public-key certificates
- Verifying that Subscriber possesses the asymmetric private key corresponding to the public-key certificate (e.g., through digital signature verification)
- Using the public-key in the Subscriber's certificate in compliance with this CP/CPS.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

Starfield offers High Assurance Code Signing Certificates. Starfield offers TLS Certificates in the following levels of assurance:

Assurance Level	**Certificate Validation Type**
Basic and Medium Assurance	Domain Validation (DV)
High Assurance	Organization and Individual Validation (OV)
Extended Validation	Extended Validation (EV)

1.4.1 Appropriate Certificate Uses

A certificate issued by Starfield shall be used only as designated by the terms of this CP/CPS and any service agreements. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the associated risks before deciding on whether to rely on a Certificate issued under this CPS.

1.4.2 Prohibited Certificate Uses

As defined in the applicable Subscriber Agreement.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP/CPS is administered by the Starfield Governance and Policy Committee.

1.5.2 Contact Person

Starfield Technologies, LLC
14455 N. Hayden Road, Suite 219
Scottsdale, AZ 85260
Phone: 480-505-8800
E-mail: practices@starfieldtech.com

The Starfield Governance and Policy Committee consists of representatives from executive management, corporate security, PKI operations, and legal.

Obligations of the Starfield Governance and Policy Committee (GPC) include:

- Approving and maintaining this CP/CPS
- Interpreting adherence to this CP/CPS
- Specifying the content of public-key certificates
- Resolving or causing resolution of disputes related to this CP/CPS
- Remaining current regarding security threats and ensuring that appropriate actions are taken to counteract significant threats.

1.5.3 Person Determining CPS Suitability for the Policy

The Starfield Governance and Policy Committee determines the suitability of this CPS for the policy based on the results of independent audits.

1.5.4 CPS Approval Procedure

All changes to this document are approved by a quorum of The Starfield Governance and Policy Committee.

1.6 Definitions and Acronyms

- Applicant - the natural person or legal entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber.
- Applicant Representative - a natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- Attestation Letter - a letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
- Authorization Domain Name - the Domain Name used to obtain authorization for certificate issuance for a given FQDN.
- Authorized Port - one of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).
- Base Domain Name - the portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix.
- Basic Assurance – Starfield's vetting process that verifies access to the domain
- Baseline Requirements (BR) - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published by the CA/Browser Forum (http://www.cabforum.org)
- Certificate - digital record that contains information such as the Subscriber's distinguished name and public key, and the signer's signature and data
- Certificate Revocation List (CRL) – periodically published listing of all certificates that have been revoked for use by Relying Parties
- Certificate Signing Request (CSR) – a message sent to the certification authority containing the information required to issue a digital certificate
- Certification Authority (CA) – see 1.3.1
- Code Signing Certificate – a certificate issued to an organization for the purpose of digitally signing software
- Compromise - a loss, theft, disclosure, modification, unauthorized use, or other breach of security related to a Private Key
- Custom Certificate – a certificate profile defined for a specific, non-standard usage
- Distinguished Name (DN) – a globally unique identifier representing a Subscriber
- Domain Authorization Document - documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar attesting to the authority of an Applicant to request a Certificate for a specific domain namespace.
- Domain Contact - the Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record
- Domain Name - the label assigned to a node in the Domain Name System.
- Domain Name Registrant - sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- Domain Name Registrar: a person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
- Extended Validation (EV) – certificate issued under the Guidelines for the Issuance and Management of Extended Validation Certificates published by the CA/Browser Forum (http://www.cabforum.org)
- Fully-Qualified Domain Name (FQDN) - a Domain Name that includes the labels of all superior nodes in the Internet Domain Name System
- Governance and Policy Committee (GPC) – the Starfield committee which creates and maintains the policies related to the Starfield Public Key Infrastructure. Also known as the Policy Authority Committee (PAC)
- Hardware Security Module (HSM) –a specialized computer hardware system designed to securely store encryption keys
- High Assurance – Starfield's vetting process that verifies the identity of the individual or organization that requested the certificate and access to the domain
- Medium Assurance – Starfield's vetting process that verifies access to the domain
- Online Certificate Status Protocol (OCSP) – A standardized query/response protocol whereby a client can request the status of a given Certificate and be given a response that will indicate whether the Certificate is valid or revoked.
- Policy Authority Committee – See Governance and Policy Committee
- Private Key – a confidential encrypted electronic data file that interfaces with a Public Key using the same encryption algorithm, in order to verify Digital Signatures and encrypt files or messages
- Public Key – an encrypted electronic data file that is publicly available for interfacing with a Private Key
- Registration Authority (RA) – see 0
- Reliable Data Source - an identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
- Reliable Method of Communication - a method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
- Relying Party – an individual or entity that acts in reliance on a Certificate or digital signature associated with a Certificate
- Relying Party Agreement – an agreement which specifies the stipulations under which a person or organization acts as a Relying Party

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- Reseller – a person or organization which is given permission by Starfield to sell products to Subscribers
- Starfield – Starfield Technologies, LLC, and its resellers
- Starfield PKI - the Starfield Public Key Infrastructure that provides Certificates for individuals and entities.
- Subscriber – the individual or entity that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate
- Subscriber Agreement – an agreement which specifies the stipulations under which a person or organization acts as a Subscriber
- Subject Identity Information - information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.
- Unified Communications Certificate (UCC) – certificate that includes multiple fully qualified domain names in the Subject Alternative Name extension.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

In providing Repository services, obligations of the Starfield PKI include:

- Storing and distributing public-key certificates (where relevant)
- Storing and distributing certificate status information (such as CRLs and/or online certificate status)
- Storing and distributing this CP/CPS and subsequent updates.
- Storing and distributing the Relying Party and Subscriber agreements.

The Starfield Repository is located at http://www.starfieldtech.com/repository.

2.2 Publication of Certification Information

The Starfield repository shall contain the current and historical versions of this CP/CPS, a fingerprint of the Starfield Root CAs, current CRLs for the Starfield CAs, and other information relevant to Subscribers and Relying Parties.

2.3 Time or Frequency of Publication

This CP/CPS is updated and published on no less than an annual basis. CRLs and OCSP responses are published in accordance with 4.9.7 and 4.9.9.

2.4 Access Controls on Repositories

Read access to the Starfield repository is unrestricted. Write access to the repository is restricted to authorized Starfield PKI personnel through the use of appropriate logical access controls.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

All certificate holders require either a Distinguished Name in the Subject field that is in compliance with the X.500 standard for Distinguished Names, or a set of Subject Alternative Name values in the Subject Alternative Name extension. In the case where subject identity information is contained solely in the Subject Alternative Name extension, the Subject field of the certificate shall be empty. The Starfield PKI approves naming conventions for the creation of distinguished names and Subject Alternative Name values for certificate applicants.

The Issuer and Subject Distinguished Name fields for Certificates issued by Starfield are populated in accordance with 7.1.

3.1.2 Need for Names to be Meaningful

For Starfield PKI certificates that contain a Distinguished Name in the Subject field, said Distinguished Names shall be meaningful. For Starfield PKI certificates with an empty Subject field, any information contained in the Subject Alternative Name extension may or may not be meaningful depending on the type and intended use of the certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

For Internationalized Domain Names (IDNs), Starfield may include the Punycode representation of the name(s) in one or more Subject fields.

3.1.4 Rules for Interpreting Various Name Forms

Refer to Section 3.1.1

3.1.5 Uniqueness of Names

Refer to Sections 3.1.1 and 3.1.6.

3.1.6 Recognition, Authentication and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon others' Intellectual Property Rights. Starfield does not verify whether a Certificate Applicant has Intellectual Property rights in the name appearing in a Certificate Application nor does Starfield arbitrate, mediate, prosecute, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. Starfield may, without liability to any Certificate applicant, reject or suspend any Certificate application because of such dispute.

3.2 Initial Identity Validation

For Basic and Medium Assurance Domain Validated SSL Server Certificate Subscribers, Starfield verifies the following:

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application using the methods described in 3.2.2.4.

For High Assurance Organizational Validated SSL Server Certificate Subscribers, Starfield verifies the following:

- the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application using the methods described in 3.2.2.4.
- the individual requesting the certificate is authorized to do so by the organization named in the certificate using the methods described in 3.2.5
- the organization name represents an organization validated using the methods described in 3.2.2.

For High Assurance Code Signing Certificate Subscribers, Starfield verifies the following:

- the individual requesting the certificate is authorized to do so by the organization named in the certificate using the methods described in 3.2.5.
- the organization name represents an organization currently validated using the methods described in 3.2.2.

For Extended Validation SSL Server Certificate 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

3.2.1 Method to Prove Possession of Private Key

The Subscriber's certificate request must contain the public key to be certified and be digitally signed with the corresponding private key.

3.2.2 Authentication of Organization Identity

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, Starfield verifies the identity and address of the organization and that the address is the Applicant's address of existence or operation using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by Starfield or a third party who is acting as an agent for Starfield; or
4. An Attestation Letter.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Starfield may use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address, or Starfield may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification determined to be reliable.

3.2.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, Starfield verifies the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the Starfield determines to be reliable.

3.2.2.3 Verification of Country

If the subject:countryName field is present, then Starfield shall verify the country associated with the Subject using one of the following:

1. The IP Address range assignment by country for either
    a. The web site's IP address, as indicated by the DNS record for the web site, or
    b. The Applicant's IP address;
2. The ccTLD of the requested Domain Name;
3. Information provided by the Domain Name Registrar; or
4. A method identified in 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

Domain names included in the Subject Common Name or Subject Alternative Name fields of an End Entity Certificate may be fully qualified or wildcard. Wildcard certificates are validated in accordance with 3.2.2.6 of the Baseline Requirements.

Verification of domain name access is performed when a domain name is first requested for a certificate in a given customer account.

Verification of domain name access may be performed when a Subscriber requests the renewal of a certificate in accordance with 4.6 & 3.6.

In compliance with the CA / Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, for each Fully-Qualified Domain Name listed in a Certificate, Starfield confirms that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by using one or more of the following methods:

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

3.2.2.4.1 Validating the Applicant as a Domain Contact

For certificates issued prior to August 1, 2018 confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar by determining that the domain was registered using the same account as the certificate. (BR 3.2.2.4.1)

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Communicating a Random Value via email, fax, SMS, or postal mail to a Domain Contact and receiving a confirming response utilizing the Random Value to the request for approval. (BR 3.2.2.4.2)

3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. (BR 3.2.2.4.3)

Starfield will NOT perform validations using this method after May 31, 2019. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.

3.2.2.4.4 Constructed Email to Domain Contact

Communicating with the Domain's administrator by (i) using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value. (BR 3.2.2.4.4)

3.2.2.4.5 Domain Authorization Document

For certificates issued on or after August 1, 2018, this method is not used for validation.

3.2.2.4.6 Agreed-Upon Change to Website

Having the Applicant demonstrate practical control over the FQDN by placing a Random Value generated by Starfield on an online web page located at /.well-known/pki-validation/ on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port. (BR 3.2.2.4.6)

Starfield will NOT perform validations using this method after June 3, 2020. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.

3.2.2.4.7 DNS Change

Having the Applicant demonstrate practical control over the FQDN by confirming the presence of a Random Value generated by Starfield in a DNS TXT or CAA record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character. (BR 3.2.2.4.7)

3.2.2.4.8 IP Address

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

No IP address certificates are issued under this CPS.

3.2.2.4.9 Test Certificate

Starfield does not validate domain authorization or control by confirming presence of a Test Certificate. The URL's for test sites can be found in the table below.

CA	Valid	Revoked	Expired
GoDaddy	https://valid.gdi.catest.godaddy.com	https://revoked.gdi.catest.godaddy.com	https://expired.gdi.catest.godaddy.com
GoDaddy - G2	https://valid.gdig2.catest.godaddy.com	https://revoked.gdig2.catest.godaddy.com	https://expired.gdig2.catest.godaddy.com
GoDaddy - G3	https://valid.gdig3.catest.godaddy.com	https://revoked.gdig3.catest.godaddy.com	https://expired.gdig3.catest.godaddy.com
GoDaddy - G4	https://valid.gdig4.catest.godaddy.com	https://revoked.gdig4.catest.godaddy.com	https://expired.gdig4.catest.godaddy.com
Starfield	https://valid.sfi.catest.starfieldtech.com	https://revoked.sfi.catest.starfieldtech.com	https://expired.sfi.catest.starfieldtech.com
Starfield - G2	https://valid.sfig2.catest.starfieldtech.com	https://revoked.sfig2.catest.starfieldtech.com	https://expired.sfig2.catest.starfieldtech.com
Starfield - G3	https://valid.sfig3.catest.starfieldtech.com	https://revoked.sfig3.catest.starfieldtech.com	https://expired.sfig3.catest.starfieldtech.com
Starfield - G4	https://valid.sfig4.catest.starfieldtech.com	https://revoked.sfig4.catest.starfieldtech.com	https://expired.sfig4.catest.starfieldtech.com
Starfield Services			https://expired.sfs.catest.starfieldtech.com

3.2.2.4.10 TLS Using a Random Number

This method of domain validation is not used.

3.2.2.4.11 Any Other Method

This method of domain validation is not used.

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant is the Domain Name Contact directly with the Domain Name Registrar by determining that the domain was registered using the same account as the certificate. (BR 3.2.2.4.12)

3.2.2.4.13 Email to DNS CAA Contact

This method of domain validation is not used.

3.2.2.4.14 Email to DNS TXT Contact

This method of domain validation is not used.

3.2.2.4.15 Phone Contact with Domain Contact

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, Starfield MAY request to be transferred to the Domain Contact.

In the event of reaching voicemail, Starfield may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to Starfield approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, Starfield MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. (BR 3.2.2.4.15)

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

This method of domain validation is not used.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

This method of domain validation is not used.

3.2.2.4.18 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and
Starfield MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

MUST be located on the Authorization Domain Name, and
MUST be located under the "/.well-known/pki-validation" directory, and
MUST be retrieved via either the "http" or "https" scheme, and
MUST be accessed over an Authorized Port.

If Starfield follows redirects the following apply:

Redirects MUST be initiated at the HTTP protocol layer (e.g. using a 3xx status code).
Redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.
Redirects MUST be to resource URLs with either via the "http" or "https" scheme.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

Starfield MUST provide a Random Value unique to the certificate request.
The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, Starfield MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. (BR 3.2.2.4.18)

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.

Starfield MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The token (as defined in RFC 8555, section 8.3) MUST NOT be used for more than 30 days from its creation.

If Starfield follows redirects:

Redirects MUST be initiated at the HTTP protocol layer (e.g. using a 3xx status code).
Redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.
Redirects MUST be to resource URLs with either via the "http" or "https" scheme.
Redirects MUST be to resource URLs accessed via Authorized Ports.

Note: Once the FQDN has been validated using this method, Starfield MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. (BR 3.2.2.4.19)

3.2.2.5 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, Starfield evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. Starfield considers the following during its evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Databases maintained by Starfield, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this section.

3.2.3 Authentication of Individual Identity

For High Assurance Individual Subscribers, Starfield verifies the following:

- the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application using the methods described in 3.2.2.4.
- the identity of the individual named in the certificate application using the following methods:

    - Starfield verifies the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type).
    - Starfield verifies the Applicant's address using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement.
    - Starfield verifies the certificate request with the Applicant using a Reliable Method of Communication.

3.2.4 Non-verified Subscriber Information

Not applicable.

3.2.5 Validation of Authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, Starfield uses a Reliable Method of Communication including email, telephone, and postal services to verify the authenticity of the Applicant Representative's certificate request. Using a Reliable Method of Communication, Starfield establishes the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, Starfield has a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then Starfield does not accept any certificate requests that are outside this specification. Starfield will provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation

Refer to Section 10.3 for all cross certificates that identify the CA as the Subject.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Subscriber requests for routine re-key are authenticated using a shared secret.

3.3.2 Identification and Authentication for Re-key After Revocation

The process for re-key after revocation of a Subscriber certificate is complete re-enrollment, which requires the generation of a new Subscriber key pair and the re-performance of the initial Subscriber identification and authentication procedures specified in 3.2.

3.4 Identification and Authentication for Revocation Request

Subscriber certificate revocation requests may be submitted by the Subscriber via an online certificate revocation request page. Such requests are authenticated using a shared secret.

If the revocation request cannot be authenticated using a shared secret, the RA must perform sufficient procedures to authenticate the revocation request in accordance with Starfield's revocation request processing procedures.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Certificate applications must include all information required by the relevant Starfield certificate application form.

4.1.1 Who Can Submit a Certificate Application

Either the Applicant or an authorized Certificate Requestor may submit certificate requests.

Starfield maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns and uses this information to identify subsequent suspicious certificate requests.

4.1.2 Enrollment Process and Responsibilities

Enrollment requires a completed certificate request, acceptance or execution of a Subscriber Agreement, and a Certificate Signing Request (CSR) containing the public key to be signed.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

When a certificate application is received, Starfield performs the validation required for the type of certificate in question as described in 3.2.

Prior to issuing a certificate, Starfield processes RFC 6844 Certificate Authority Authorization (CAA) records for each FQDN in the certificate according to the requirements defined in the

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. Starfield recognizes the following set of issuer domain names in CAA "issue" or "issuewild" records as permitting certificate issuance:

- godaddy.com
- starfieldtech.com

Starfield will only use documents and data to verify certificate information that is in accordance with the maximum time permitted for reuse as per the Baseline Requirements (BR) and the Guidelines for the Issuance and Management of Extended Validation Certificates.

Starfield relies on internal and 3rd party data to identify high risk Certificate requests prior to the Certificate's approval and denies these requests and/or subjects them to additional verification procedures.

Internationalized Domain Names (IDNs) containing mixed character sets within a label are subjected to additional verification procedures.

4.2.2 Approval or Rejection of Certificate Applications

Starfield will reject any certificate application that cannot be verified. Starfield may also reject a certificate application if Starfield believes that issuing the Certificate could damage or diminish Starfield's reputation or business.

Starfield enforces separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate.

4.2.3 Time to Process Certificate Applications

If domain validation is not completed within 45 days from certificate request, the certificate application is rejected. The RA can choose to extend this timeframe on an individual basis.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Certificates are generated, issued and published only after the RA performs the required identification and authentication steps in accordance with 4.2.1 and 3.2.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Subscribers are notified of issuance via email or API methods.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

A Subscriber's receipt of a certificate and subsequent use of the key pair and certificate constitute certificate acceptance. By accepting a certificate, the Subscriber:

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- Agrees to be bound by the continuing responsibilities, obligations and duties imposed by this CP/CPS,
- Agrees to be bound by the Subscribing Party agreement, and
- Represents and warrants that to its knowledge no unauthorized person has had access to the private key associated with the certificate, and
- Represents and warrants that the certificate information it has supplied during the registration process is truthful and has been accurately and fully published within the certificate.

4.4.2 Publication of the Certificate by the CA

CA certificates are published in the Starfield repository.

All SSL certificates are published in one or more publicly accessible Certificate Transparency (CT) logs.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber obligations for protection of private keys and usage restrictions are listed in the relevant Starfield Subscriber Agreement.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Party obligations for verification of public keys and usage restrictions are listed in the Starfield Relying Party Agreement.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Certificate renewal, defined as the process whereby a new certificate with an extended validity period is created for an existing Distinguished Name, is permitted for CA Certificates.

4.6.2 Who May Request Renewal

Either the Applicant or an authorized Certificate Requestor may submit renewal requests.

Starfield maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns and uses this information to identify subsequent suspicious certificate requests.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

4.6.3 Processing Certificate Renewal Requests

Subscribers are permitted to reuse a previous certificate request to replace an expiring or expired Certificate. Where the Subscriber holds a Certificate and the initial Subscriber identification and authentication process (as described in 3.2) has been performed within the maximum time permitted for reuse as per the Baseline Requirements (BR) and the Guidelines for the Issuance and Management of Extended Validation Certificates, Starfield may authenticate a renewal certificate request using a shared secret. Starfield will require re-verification and if Starfield believes that the information has become inaccurate.

4.6.4 Notification of New Certificate Issuance to Subscriber

Subscribers are notified of issuance via email or API methods.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As described in 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

As described in 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

Subscribers are permitted to submit an unlimited number of requests to re-key any valid Certificate during the validity period of the Certificate. After re-keying a Certificate, Starfield may revoke the old Certificate in up to 72 hours.

4.7.2 Who May Request Certification of a New Public Key

Starfield, the Applicant, or an authorized Certificate Requestor may submit re-key requests.

4.7.3 Processing Certificate Re-keying Requests

Re-key requests generally follow the process used for renewals (as described in 4.6.3).

4.7.4 Notification of New Certificate Issuance to Subscriber

Subscribers are notified of issuance via email or API methods.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As described in 4.4.1.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

4.7.6 Publication of the Re-keyed Certificate by the CA

As described in 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.8 Certificate Modification

Starfield defines certificate modification as the issuance of a new certificate with some change to information contained in the certificate such as the addition or removal of a SAN.

4.8.1 Circumstance for Certificate Modification

Subscribers are permitted to request an unlimited number of modifications to any valid Certificate during the validity period of the Certificate.

4.8.2 Who May Request Certificate Modification

Starfield, the Subscriber, or an authorized Certificate Requestor may request modification.

4.8.3 Processing Certificate Modification Requests

Modification requests generally follow the process used for renewals (as described in 4.6.3).

4.8.4 Notification of New Certificate Issuance to Subscriber

Subscribers are notified of issuance via email or API methods.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As described in 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

As described in 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.9 Certificate Revocation and Suspension

Starfield supports certificate revocation for all Starfield CAs. Starfield does not support certificate suspension.

4.9.1 Circumstances for Revocation

A certificate may be revoked under any or all of the following circumstances:

- The Subscriber or authorized Reseller on behalf of the Subscriber requests certificate revocation in accordance with 4.9.3.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- The certificate subject can be shown to have violated the stipulations of this CP/CPS, or compromise the security or integrity of the Starfield PKI.
- The Subscriber can be shown to have violated the stipulations of the Subscriber Agreement.
- Compromise of the Subscriber's private key is known or suspected.
- The authenticated organization or individual name in the Subject field of the Subscriber's certificate changes before the certificate expires.
- The Subscriber fails to pay any invoice from Starfield within forty-five (45) days of receiving it.

4.9.2 Who Can Request Revocation

Subscriber certificate revocation can be initiated by the Subscriber, Starfield, or authorized Resellers.

4.9.3 Procedure for Revocation Request

Starfield maintains a continuous 24x7 ability to accept and respond to revocation requests and related inquiries. Subscribers can perform certificate revocation requests via their online account. These requests are authenticated using a shared secret or in accordance with Starfield's revocation request processing procedures.

For reporting suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other type of suspicious activity with a certificate, contact Starfield at practices@starfieldtech.com.

4.9.4 Revocation Request Grace Period

Starfield validates automated revocation requests (i.e., where a shared secret is correctly provided) on receipt. Starfield commences the validation of non-automated revocation requests within one business day of receipt.

Starfield immediately processes authenticated revocation requests. A certificate's revoked status is reflected on a CRL and in an OCSP response published at intervals specified below. Revoked certificates are listed in the CRL and in OCSP responses until the certificate expires, with the exception of Code Signing certificates which are retained on the CRL and in OCSP responses for 20 years after the latter of certificate revocation or expiration.

4.9.5 Time Within Which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, Starfield will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, Starfield will work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which Starfield will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1. The date selected by Starfield will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
5. Relevant legislation.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties are required to check certificate status using the applicable CRL and/or OCSP before relying upon a certificate.

4.9.7 CRL Issuance Frequency

CRLs for Starfield CAs are issued in accordance with the following table.

CA Type	CRL Publication Frequency
Root CAs	Every 365 days or less and upon certificate revocation
Issuing CAs	Every 7 days or less

4.9.8 Maximum Latency for CRLs (if applicable)

No Stipulation.

4.9.9 On-line Revocation/Status Checking Availability

Relying Parties are required to check certificate status using the applicable CRL and/or OCSP before relying upon a certificate.
OCSP responses conform to RFC6960 and/or RFC5019. OCSP responses either:
1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-line Revocation Checking Requirements

OCSP responses for Starfield CAs are issued in accordance with the following table.

CA Type	OCSP Update Frequency
Root CAs	Every 365 days or less and upon certificate revocation if OCSP is enabled for the Root CA

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

CA Type	OCSP Update Frequency
Issuing CAs	Every 4 days or less

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder does not respond with a "good" status.

4.9.11 Other Forms of Revocation Advertisements Available

Starfield does not require OCSP stapling.

4.9.12 Special Requirements Regarding Key Compromise

There is no deviation from the certificate revocation procedures specified above when the revocation of a Subscriber certificate is due to private key compromise.

In addition to the procedures specified above, if deemed necessary, Starfield uses commercially reasonable efforts to notify potential Relying Parties if Starfield discovers, or has reason to believe, that there has been a compromise of a Starfield CA private key.

4.9.13 Circumstances for Suspension

We do not perform certificate suspension.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Starfield publishes certificate status information via CRL and OCSP. Revocation entries remain on the CRL and OCSP responses until after the certificate’s expiration date.

Starfield published both full master CRLs and partitioned CRLs. URLs to partitioned CRLs are included in the certificate and master CRLs are published on the Starfield repository.

4.10.2 Service Availability

Starfield’s CRL and OCSP services incorporate a distributed design intended to provide 24x7 availability.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

The Starfield PKI allows Subscribers, Relying Parties, Application Software Vendors, and other third parties to report complaints or suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates via email as published in the Starfield repository.

Starfield maintains a continuous 24/7 ability to respond to any high priority certificate problem reports and to revoke certificates in accordance with 4.9 and/or report the problem to law enforcement officials.

4.10.3 Optional Features

No Stipulation.

4.11 End of Subscription

No Stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The escrow of CA and Subscriber private keys, for purposes of access by law enforcement or any other reason, is not supported by the Starfield PKI.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No Stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

Starfield PKI systems are hosted and managed using secure facilities in the Phoenix, Arizona and Ashburn, Virginia metropolitan areas with multiple levels of physical access controls.

5.1.2 Physical Access

Production Starfield PKI systems are housed in a secure facility requiring two factor authentication and dual control access to any physical device in the CA environment. Physical access to the CA facility is automatically logged and video recorded on a 24x7 basis. Physical access to the CA facility is monitored 24x7 by onsite security personnel.

5.1.3 Power and Air Conditioning

The supply of power to Starfield CA systems is protected through the use of UPS systems and generators. Climate control systems have been implemented to ensure that the temperature within the CA facility is maintained within reasonable operating limits.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

5.1.4 Water Exposures

The CA hosting facilities have been verified to reside outside of any designated 100-year flood plain.

5.1.5 Fire Prevention and Protection

The Starfield CA hosting facility is equipped with a smoke detection system and a pre-action dry pipe fire suppression system.

5.1.6 Media Storage

Media containing production software, production data, and system audit information is stored secured with appropriate physical and logical access controls designed to limit access to authorized personnel.

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Other waste is disposed of in accordance with Starfield's normal waste disposal requirements.

5.1.8 Offsite Backup

Offsite backup media are stored in a physically secure manner using a bonded third-party storage facility.

Cryptographic devices, smart cards, and other devices that may contain private keys or keying material are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal.

5.2 Procedural Controls

5.2.1 Trusted Roles

All Starfield personnel involved in the operation of the Starfield PKI are considered to serve in "trusted roles." Within the Starfield PKI, the following trusted roles exist:

- ***Security***, responsible for establishing and monitoring compliance with security policies, procedures, and standards.
- ***Engineering/Architecture***, responsible for the design and development of Starfield PKI systems.
- ***PKI Operations***, responsible for administering, maintaining and monitoring the systems supporting the Starfield PKI.
- ***Key Management***, responsible for management of cryptographic materials.
- ***RA Operations***, responsible for processing certificate requests and revocation requests.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

5.2.2 Number of Persons Required Per Task

Cryptographically sensitive operations within the Starfield PKI such as CA key generation, CA key recovery, CA key activation and CA system configuration require the participation of multiple "trusted" individuals in accordance with 6.2.2. Other operations may require only one trusted individual.

5.2.3 Identification and Authentication for Each Role

Each person performing a trusted role within the Starfield PKI must be authorized by management to perform such functions and must satisfy the personnel requirements specified in 5.3.

5.2.4 Roles requiring separation of duties

Approval of EV certificate requests must be performed by a person other than the one who verified the information in the request.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The recruitment and selection practices for Starfield PKI personnel take into account the background, qualifications, experience, and clearance requirements of each position, which are compared against the profiles of potential candidates.

5.3.2 Background Check Procedures

Background checks are performed prior to their commencement of employment with Starfield. Such checks include criminal record and may include other items as applicable to the role.

Starfield employees are required to sign a nondisclosure agreement and are required to adhere to Starfield PKI policies and procedures.

5.3.3 Training Requirements

All Starfield PKI personnel receive on the job training covering some or all of the following topics as relevant to their role:

- Basic PKI concepts
- This CP/CPS
- Documented Starfield PKI security and operational policies and procedures
- The use and operation of PKI system software
- Common threats to the validation process including phishing and other social engineering tactics

Starfield requires all validation specialists to pass an examination provided on this CP/CPS, the Guidelines for Issuance and Management of Extended Validation Certificates and the Baseline Requirements (BR) prior to validating and approving the issuance of Certificates.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Starfield documents that each validation specialist possesses the skills required by a task before allowing the validation specialist to perform that task.

Starfield maintains records of training and ensures that personnel entrusted with validation specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

5.3.4 Retraining Frequency and Requirements

Starfield PKI personnel receive formal or informal training on the use of deployed PKI products and Starfield PKI policies and procedures at the time a PKI role is first granted and annually. Security awareness campaigns are ongoing.

5.3.5 Job Rotation Frequency and Sequence

No Stipulation.

5.3.6 Sanctions for Unauthorized Actions

In accordance with corporate polices, appropriate disciplinary actions will be taken for unauthorized actions or other violations of Starfield PKI policies and procedures.

If a person in a trusted role is cited by Starfield management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role following identification of any unauthorized actions. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role, dismiss the individual from employment, or take any other actions as it deems appropriate (and subject to restrictions under applicable laws).

5.3.7 Independent Contractor Requirements

Starfield PKI may employ contractors as necessary. Where contractors are used by the Starfield PKI, they are subject to background check procedures comparable to those specified in 5.3.1 and 5.3.2.

5.3.8 Documentation Supplied to Personnel

Starfield PKI personnel are required to read this CP/CPS. They are also provided with Starfield PKI policies, procedures, and other documentation relevant to their job functions.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The Starfield PKI logs the following events:

- Significant CA key life cycle management events including CA key generation backup, storage, archival, and destruction and other cryptographic device lifecycle management events
- CA and Subscriber certificate life cycle management events
  - Requests for certificates, renewal, re-key, and revocation

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- Successful or unsuccessful processing of requests
- Generation and issuance of certificates
- Revocation of certificates
- Issuance of CRLs and generation of OCSP entries
- All verification activities required by applicable guidelines
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls

- Security-sensitive operating system events
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from CA facility
- CA facility entry/exit.
- Separation of validation duties between multiple RAs for Extended Validation certificates

All audit logs include, at a minimum:

- Date and time of entry
- Identity of the persona and entity making the journal entry
- Description of entry

5.4.2 Frequency of Processing Log

Audit logs are reviewed on an as-needed basis.

5.4.3 Retention Period for Audit Log

Audit logs are retained as follows:

Log Type	Retention Period
Logs of CA key management activity	30 years
CA system logs of certificate management activity	30 years
Operating system logs	7 years
Physical access system logs	7 years
Manual logs of physical access	7 years
Logs of all certificates, revocations and documentation relating to verification of certificate requests	7 years
Video recording of CA facility access	90 days

5.4.4 Protection of Audit Log

Production and archived logical and physical audit logs are protected using a combination of physical and logical access controls.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

5.4.5 Audit Log Backup Procedures

Audit logs are backed up on a periodic basis.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network, and operating system level. Manually generated audit data is recorded by Starfield employees.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual or system that caused the event.

5.4.8 Vulnerability Assessments

Starfield performs periodic vulnerability assessments of its PKI environment including:

- External vulnerability scans are conducted on at least a quarterly basis. Testing includes applications publicly available.
- Internal vulnerability scans of internal PKI networks are performed on at least a quarterly basis.
- Annually, a penetration test of the entire Starfield PKI is conducted which includes tests of customer facing applications, the certificate vetting application, and critical PKI infrastructure. Critical and high vulnerabilities identified as part of the assessment are documented and tracked to completion. The results of such assessments are used to enhance the security of the environment.

Upon completion of each assessment, a Corrective Action Plan will be developed to mitigate any pertinent security issues (i.e., findings) and associated risks identified by the assessment. Critical vulnerabilities that are discovered should be mitigated within 96 hours of discovery. In the event that the issue cannot be mitigated with 96 hours, the issue must be documented with justification of the delay and a timeline for completion.

5.5 Records Archival

The Starfield PKI maintains an archive of relevant records for each CA.

5.5.1 Types of Records Archived

Starfield maintains an archive of logs that include the recorded events specified in 5.4.1.

5.5.2 Retention Period for Archive

Starfield archives and retains audit logs in accordance with 5.4.3.

5.5.3 Protection of Archive

See 5.4.4.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

5.5.4 Archive Backup Procedures

Starfield maintains copies of its archived records at separate locations.

5.5.5 Requirements for Time-Stamping of Records

Starfield PKI system clocks are synchronized with a third-party time source. Automated journal entries include a system generated date and time field. Manual journal entries include a manually entered date and time field.

5.5.6 Archive Collection System (Internal or External)

No Stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No Stipulation.

5.6 Key Changeover

Starfield CAs will stop issuing certificates and will be re-keyed or terminated before the maximum key usage period for certificate signing is reached in accordance with 6.3.2. The CA will continue to sign and publish CRLs until the end of the CA certificate lifetime. The key changeover or CA termination process will be performed such that it causes minimal disruption to Subscribers and Relying Parties. Affected entities will be notified prior to the planned key changeover.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Starfield has documented business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. Starfield performs tests, reviews, and updates to these procedures at least annually. These procedures meet the requirements in BR 5.7.1.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

Starfield performs regular system backups that can be utilized to recover in the case of resource, software, or data corruption. Starfield also keeps copies of CA private keys in a secure off-site location.

5.7.3 Entity Private Key Compromise Procedures

Starfield has implemented a combination of physical, logical and procedural controls to guard against CA key compromise. In the event of a known or suspected CA key compromise, Starfield management will assess the situation and determine the appropriate course of action.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

5.7.4 Business Continuity Capabilities After a Disaster

Starfield maintains a disaster recovery plan and performs periodic testing of the plan to ensure its effectiveness in the event of a disaster.

5.8 CA or RA Termination

In the event that it is necessary to terminate the operation of a Starfield CA, Starfield management will plan and coordinate the termination process with its Subscribers and Relying Parties such that the impact of the termination is minimized. Starfield will provide as much prior notice as is practicable and reasonable to Subscribers and Relying Parties and preserve relevant records for a period of time deemed fit for functional and legal purposes. Relevant certificates will be revoked no later than the time of the termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Starfield CA key pairs are generated in and protected by hardware security modules certified to FIPS 140level 3. CA key pair generation requires the participation of multiple trusted employees.

Subscriber key pair generation is performed by the Subscriber. It is recommended that the Subscriber use a FIPS 140-2 certified cryptographic module for key generation.

6.1.2 Private Key Delivery to Subscriber

Starfield CA key pairs do not require delivery as they are generated and managed by the Starfield PKI. As Subscriber key pairs are generated by the Subscriber, there is no private key transportation requirement.

6.1.3 Public Key Delivery to Certificate Issuer

CA certificate requests are generated and processed by Starfield employees using a controlled process that requires the participation of multiple trusted individuals. CA certificate requests are PKCS #10 requests and accordingly contain the requesting CA's public key and are digitally signed by the requesting CA's private key.

For Subscriber certificate requests, the Subscriber's public key is submitted to the CA using a certificate request signed with the Subscriber's private key. This mechanism ensures that:

- the public key has not been modified during transit and
- the sender possesses the private key corresponding to the transferred public key.

6.1.4 CA Public Key Delivery to Relying Parties

The Starfield Root CA is made available to Relying Parties through its inclusion in common browser software.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

The Starfield Root CA certificates may also be downloaded from the Starfield repository. A 256-bit SHA-256 hash of the Starfield Root CA certificates is posted in the Starfield repository so that users may verify the authenticity of the Starfield Root CA certificates.

6.1.5 Key Sizes

Starfield CA key pairs used to issue certificates after January 1, 2012 are 2048 bit or higher RSA keys. Subscriber key pairs in certificates issued after January 1, 2012 are 2048 bit or higher RSA keys.

Certificates meet the following requirements for algorithm type and key size.

(1) Root CA Certificates

	Validity period beginning on or before 31 Dec 2010	**Validity period beginning after 31 Dec 2010**
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048**	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)***	L= 2048 N= 224 or L= 2048 N= 256	L= 2048 N= 224 or L= 2048 N= 256

(2) Subordinate CA Certificates

	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	**Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013**
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)***	L= 2048, N= 224 or L= 2048, N= 256	L= 2048 N= 224 or L= 2048 N= 256

(3) Subscriber Certificates

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)***	L= 2048, N= 224 or L= 2048, N= 256	L= 2048 N= 224 or L= 2048 N= 256

* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 7.1.3.

** A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as a trust anchor for Subscriber Certificates issued in accordance with these Requirements.

*** L and N (the bit lengths of modulus p and divisor q, respectively) are described in the Digital Signature Standard, FIPS 186-4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).

6.1.6 Public Key Parameters Generation and Quality Checking

Starfield generates CA Key Pairs using secure algorithms and parameters based on current research and industry standards. Starfield uses a cryptomodule that conforms to FIPS 186-2 and provides random number generation and on-board generation of up to 4096-bit RSA Public Keys and a wide range of ECC curves.

Starfield checks Subscriber RSA public keys to ensure value of this public exponent equates to an odd number equal to three or more.

6.1.7 Key Usage Purposes

Key pairs may be used as follows:

Entity	Permitted Key Usage
Root CAs	Signing of certificates for Subordinate CAs and other purposes as required for the Starfield PKI and CRLs.
Issuing CAs	Signing of certificates for Subscribers and other purposes as required for the Starfield PKI and CRLs.
Subscriber	Server authentication, digital signature, key encipherment, data encryption.

The key usage extension is set in accordance with the certificate profile requirements specified in 7.1.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The Starfield PKI uses cryptographic modules that are certified to FIPS 140Level 3 and meet industry standards for random number and prime number generation.

6.2.2 Private Key Multi-Person Control

The Root CA is operated in offline mode. The participation of multiple trusted employees is required to perform sensitive CA private key operations (including hardware security module (HSM) activation, Sub-CA certificate signing, CRL signing, CA key backup, and CA key recovery).

The Issuing CA is operated in online mode. The participation of multiple trusted employees is required to perform sensitive CA private key operations (including HSM activation, CA key backup, and CA key recovery).

6.2.3 Private Key Escrow

The escrow of CA and Subscriber private keys, for purposes of access by law enforcement or any other reason, is not supported by the Starfield PKI.

6.2.4 Private Key Backup

Backup copies of CA private keys are stored in encrypted form using cryptographic modules that meet the requirements specified in 6.2.1.

Once a CA has reached the end of its maximum usage period as defined in 6.3.2, HSMs containing the CA private key will be zeroized and/or securely destroyed.

Subscriber private keys are not backed up by the Starfield PKI.

6.2.5 Private Key Archival

Once a CA has reached the end of its maximum usage period as defined in 6.3.2, HSMs containing the CA private key will be zeroized and/or securely destroyed.

Subscriber private keys are not archived by the Starfield PKI.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CA private keys are generated and used only within hardware cryptographic modules meeting the requirements of 6.2.1. The private key exists outside hardware cryptographic modules only in encrypted form.

6.2.7 Private key storage on cryptographic module

CA private keys are stored within hardware cryptographic modules meeting the requirements of 6.2.1.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

6.2.8 Method of Activating Private Keys

Hardware modules used for CA private key protection utilize an activation mechanism as described in 6.2.2.

6.2.9 Method of Deactivating Private Key

CA private keys are de-activated by securing the partition on the HSM device.

6.2.10 Method of Destroying Private Key

CA private key destruction requires the participation of multiple trusted Starfield employees and approval from Starfield management. When CA key destruction is required, CA private keys will be completely destroyed through zeroization and/or physical destruction of the device in accordance with manufacturers' guidance.

6.2.11 Cryptographic Module Rating

Refer to 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Copies of CA and Subscriber certificates are archived in accordance with 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

For Starfield PKI CAs and Subscribers, key and certificate usage periods meet the following requirements.

Entity	Maximum Key Usage Period (for certificate signing)*	Maximum Key Usage Period (for CRL signing)	Maximum Certificate Validity Period
Root CAs	15 years	20 years	30 years
Issuing CAs	20 years	25 years	20 years
Subscribers	N/A	N/A	825 days

Subscriber Certificates	Maximum Certificate Validity Period
Basic and Medium Assurance Domain Validated SSL Server Certificate	825 days
High Assurance Organizational Validated SSL Server Certificate Subscribers	825 days
High Assurance Code Signing Certificate Subscribers	39 months
Extended Validation SSL Server Certificate Subscribers	825 days

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

* Maximum Key Usage Period does not apply to certificates that serve an infrastructure purpose, such as OCSP Responder certificates or Timestamp Authority certificates. Timestamp authority certificates have a maximum validity period of 135 months.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

HSMs used for CA private key protection are configured to require multiple key shareholders as described in 6.2.2.

6.4.2 Activation Data Protection

The activation materials are used only when needed and stored in a secure site when not in use.

6.4.3 Other Aspects of Activation Data

No Stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Starfield's systems maintaining CA software and data files are secure from unauthorized access. In addition, access to production servers is limited to those individuals with a valid business reason for such access.

Starfield's production network is separate from other components. This separation prevents network access except through specific application processes. Starfield has sophisticated access control technologies in place to protect the production network from unauthorized internal and external access and to limit network activities accessing production systems. Access controls in use include, but are not limited to, multifactor authentication.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

All CA software is developed in accordance with documented Software Development Life Cycle processes. Reviews of all changes are made during multiple points of the software development. Approval to deploy changes requires multiple individuals. All code is verified, using digital signatures and hashing, before being deployed into the production CA environment.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

6.6.2 Security Management Controls

Starfield has tools and processes in place to control and monitor the configurations of the CA systems. Starfield validates the integrity of all software before release into production.

6.6.3 Life Cycle Security Controls

No Stipulation.

6.7 Network Security Controls

The Starfield network is secured through the use of preventative (properly configured routers and firewalls) and detective controls (monitoring systems). Starfield performs all CA and RA functions using networks secured in accordance with the Starfield Operations Guide to ensure the systems are secure.

6.8 Time-Stamping

Starfield maintains Network Time Protocol (NTP) enabled devices which use the GPS system to synchronize its clock. The servers, via NTP, then synchronize their system clock to these devices which are used to generate time stamps.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number

Starfield issues X.509 Version 3 certificates.

7.1.2 Certificate Extensions

Extensions used in Starfield certificates are documented in Appendix A.

7.1.3 Algorithm Object Identifiers

Starfield signs certificates with the following algorithms:

- Sha1RSA* 1.2.840.113549.1.1.5
- sha256RSA 1.2.840.113549.1.1.11
- ECDSAsha384 1.2.840.10045.4.3.3

* CAs do not issue OCSP, or Subscriber SSL Certificates utilizing the SHA-1 algorithm.

7.1.4 Name Forms

Every Starfield certificate is uniquely identified by its Subject and incorporate a unique identifying serial number. Starfield certificates support name chaining as specified in RFC 5280, section 4.1.2.4.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

7.1.5 Name Constraints

Starfield does not perform name constraints.

7.1.6 Certificate Policy Object Identifier

Starfield uses the following certificate policy oids in end-entity certificates:

- Medium Assurance certificates - 2.16.840.1.114413.1.7.23.1 and 2.16.840.1.114414.1.7.23.1
- High Assurance Server and Code Signing certificates - 2.16.840.1.114413.1.7.23.2 and 2.16.840.1.114414.1.7.23.2
- Extended Validation certificates - 2.16.840.1.114413.1.7.23.3 and 2.16.840.1.114414.1.7.23.3

7.1.7 Usage of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifier Syntax and Semantics

Starfield certificates include a link to our repository where this CPS and other applicable agreements may be viewed.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation.

7.2 CRL Profile

7.2.1 Version Number

Starfield issues version 1 and 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

7.2.2.1 Root CAs

The following CRL profile is used for root certificates in the Starfield PKI.

Field	Description
Signature	SHA-1 or SHA-256
Issuer	Subject of the corresponding root certificate
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	365 days after This Update.
CRL extensions (V1 and V2)	
CRL Number	Unique value for each CRL issued by the corresponding root certificate.
Authority Key Identifier	SHA-1 hash of the public key of the corresponding root certificate

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Revoked Certificates	List of information regarding revoked certificates. CRL entries include: • ***Serial Number***, identifying the revoked certificate ***Revocation Date***, including the date and time of certificate revocation
CRL Entry Extensions V1 and V2 and optional for any given CRL entry)	
CRL Reason Code	One of the following reason codes: unspecified (0) keyCompromise (1) cACompromise (2) affiliationChanged (3) superseded (4) cessationOfOperation (5) certificateHold (6) removeFromCRL (8) privilegeWithdrawn (9) aACompromise (10)
Invalidity Date	A GeneralizedTime denoting the effective time when the given serial number is to be considered invalid.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

7.2.2.2 Issuing CAs

The following CRL profile is used for Starfield Issuing CAs.

Field	Description
Signature	SHA-1 or SHA-256
Issuer	Subject of the corresponding Issuing CA certificate
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	365 days after This Update.
CRL extensions (V1 and V2)	
CRL Number	Unique value for each CRL issued by the corresponding Issuing CA certificate.
Authority Key Identifier	SHA-1 hash of the public key of the corresponding Issuing CA certificate
Revoked Certificates	List of information regarding revoked certificates. CRL entries include: • Serial Number, identifying the revoked certificate • Revocation Date, including the date and time of certificate revocation
CRL Entry Extensions V1 and V2 and optional for any given CRL entry)	
CRL Reason Code	One of the following reason codes: unspecified (0) keyCompromise (1) cACompromise (2) affiliationChanged (3) superseded (4) cessationOfOperation (5) certificateHold (6) removeFromCRL (8) privilegeWithdrawn (9) aACompromise (10)
Invalidity Date	A GeneralizedTime denoting the effective time when the given serial number is to be considered invalid.

7.3 OCSP Profile

7.3.1 Version Number

Starfield OCSP responses conform to version 1 of RFC 6960.

7.3.2 OCSP Extensions

No stipulation.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

The Starfield PKI is subject to an annual WebTrust for Certification Authorities (WebTrust for CAs) examination. The Starfield PKI is also subject to an annual WebTrust for Extended Validation (WebTrust for EV) examination, as it relates to the issuance of Extended Validation certificates from the Starfield issuing CAs.

8.2 Identity/Qualifications of Assessor

Auditors demonstrating proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function shall perform the annual WebTrust for CAs and WebTrust for EV examinations. The audit firm must be currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits, be a member of the American Institute of Certified Public Accountants (AICPA), and maintain professional liability/errors & omissions insurance with policy limits of at least one million United States Dollars ($1,000,000.00) in coverage.

8.3 Assessor's Relationship to Assessed Entity

The entity that performs the annual audit shall be organizationally independent of Starfield.

8.4 Topics Covered by Assessment

The scope of the annual audit shall include the requirements of this CP/CPS, CA environmental controls, CA key management, and certificate life cycle management.

8.5 Actions Taken as a Result of Deficiency

Significant deficiencies identified during the compliance audit will result in a determination of actions to be taken. The Starfield Governance and Policy Committee makes this determination with input from the auditor. Starfield Management is responsible for ensuring that corrective action plans are promptly developed and corrective action is taken within a period of time commensurate with the significance of such matters identified.

Should a severe deficiency be identified that might compromise the integrity of the Starfield PKI, Starfield Management will consider, with input from the auditor, whether suspension of Starfield PKI operations is warranted. Should a severe deficiency be identified that might compromise the integrity of a particular CA, Starfield PKI Management will assess whether suspension of the particular CA's operations is warranted.

8.6 Communication of Results

Compliance audit results are communicated to Starfield Management and others deemed appropriate by Starfield Management. Starfield makes letters showing compliance with annual external audit reports publicly available in the Starfield repository (certs.secureserver.net/repository).

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

8.7 Self –Audits

On at least a quarterly basis, Starfield performs regular internal audits against a randomly selected sample of at least three percent of its SSL/TLS Server Certificates issued since the last internal audit. Self-audits on server and code signing Certificates are performed in accordance with Guidelines adopted by the CA / Browser Forum.

8.8 Specification Administration

8.8.1 Specification Change Procedures

Modifications to this CP/CPS are approved by the Starfield Governance and Policy Committee and become effective upon publication in the Starfield repository.

8.8.2 Publication and Notification Policies

This CP/CPS and subsequent revisions are published in the Starfield repository in accordance with 2.6.1. Starfield may change this document at any time without prior notice.

8.9 CPS Approval Procedures

See 8.8.1.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Starfield and Customers may charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

Starfield reserves the right to charge a fee for making a Certificate available in a repository or otherwise.

9.1.3 Revocation or Status Information Access Fees

Starfield does not charge a fee as a condition of making the CRLs required by CPS 4.4.9 available in a repository or otherwise available to Relying Parties. Starfield reserves the right to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. Starfield does not permit access to revocation information, Certificate status information, or time stamping in its repository by third parties that provide products or services that utilize such Certificate status information without Starfield's prior express written consent.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

9.1.4 Fees for Other Services

Starfield licenses this CPS under the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license (https://creativecommons.org/licenses/by-nd/4.0/legalcode).

9.1.5 Refund Policy

The following refund policy is in effect:

Starfield employs strict practices and policies in its certification operations and in issuing certificates. If for any reason a Subscriber is not completely satisfied with the certificate that has been issued to the Subscriber, the Subscriber may ask Starfield to revoke the certificate within 30 days of issuance for a refund, minus any fees. Following the initial 30 day period, a Subscriber may ask Starfield to revoke the certificate and provide a refund if Starfield has breached a warranty or other material obligation under this CPS relating to the Subscriber or the subscriber's certificate. After Starfield revokes the subscriber's certificate, Starfield will promptly credit the Subscriber's credit card account (if the certificate was paid for via credit card) or otherwise reimburse the Subscriber via check, for the full amount minus fees, of the amount paid for the certificate. To request a refund, please call customer service at +1 (480) 505-8855. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

9.2 Financial Responsibility

Subscribers and Relying Parties shall be responsible for the financial consequences to such Subscribers, Relying Parties, and to any other persons, entities, or organizations for any transactions in which such Subscribers or Relying Parties participate and which use Starfield Certificates or any services provided in respect to Starfield Certificates. Starfield makes no representations and gives no warranties or conditions regarding the financial efficacy of any transaction completed utilizing a Starfield Certificate or any services provided in respect to Starfield Certificates and neither Starfield nor any independent third-party RA operating under a Starfield CA, nor any Resellers, Co-marketers, nor any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall have any liability except as explicitly set forth herein in respect to the use of or reliance on a Starfield Certificate or any services provided in respect to Starfield Certificates.

9.2.1 Insurance Coverage

No Stipulation.

9.2.2 Other Assets

No Stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

No Stipulation.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Sensitive Starfield PKI information must remain confidential to Starfield. The following information is considered confidential to Starfield and may not be disclosed:

- Starfield PKI policies, procedures and technical documentation supporting this CP/CPS
- Subscriber registration records, including:
  - Certificate applications, whether approved or rejected
  - Proof of identification documentation and details
  - Certificate information collected as part of the registration records, beyond that which is required to be included in Subscriber certificates
- Audit trail records
- Any private key within the Starfield PKI hierarchy
- Compliance audit results except for WebTrust for CAs audit reports which may be published at the discretion of Starfield Management

9.3.2 Information not Within the Scope of Confidential Information

This CP/CPS and Certificates and CRLs issued by Starfield are not considered confidential. Subscriber certificate status information is made available to Relying Parties through the use of CRLs and OCSP.

9.3.3 Responsibility to Protect Confidential Information

No Stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Starfield processes personal data in accordance with the privacy policy posted here: https://www.godaddy.com/agreements/showdoc?pageid=PRIVACY&isc=gdbbc687

9.4.2 Information Treated as Private

See 9.4.1.

9.4.3 Information Not Deemed Private

See 9.4.1.

9.4.4 Responsibility to Protect Private Information

See 9.4.1.

9.4.5 Notice and Consent to Use Private Information

See 9.4.1.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

As a general principle, no document or record (including registration records) belonging to or controlled by the Starfield PKI is released to law enforcement agencies or officials except where the law enforcement official is properly identified and where the release of specific information is:

- required by applicable laws or regulations
- pursuant to a subpoena or order of a court or other government or regulatory authority with which Starfield is legally obligated to comply
- pursuant to a demand made by any government regulatory agency or authority with jurisdiction over Starfield.

As a general principle, no document or record belonging to or controlled by the Starfield PKI is released to any person except where:

- a properly constituted instrument requiring production of the information is produced and
- the person requiring production is a person authorized to do so by a court of law and is properly identified.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property Rights

Intellectual Property Rights among Starfield PKI Participants other than Subscribers and Relying Parties are governed by the applicable agreements among such Starfield PKI Participants. The following subsections of CPS 2.6 apply to Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

The Intellectual Property Rights pertaining to the Certificates of CAs and revocation information that are issued by CAs shall be retained by those CAs. Provided the Certificates are reproduced in full and that use of such Certificates is subject to the Relying Party agreement, Starfield and Subscribers grant permission to reproduce and distribute the Certificates on a nonexclusive royalty-free basis. Starfield and Subscribers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable Relying party agreement or any other applicable agreements.

9.5.2 Property Rights in the Agreement

Starfield PKI Participants acknowledge that Starfield retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights to Names

Certificate applicants retain all rights, if they have any, in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

issued to them. Starfield retains all rights it has in any trademark, service mark, trade name, or other identifying trade symbols that it owns.

9.5.4 Property Rights in Keys and Key Material

All Key Pairs corresponding to Certificates of CAs and end-user Subscribers are the property of those CAs and end-users, regardless of where they are stored physically, and those persons retain all Intellectual Property Rights in and to those key pairs. Without limiting the generality of the foregoing, Starfield's Root CA Public keys and the root Certificates containing them are the property of Starfield. Starfield grants licenses to software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, without limiting the generality of the foregoing, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares.

The following are the property of Starfield:

- This CPS
- Starfield-specified Certificate Policies
- Policies and procedures supporting the operation of the Starfield PKI
- Starfield-specified Object Identifiers (OIDs)
- Certificates and CRLs issued by Starfield CAs
- Distinguished Names (DNs) used to represent entities within the Starfield PKI
- CA and infrastructure key pairs

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The warranties, disclaimers of warranty, and limitations of liability among Starfield, its Resellers, and their respective Customers within the Starfield PKI are set forth and governed by the agreements among them. This CPS 9.6.1 relates only to the warranties that certain CAs (Starfield CAs) must make to end-Subscribers receiving Certificates from them and to Relying Parties, the disclaimers of warranties they shall make to those Subscribers and Relying Parties, and the limitations of liability they can place on those Subscribers and Relying Parties.

Starfield uses, and (where required) Resellers shall use, Subscriber agreements and Relying party agreements in accordance with CPS 1.3. These Subscriber agreements shall meet the requirements imposed by Starfield (in the case of Resellers). Requirements that Subscriber agreements contain warranties, disclaimers, and limitations of liability below apply to those Resellers that use Subscriber agreements. Starfield agrees to such requirements in its Subscriber agreements. Starfield's practices concerning warranties, disclaimers, and limitations in Relying Parties agreements apply to Starfield. Note that terms applicable to Relying Parties shall also be included in Subscriber agreements, in addition to Relying party agreements, because subscribers often act as Relying Parties as well.

Applicants, Subscribers, and Relying Parties acknowledge and agree that operations in relation to Starfield Certificates and Starfield Certificate Applications are dependent on the transmission of

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

information over communication infrastructures such as, without limitation, the Internet, telephone and telecommunications lines and networks, servers, firewalls, proxies, routers, switches, and bridges ("Telecommunication Equipment") and that this Telecommunication Equipment is not under the control of Starfield or any independent third-party RA operating under a Starfield CA, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing. Neither Starfield nor any independent third-party RA operating under a Starfield RA, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall be liable for any error, failure, delay, interruption, defect, or corruption in relation to a Starfield Certificate, a Starfield CRL, a Starfield OCSP Response, or a Starfield Certificate Application to the extent that such error, failure, delay, interruption, defect, or corruption is caused by such Telecommunication Equipment.

9.6.1.1 Starfield Certification Authority Warranties to Subscribers and Relying Parties

- **Right to Use Domain Name or IP Address:** That, at the time of issuance, Starfield **(i)** implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); **(ii)** followed the procedure when issuing the Certificate; and **(iii)** accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- **Authorization for Certificate:** That, at the time of issuance, Starfield **(i)** implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; **(ii)** followed the procedure when issuing the Certificate; and **(iii)** accurately described the procedure in Starfield's Certificate Policy and/or Certification Practice Statement;
- **Accuracy of Information:** That, at the time of issuance, Starfield **(i)** implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); **(ii)** followed the procedure when issuing the Certificate; and **(iii)** accurately described the procedure in Starfield's Certificate Policy and/or Certification Practice Statement;
- **No Misleading Information:** That, at the time of issuance, Starfield **(i)** implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; **(ii)** followed the procedure when issuing the Certificate; and **(iii)** accurately described the procedure in Starfield's Certificate Policy and/or Certification Practice Statement;
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, Starfield **(i)** implemented a procedure to verify the identity of the Applicant in accordance with Section 3; **(ii)** followed the procedure when issuing the Certificate;
- **Subscriber Agreement:** That, if Starfield and the Subscriber are not Affiliated, the Subscriber and Starfield are parties to a legally valid and enforceable Subscriber Agreement that satisfies these requirements, or, if Starfield and the Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use;
- **Status:** That Starfield maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- **Revocation:** That Starfield will revoke the Certificate for any of the reasons specified in this document.

9.6.2 RA Representations and Warranties

No Stipulation.

9.6.3 Subscriber Representations and Warranties

Subscribers are obligated by Starfield's Subscriber Agreements to warrant that, among other things:

- All digital signatures created using the private key corresponding to the public key listed in the Certificate belong to that Subscriber and the Certificate has been accepted and is functional – it has not expired or been revoked - at the time the digital signature is created,
- No unauthorized users have had access to the Subscriber's private key,
- All representations in the Certificate Application by the Subscriber are true,
- The information from the Subscriber in the Certificate is true,
- Any usage of the Certificate is for authorized and lawful reasons only, consistent with this CPS,
- The Subscriber is not a CA but is an end-user Subscriber and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise (with the exception of signing code with a Code Signing Certificate), and
- The Subscriber is not using the Certificate Service in any way that infringes upon the rights of third parties.
- The Subscriber is not using their Code Signing Certificate to digitally sign hostile code, including spyware or other malicious software (malware) downloaded without user consent.

These requirements shall be in other Subscriber Agreements.

9.6.4 Relying Party Representations and Warranties

You warrant and represent that:
(a) the Certificate is being used lawfully by You and with authorization;
(b) You are using the Certificate in a Relying Party capacity;
(c) You disclaim any fiduciary relationship between Starfield and any non-Starfield Certification Authorities, and between You and any Subscriber; and
(d) You understand that a Starfield Subscriber is solely responsible for the generation and security of the Private Key corresponding to the Public Key contained in the Subscriber's Certificate, and that the Subscriber may have failed to keep the Certificate secure and if so, the Private Key may have become compromised.

9.6.5 Representations and Warranties of Other Participants

No Stipulation.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

9.7 Disclaimers of Warranties

STARFIELD, ITS CAS, ITS RESELLERS, CO-MARKETERS, SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, AND EMPLOYEES MAKE NO REPRESENTATIONS AND EXPRESSLY DISCLAIM ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE, SATISFACTORY TITLE, AND ALSO INCLUDING WARRANTIES THAT ARE STATUTORY OR BY USAGE OF TRADE. STARFIELD MAKES NO WARRANTY THAT ITS SERVICE(S) WILL MEET ANY EXPECTATIONS, OR THAT THE SERVICE(S) WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE, OR THAT DEFECTS WILL BE CORRECTED. STARFIELD DOES NOT WARRANT, NOR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR RESULTS OF, ANY OF THE SERVICES WE PROVIDE, IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

9.7.1 Fiduciary Relationships

Starfield is not the agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties. Starfield's Subscriber agreements and Relying party agreements shall disclaim, to the extent permitted by law, any fiduciary relationship between Starfield or a non-Starfield CA or RA, and between a Subscriber or Relying party.

9.8 Limitations of Liability

STARFIELD SHALL NOT BE LIABLE FOR ANY LOSS OF CERTIFICATE SERVICES UNLESS DUE TO A FAILURE OR BREACH OF THE CERTIFICATE ENCRYPTION.

THE TOTAL CUMULATIVE LIABILITY OF STARFIELD, ANY INDEPENDENT THIRD-PARTY RA OPERATING UNDER A STARFIELD CA, ANY RESELLERS, OR CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING TO ANY APPLICANT, SUBSCRIBER, RELYING PARTY OR ANY OTHER PERSON, ENTITY, OR ORGANIZATION ARISING OUT OF OR RELATING TO ANY STARFIELD CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO STARFIELD CERTIFICATES, INCLUDING ANY USE OR RELIANCE ON ANY STARFIELD CERTIFICATE, SHALL NOT EXCEED (A) $0.00 USD FOR EACH BASIC ASSURANCE CERTIFICATE ("BASIC ASSURANCE CUMULATIVE DAMAGE LIMIT"); (B) $10,000.00 USD FOR EACH MEDIUM ASSURANCE CERTIFICATE ("MEDIUM ASSURANCE CUMULATIVE DAMAGE LIMIT"); (C) $25,000.00 USD FOR EACH HIGH ASSURANCE CERTIFICATE ("HIGH ASSURANCE CUMULATIVE DAMAGE LIMIT"); OR (D) $50,000.00 USD FOR EACH EXTENDED VALIDATION CERTIFICATE ("EXTENDED VALIDATION CUMULATIVE DAMAGE LIMIT") (COLLECTIVELY, "CUMULATIVE DAMAGE LIMITS"). THESE CUMULATIVE DAMAGE LIMITS SHALL APPLY PER STARFIELD CERTIFICATE REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CAUSES OF ACTION ARISING OUT OF OR RELATED TO SUCH STARFIELD CERTIFICATE OR

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

ANY SERVICES PROVIDED IN RESPECT TO SUCH STARFIELD CERTIFICATE. THE FOREGOING LIMITATIONS SHALL APPLY TO ANY LIABILITY WHETHER BASED IN CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE), LEGISLATION OR ANY OTHER THEORY OF LIABILITY, INCLUDING ANY DIRECT, INDIRECT, SPECIAL, STATUTORY, PUNITIVE, EXEMPLARY, CONSEQUENTIAL, RELIANCE, OR INCIDENTAL DAMAGES.

STARFIELD, ANY INDEPENDENT THIRD-PARTY RA OPERATING UNDER A STARFIELD CA, OR DIRECTORS OF ANY OF THE FOREGOING SHALL NOT BE LIABLE TO ANY SUBSCRIBER, RELYING PARTY, OR ANY OTHER PERSON, ENTITY, OR ORGANIZATION FOR ANY LOSSES, COSTS, EXPENSES, LIABILITIES, DAMAGES, CLAIMS OR SETTLEMENT AMOUNTS ARISING OUT OF OR RELATING TO ANY PROCEEDING OR ALLEGATION THAT A STARFIELD CERTIFICATE OR ANY INFORMATION CONTAINED IN A STARFIELD CERTIFICATE INFRINGES, MISAPPROPRIATES, DILUTES, UNFAIRLY COMPETES WITH, OR OTHERWISE VIOLATES ANY PATENT, TRADEMARK, COPYRIGHT, TRADE SECRET, OR ANY INTELLECTUAL PROPERTY RIGHT OR OTHER RIGHT OF ANY PERSON, ENTITY, OR ORGANIZATION IN ANY JURISDICTION.

SHOULD LIABILITY ARISING OUT OF OR RELATING TO A STARFIELD CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO A STARFIELD CERTIFICATE EXCEED THE CUMULATIVE DAMAGE LIMITS, THE AMOUNTS AVAILABLE UNDER THE CUMULATIVE DAMAGE LIMITS SHALL BE APPORTIONED FIRST TO THE EARLIEST CLAIMS TO ACHIEVE FINAL DISPUTE RESOLUTION UNLESS OTHERWISE ORDERED BY A COURT OF COMPETENT JURISDICTION. IN NO EVENT SHALL STARFIELD OR ANY INDEPENDENT THIRD-PARTY RA OPERATING UNDER ANY STARFIELD CERTIFICATION AUTHORITY, OR ANY RESELLERS, CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING BE OBLIGATED TO PAY MORE THAN THE CUMULATIVE DAMAGE LIMITS FOR ANY STARFIELD CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO ANY STARFIELD SERVER CERTIFICATE REGARDLESS OF APPORTIONMENT AMONG CLAIMANTS.

STARFIELD, INDEPENDENT THIRD-PARTY RAs OPERATING UNDER A STARFIELD CERTIFICATION AUTHORITY, RESELLERS, CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING SHALL NOT BE LIABLE FOR ANY INCIDENTAL, SPECIAL, STATUTORY, PUNITIVE, EXEMPLARY, INDIRECT, RELIANCE, OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, LOSS OF BUSINESS OPPORTUNITIES, LOSS OF GOODWILL, LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA, LOST SAVINGS OR OTHER SIMILAR PECUNIARY LOSS) WHETHER ARISING FROM CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE), LEGISLATION OR ANY OTHER THEORY OF LIABILITY.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY STATED HEREIN AND EVEN IF STARFIELD OR ANY INDEPENDENT THIRD-PARTY
OPERATING UNDER A STARFIELD CERTIFICATION AUTHORITY, OR ANY RESELLERS, CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THESE LIMITATIONS SET FORTH ABOVE MAY NOT APPLY TO CERTAIN APPLICANTS, SUBSCRIBERS, RELYING PARTIES, OR OTHER PERSONS, ENTITIES, OR ORGANIZATIONS. THE DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, AND CONDITIONS AND THE LIMITATIONS OF LIABILITY IN THIS STARFIELD CERTIFICATION PRACTICE STATEMENT CONSTITUTE AN ESSENTIAL PART OF THE STARFIELD CPS, ANY SUBSCRIPTION AGREEMENTS, AND ANY RELYING PARTY AGREEMENTS. ALL APPLICANTS, SUBSCRIBERS, RELYING PARTIES, AND OTHER PERSONS, ENTITIES, AND ORGANIZATIONS ACKNOWLEDGE THAT BUT FOR THESE DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, AND CONDITIONS AND LIMITATIONS OF LIABILITY, STARFIELD WOULD NOT ISSUE STARFIELD CERTIFICATES TO SUBSCRIBERS AND NEITHER STARFIELD NOR ANY INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER A STARFIELD CERTIFICATION AUTHORITY, NOR ANY RESELLERS, CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING WOULD PROVIDE SERVICES IN RESPECT TO STARFIELD CERTIFICATES AND THAT THESE PROVISIONS PROVIDE FOR A REASONABLE ALLOCATION OF RISK.

9.8.1.1 Hazardous Activities

Starfield Certificates and the services provided by Starfield in respect to Starfield Certificates are not designed, manufactured, or intended for use in or in conjunction with hazardous activities or uses requiring fail-safe performance, including the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control, medical devices or direct life support machines. Starfield and any independent third-party RA operating under a Starfield CA, and any Resellers, Co-marketers, and any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing specifically disclaim any and all representations, warranties, and conditions with respect to such uses, whether express, implied, statutory, by usage of trade,
or otherwise.

9.8.1.2 Other

Without limitation, neither Starfield nor any independent third-party RAs operating under a Starfield CA, nor any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall be liable to any Applicants, Subscribers, Relying Parties or any other person, entity, or organization for any losses, costs,

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to use of a Starfield Certificate or any services provided in respect to a Starfield Certificate if:

(i) the Starfield Certificate was issued as a result of errors, misrepresentations, or other acts or omissions of a Subscriber or of any other person, entity, or organization;
(ii) the Starfield Certificate has expired or has been revoked;
(iii) the Starfield Certificate has been modified or otherwise altered;

(iv) a Subscriber breached the Starfield CPS or the Subscriber's Subscription Agreement, or a Relying Party breached the Starfield CPS or the Relying Party's Relying Party Agreement;
(v) the Private Key associated with the Starfield Certificate has been Compromised; or
(vi) the Starfield Certificate is used other than as permitted by the Starfield CPS or is used in contravention of applicable law.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

Starfield's Subscriber Agreement and other Subscriber Agreements shall require Subscribers to indemnify, to the extent permitted by law, Starfield and any non-Starfield CAs or RAs against any and all liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs, and expert's fees) arising out of or relating to any use or reliance by a Relying Party on any Starfield Certificate or any service provided in respect to Starfield Certificates, including:

- Any false statement, omission or misrepresentation of fact that the Subscriber has put on the Subscriber's Certificate Application,
- Any modification made by the Subscriber to the information contained in a Starfield Certificate,
- The use of a Starfield Certificate other than as permitted by the Starfield CPS, the Subscription agreement, any Relying Party agreement, and applicable law,
- The Subscriber's failure to use a secure system, protect the Subscriber's private key, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

9.9.2 Indemnification by Relying Parties

Starfield's Subscriber Agreements and Relying Party Agreements shall require Relying Parties to indemnify Starfield and any non-Starfield CAs or RAs against, to the extent permitted by law, any and all liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs, and expert's fees) arising out of or relating to any use or reliance by a Relying Party on any Starfield Certificate or any service provided in respect to Starfield Certificates, including:

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

- Any failure by the Relying Party to perform the obligations of a Relying Party,
- Lack of proper validation of a Starfield Certificate by a Relying Party,
- Use of a Starfield Certificate other than as permitted by the Starfield CPS, the Subscription agreement, any Relying Party agreement, and applicable law,
- Failure by a Relying Party to exercise reasonable judgment in the circumstances in relying on a Starfield Certificate.
- Reliance by a Relying Party on a Certificate that is not reasonable under the circumstances, or
- The failure of a Relying Party to check the status of such Certificate to determine if it is expired or revoked.

9.10 Term and Termination

9.10.1 Term

No Stipulation.

9.10.2 Termination

No Stipulation.

9.10.3 Effect of Termination and Survival

This CP/CPS shall be binding on all successors of the parties.

If any provision of this CP/CPS is found to be unenforceable, the remaining provisions shall be interpreted to best carry out the reasonable intent of the parties. It is expressly agreed that every provision of this CP/CPS that provides for a limitation of liability or exclusion of damages, disclaimer or limitation of any warranties, promises or other obligations, is intended to be severable and independent of any other provision and is to be enforced as such.

This CPS shall be interpreted consistently with what is commercially reasonable in good faith under the circumstances and considering its international scope and uniform application. Failure by any person to enforce a provision of this CP/CPS will not be deemed a waiver of future enforcement of that or any other provision.

9.11 Individual Notices and Communications with Participants

Any notice, demand, or request pertaining to this CP/CPS shall be communicated either using email consistent with this CP/CPS, or in writing. Electronic communications shall be effective when received by the intended recipient.

9.12 Amendments

9.12.1 Procedure for Amendment

No Stipulation.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

9.12.2 Notification Mechanism and Period

No Stipulation.

9.12.3 Circumstances Under Which OID Must be Changed

No Stipulation.

9.13 Dispute Resolution Provisions

In the event of any dispute involving the services or provisions covered by this CP/CPS, the aggrieved party shall notify Starfield management regarding the dispute. Starfield management will involve the appropriate Starfield personnel to resolve the dispute.

9.14 Governing Law

The laws of the state of Arizona, USA, shall govern the enforceability, construction, interpretation, and validity of this CPS, subject to any limits appearing in applicable law, and regardless of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Arizona, USA. The choice of law is made to create uniform procedures and interpretation for all Starfield PKI participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this CPS 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

Any applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information shall apply to this CPS.

9.15 Compliance with Applicable Law

No Stipulation.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No Stipulation.

9.16.2 Assignment

No Stipulation.

9.16.3 Severability

No Stipulation.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

9.16.4 Enforcement

No Stipulation.

9.17 Other Provisions

Not applicable.

10 APPENDIX A – CERTIFICATE PROFILES

10.1 Root CAs

The following certificate profile is used for the Starfield Class 2 Certification Authority.

Field	Description
Version	V3
Serial Number	0 (0x0)
Signature Algorithm Identifier	sha1RSA
Issuer	OU=Starfield Class 2 Certification Authority O=Starfield Technologies, Inc. C=US
Valid From	June 29, 2004 17:39:16 GMT
Valid To	June 29, 2034 17:39:16 GMT
Subject	OU=Starfield Class 2 Certification Authority O=Starfield Technologies, Inc. C=US
Subject Public Key Information	RSA (2048 bits)
Extensions:	
Basic Constraints	Subject Type=CA Path Length Constraint=None
Authority Key Identifier	KeyID: bf 5f b7 d1 ce dd 1f 86 f4 5b 55 ac dc d7 10 c2 0e a9 88 e7 Certificate Issuer: Directory Address: OU=Starfield Class 2 Certification Authority O=Starfield Technologies, Inc. C=US Certificate SerialNumber=00
Subject Key Identifier	bf 5f b7 d1 ce dd 1f 86 f4 5b 55 ac dc d7 10 c2 0e a9 88 e7

The following certificate profile is used for the Starfield Root Certificate Authority – G2.

Field	Description
Version	V3
Serial Number	0 (0x0)
Signature Algorithm Identifier	sha256RSA

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Issuer	CN=Starfield Root Certificate Authority - G2 O=Starfield Technologies, Inc. L=Scottsdale S=Arizona C=US
Valid From	September 1, 2009 00:00:00 GMT
Valid To	December 31, 2037 23:59:59 GMT
Subject	CN=Starfield Root Certificate Authority - G2 O=Starfield Technologies, Inc. L=Scottsdale S=Arizona C=US
Subject Public Key Information	RSA (2048 bits)
Extensions:	
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	7c 0c 32 1f a7 d9 30 7f c4 7d 68 a3 62 a8 a1 ce ab 07 5b 27

The following certificate profile is used for the Starfield Root Certificate Authority – G3.

Field	Description
Version	V3
Serial Number	37 97 3c 60 2b ab 78 9c 96 13 69 5b 6c b0 03 10
Signature Algorithm Identifier	sha256RSA
Issuer	CN=Starfield Root Certificate Authority – G3 O=Starfield Technologies, LLC L=Scottsdale S=Arizona C=US
Valid From	September 30, 2014 07:00:00 GMT
Valid To	September 30, 2039 07:00:00 GMT
Subject	CN=Starfield Root Certificate Authority – G3 O=Starfield Technologies, LLC L=Scottsdale S=Arizona C=US
Subject Public Key Information	RSA (4096 bits)
Extensions:	
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	16 9a 33 eb ac e8 ca d2 dc 66 a7 cb 1f 96 fc 7e 76 6e 40 e3

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

The following certificate profile is used for the Starfield Certificate Authority – G4.

Field	Description
Version	V3
Serial Number	00 b1 a5 d0 12 b1 61 15 59 76 5f ee d0 07 25 45 92
Signature Algorithm Identifier	Sha384ECDSA
Issuer	CN=Starfield Root Certificate Authority – G4 O=Starfield Technologies, LLC L=Scottsdale S=Arizona C=US
Valid From	September 30, 2014 07:00:00 GMT
Valid To	September 30, 2039 07:00:00 GMT
Subject	CN=Starfield Root Certificate Authority – G4 O= Starfield Technologies, LLC L=Scottsdale S=Arizona C=US
Subject Public Key Information	ECC (384 bits) ECDSA_P384
Extensions:	
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	7a 97 c3 3f d6 ff 96 c2 fa 7a 0e 09 9e 65 16 53 cc 66 9b c7

The following certificate profile is used for the Go Daddy Class 2 Certification Authority.

Field	Description
Version	V3
Serial Number	0 (0x0)
Signature Algorithm Identifier	sha1RSA
Issuer	OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
Valid From	June 29, 2004 17:06:20 GMT
Valid To	June 29, 2034 17:06:20 GMT
Subject	OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
Subject Public Key Information	RSA (2048 bits)
Extensions:	
Basic Constraints	Subject Type=CA Path Length Constraint=None

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Authority Key Identifier	KeyID=d2 c4 b0 d2 91 d4 4c 11 71 b3 61 cb 3d a1 fe dd a8 6a d4 e3 Certificate Issuer: Directory Address: OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US Certificate SerialNumber=00
Subject Key Identifier	d2 c4 b0 d2 91 d4 4c 11 71 b3 61 cb 3d a1 fe dd a8 6a d4 e3

The following certificate profile is used for the Go Daddy Root Certificate Authority – G2.

Field	Description
Version	V3
Serial Number	0 (0x0)
Signature Algorithm Identifier	sha256RSA
Issuer	CN=Go Daddy Root Certificate Authority - G2 O=GoDaddy.com, Inc. L=Scottsdale S=Arizona C=US
Valid From	September 1, 2009 00:00:00 GMT
Valid To	December 31, 2037 23:59:59 GMT
Subject	CN=Go Daddy Root Certificate Authority - G2 O=GoDaddy.com, Inc. L=Scottsdale S=Arizona C=US
Subject Public Key Information	RSA (2048 bits)
Extensions:	
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	3a 9a 85 07 10 67 28 b6 ef f6 bd 05 41 6e 20 c1 94 da 0f de

The following certificate profile is used for the Go Daddy Root Certificate Authority – G3.

Field	Description
Version	V3
Serial Number	58 56 36 b7 32 66 ef 14 a9 d7 ca 42 21 75 9c d2
Signature Algorithm Identifier	sha256RSA

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Issuer	CN=Go Daddy Root Certificate Authority – G3 O=GoDaddy Inc. L=Scottsdale S=Arizona C=US
Valid From	September 30, 2014 07:00:00 GMT
Valid To	September 30, 2039 07:00:00 GMT
Subject	CN=Go Daddy Root Certificate Authority – G3 O=GoDaddy Inc. L=Scottsdale S=Arizona C=US
Subject Public Key Information	RSA (4096 bits)
Extensions:	
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	9e d5 9d 06 23 45 3a 8f f2 44 0e 48 6f d4 2c b8 27 ed fd 14

The following certificate profile is used for the Go Daddy Root Certificate Authority – G4.

Field	Description
Version	V3
Serial Number	7f fe 65 d7 4e 78 37 ec 59 f1 06 94 f7 e7 58 80
Signature Algorithm Identifier	Sha384ECDSA
Issuer	CN=Go Daddy Root Certificate Authority – G4 O=GoDaddy Inc. L=Scottsdale S=Arizona C=US
Valid From	September 30, 2014 07:00:00 GMT
Valid To	September 30, 2039 07:00:00 GMT
Subject	CN=Go Daddy Root Certificate Authority – G4 O=GoDaddy Inc. L=Scottsdale S=Arizona C=US
Subject Public Key Information	ECC (384 bits) ECDSA_P384
Extensions:	
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	5d bc 56 1e b0 0b 96 cc 8e fe 07 8c fc 03 f8 81 8e bf 79 5c

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

The following certificate profile is used for the Starfield Services Root Certification Authority.

Field	Description
Version	V3
Serial Number	0 (0x0)
Signature Algorithm Identifier	sha1RSA
Issuer	CN= Starfield Services Root Certification Authority OU=http://certificates.starfieldtech.com/repository/ O=Starfield Technologies, Inc. L=Scottsdale ST=Arizona C=US
Valid From	June 2, 2008 00:00:00 GMT
Valid To	December 31, 2029 23:59:59 GMT
Subject	CN= Starfield Services Root Certification Authority OU=http://certificates.starfieldtech.com/repository/ O=Starfield Technologies, Inc. L=Scottsdale ST=Arizona C=US
Subject Public Key Information	RSA (2048 bits)
Extensions:	
Key Usage (critical)	keyCertSign, cRLSign
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Authority Key Identifier	b4 c6 7f 1a 43 cc 9b 75 5d 2f c4 4b f2 8b 98 10 e9 f1 51 10
Subject Key Identifier	b4 c6 7f 1a 43 cc 9b 75 5d 2f c4 4b f2 8b 98 10 e9 f1 51 10

10.2 Issuing CA

All intermediate certificates issued by any Starfield root certificate are available in the Repository at https://certs.godaddy.com/repository.

The following certificate profile is used for Starfield Issuing (subordinate) CAs.

Field	Description
Version	V3
Serial Number	Identifying number unique within the Starfield PKI
Signature Algorithm Identifier	SHA-1, SHA-256, or SHA-384

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Issuer	Unique name matching the corresponding root certificate's Subject
Valid From	Not specified
Valid To	Up to 20 years after Valid From date
Subject	Unique name for each Issuing CA
Subject Public Key Information	RSA (1024 bits), RSA (2048 bits), RSA (4096 bits) or ECC (384 bits)
Extensions:	
Key Usage	Digital Signature, Certificate Signing, CRL Signing
Extended Key Usage	Optional. When intended to sign SSL/TLS certificates: Server Authentication, Client Authentication When intended to sign code signing certificates: Code Signing, Kernel Mode Code Signing
Basic Constraints	Subject Type=CA Path Length Constraint=None
CRL Distribution Points	Contains the URL of the corresponding root CRL
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: URI pointing to Starfield Repository
Authority Information Access	URL of the appropriate OCSP responder
Authority Key Identifier	SHA-1 hash of the corresponding root certificate's public key
Subject Key Identifier	SHA-1 hash of the certificate's public key

10.3 Cross CA Certificates

This section discloses all cross certificates that Starfield is aware of that list a CA covered by this CPS as the Subject.

The following certificate profile is used for the certificate which cross certifies the Go Daddy Root Certificate Authority - G2 with the Go Daddy Class 2 Certification Authority root.

Field	Description
Version	V3
Serial Number	1b e7 15

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Signature Algorithm Identifier	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	OU=Go Daddy Class 2 Certification Authority O = The Go Daddy Group, Inc. C = US
Valid From	January 1, 2014 07:00:00 GMT
Valid To	May 30, 2031 07:00:00 GMT
Subject	CN = Go Daddy Root Certificate Authority - G2 O = GoDaddy.com, Inc. L = Scottsdale S = Arizona C = US
Subject Public Key Information	RSA (2048 bit) (OID: 1.2.840.113549.1.1.1)
Extensions:	
Basic Constraints (critical)	Subject Type=CA
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	3a 9a 85 07 10 67 28 b6 ef f6 bd 05 41 6e 20 c1 94 da 0f de
Authority Key Identifier	KeyID= d2 c4 b0 d2 91 d4 4c 11 71 b3 61 cb 3d a1 fe dd a8 6a d4 e3
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.godaddy.com
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.godaddy.com/gdroot.crl
Certificate Policies	[1]Certificate Policy: Policy Identifier=anyPolicy (OID: 2 5 29 32 0) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://certs.godaddy.com/repository/

Note that the above certificate has been reissued. The prior instance is Valid From May 3, 2011 07:00:00 GMT, has the Serial Number 20 03, and includes Subject: OU=https://certs.starfieldtech.com/repository/.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

The following certificate profile is used for the certificate which cross certifies the Starfield Root Certificate Authority - G2 with the Starfield Class 2 Certification Authority root.

Field	Description
Version	V3
Serial Number	39 14 84
Signature Algorithm Identifier	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	OU=Starfield Class 2 Certification Authority O = Starfield Technologies, Inc. C = US
Valid From	January 1, 2014 07:00:00 GMT
Valid To	May 3, 2031 07:00:00 GMT
Subject	CN = Starfield Root Certificate Authority - G2 O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Subject Public Key Information	RSA (2048 bit) (OID: 1.2.840.113549.1.1.1)
Extensions:	
Basic Constraints (critical)	Subject Type=CA
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	7c 0c 32 1f a7 d9 30 7f c4 7d 68 a3 62 a8 a1 ce ab 07 5b 27
Authority Key Identifier	KeyID= bf 5f b7 d1 ce dd 1f 86 f4 5b 55 ac dc d7 10 c2 0e a9 88 e7
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.starfieldtech.com
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.starfieldtech.com/sfroot.crl
Certificate Policies	[1]Certificate Policy: Policy Identifier=anyPolicy (OID: 2 5 29 32 0) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://certs.starfieldtech.com/repository/

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Note that the above certificate has been reissued. The prior instance is Valid From May 3, 2011 07:00:00 GMT, has the Serial Number 20 06, and includes Subject: OU=https://certs.starfieldtech.com/repository/.

The following certificate profile is used for the certificate which cross certifies the Starfield Services Root Certificate Authority - G2 with the Starfield Services Root Certificate Authority root.

Field	Description
Version	V3
Serial Number	30 dc a9
Signature Algorithm Identifier	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	CN=Starfield Services Root Certificate Authority OU=http://certificates.starfieldtech.com/repository/ O = Starfield Technologies, Inc. L=Scottsdale S=Arizona C = US
Valid From	January 1, 2014 07:00:00 GMT
Valid To	May 30, 2031 07:00:00 GMT
Subject	CN = Starfield Services Root Certificate Authority - G2 O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Subject Public Key Information	RSA (2048 bit) (OID: 1.2.840.113549.1.1.1)
Extensions:	
Basic Constraints (critical)	Subject Type=CA
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	9c 5f 00 df aa 01 d7 30 2b 38 88 a2 b8 6d 4a 9c f2 11 91 83
Authority Key Identifier	KeyID=b4 c6 7f 1a 43 cc 9b 75 5d 2f c4 4b f2 8b 98 10 e9 f1 51 10
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.starfieldtech.com

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.starfieldtech.com/sfsroot.crl
Certificate Policies	[1]Certificate Policy: Policy Identifier=anyPolicy (OID: 2 5 29 32 0) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://certs.starfieldtech.com/repository/

Note that the above certificate has been reissued. The prior instance is Valid From May 3, 2011 07:00:00 GMT, has the Serial Number 20 06, and includes Subject: OU=https://certs.starfieldtech.com/repository/.

The following certificate profile is used for a certificate which cross certifies the Starfield Services Root Certificate Authority - G2 with the Starfield Class 2 Certification Authority root.

Field	Description
Version	V3
Serial Number	00 d8 c9 33 43 fe 5d 39 29
Signature Algorithm Identifier	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	OU=Starfield Class 2 Certification Authority O = Starfield Technologies, Inc. C = US
Valid From	September 2, 2009 00:00:00 GMT
Valid To	June 28, 2034 18:00:00 GMT
Subject	CN = Starfield Services Root Certificate Authority - G2 O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Subject Public Key Information	RSA (2048 bit) (OID: 1.2.840.113549.1.1.1)
Extensions:	
Basic Constraints (critical)	Subject Type=CA
Key Usage (critical)	keyCertSign, cRLSign
Subject Key Identifier	9c 5f 00 df aa 01 d7 30 2b 38 88 a2 b8 6d 4a 9c f2 11 91 83
Authority Key Identifier	KeyID=bf 5f b7 d1 ce dd 1f 86 f4 5b 55 ac dc d7 10 c2 0e a9 88 e7

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://o.ss2.us [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://x.ss2.us/x.cer
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = http://s.ss2.us/r.crl
Certificate Policies	[1]Certificate Policy: Policy Identifier=anyPolicy (OID: 2 5 29 32 0)

Note that the above certificate has been reissued. The prior instance has the Serial Number 00 a7 0e 4a 4c 34 82 b7 7f and a Valid To date of June 28, 2034 17:39:16 GMT.

10.4 End Entity SSL Certificates

The following certificate profile is used for Go Daddy branded Subscriber Certificates issued from the Go Daddy Issuing CA. At a minimum, the following fields will be populated as described, in accordance with IETF RFC 5280.

Field	Description
Version	V3
Serial Number	unique value with 64-bits of entropy for each certificate issued by the Issuing CA
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	serialNumber = 07969287 CN = Go Daddy Secure Certification Authority OU=http://certificates.godaddy.com/repository O = GoDaddy.com, Inc. L = Scottsdale S = Arizona C = US
Valid From	Date and time of Certificate issuance
Valid To	A date up to the maximum permitted validity period at the time of issuance after Certificate issuance (depending on SSL certificate type).
Subject (Medium Assurance Certificates	CN = domain name of Subscriber's web site OU = "Domain Control Verified" or similar text indicating the assurance level of the certificate.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Subject (High Assurance Certificates	CN = domain name of Subscriber's web site O = Subscriber's organization or individual name L = City/town S = State C = Country
Subject (Extended Validation Certificates)	CN = domain name of Subscriber's web site O = Subscriber's full legal organization name. An assumed name or DBA may also be included L = City/town of place of business S = State of place of business C = Country of place of business serialNumber= Registration number assigned by incorporating authority or date of incorporation or registration businessCategory=vetting category used to issue certificate as defined in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates jurisdictionLocalityName= City/town of incorporation or registration (if applicable) jurisdictionStateOrProvinceName= State of incorporation or registration (if applicable) jurisdictionCountryName= Country of incorporation or registration
Subject Public Key Information	RSA (2048 bits or greater)
Extensions:	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Key Usage (critical)	Digital Signature, Key Encipherment
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = <current CRL URI> The specific URI will vary depending on certificate type and CRL scope.
Certificate Policies (Medium Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114413.1.7.23.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository/

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Certificate Policies (High Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114413.1.7.23.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository/
Certificate Policies (Extended Validation Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114413.1.7.23.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository/
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.godaddy.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certificates.godaddy.com/repository/gd_intermediate.crt
Authority Key Identifier	KeyID: fd ac 61 32 93 6c 45 d6 e2 ee 85 5f 9a ba e7 76 99 68 cc e7
Subject Alternative Name	Required, set to: 1. DNS=fully qualified domain name of the Subscriber's site, domain name remaining after removing "www." from the left hand portion of the fully qualified domain name. And/or: 2. DNS=domain name of Subscriber's site, domain name of additional sites which have undergone the following verification step as part of the authentication process: the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application (per 3.2.12)
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate
1.3.6.1.4.1.11129.2.4.2 (Extended Validation Certificates)	One or more RFC 6962 Signed Certificate Timestamps

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

The following certificate profile is used for Starfield branded Subscriber Certificates issued from the Starfield Issuing CA. At a minimum, the following fields will be populated as described, in accordance with IETF RFC 5280.

Field	Description
Version	V3
Serial Number	unique value with 64-bits of entropy for each certificate issued by the Issuing CA
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	serialNumber = 10688435 CN = Starfield Secure Certification Authority OU=http://certificates.starfieldtech.com/repository O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Valid From	Date and time of Certificate issuance
Valid To	A date up to the maximum permitted validity period at the time of issuance after Certificate issuance (depending on SSL certificate type).
Subject (Medium Assurance Certificates	CN = domain name of Subscriber's web site OU = "Domain Control Verified" or similar text indicating the assurance level of the certificate.
Subject (High Assurance Certificates	CN = domain name of Subscriber's web site O = Subscriber's organization or individual name L = City/town S = State C = Country
Subject (Extended Validation Certificates)	CN = domain name of Subscriber's web site O = Subscriber's full legal organization name. An assumed name or DBA may also be included L = City/town of place of business S = State of place of business C = Country of place of business serialNumber= Registration number assigned by incorporating authority or date of incorporation or registration businessCategory=vetting category used to issue certificate as defined in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates jurisdictionLocalityName= City/town of incorporation or registration (if applicable) jurisdictionStateOrProvinceName= State of incorporation or registration (if applicable) jurisdictionCountryName= Country of incorporation or registration
Subject Public Key Information	RSA (2048 bits or greater)

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Extensions:	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Key Usage (critical)	Digital Signature, Key Encipherment
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL =<current CRL URI> The specific URI will vary depending on certificate type and CRL scope.
Certificate Policies (Medium Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/
Certificate Policies (High Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/
Certificate Policies (Extended Validation Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.starfieldtech.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certificates.starfieldtech.com/repository/sf_intermediate.crt
Authority Key Identifier	KeyID: 49 4b 52 27 d1 1b bc f2 a1 21 6a 62 7b 51 42 7a 8a d7 d5 56

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Subject Alternative Name	Required, set to: 1. DNS=fully qualified domain name of the Subscriber's site, domain name remaining after removing "www." from the left hand portion of the fully qualified domain name. And/or: 2. DNS=domain name of Subscriber's site, domain name of additional sites which have undergone the following verification step as part of the authentication process: the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application (per 3.2.12)
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate
1.3.6.1.4.1.11129.2.4.2 (Extended Validation Certificates)	One or more RFC 6962 Signed Certificate Timestamps

The following certificate profile is used for Go Daddy branded Subscriber Certificates issued from the Go Daddy Issuing CA – G2. At a minimum, the following fields will be populated as described, in accordance with IETF RFC 5280.

Field	Description
Version	V3
Serial Number	unique value with 64-bits of entropy for each certificate issued by the Issuing CA
Signature Algorithm Identifier	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	CN = Go Daddy Secure Certificate Authority - G2 OU=http://certs.godaddy.com/repository/ O = GoDaddy.com, Inc. L = Scottsdale S = Arizona C = US
Valid From	Date and time of Certificate issuance
Valid To	A date up to the maximum permitted validity period at the time of issuance after Certificate issuance (depending on SSL certificate type).
Subject (Basic and Medium Assurance Certificates	CN = domain name of Subscriber's web site OU = "Domain Control Verified" or similar text indicating the assurance level of the certificate.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Subject (High Assurance Certificates	CN = domain name of Subscriber's web site O = Subscriber's organization or individual name L = City/town S = State C = Country
Subject (Extended Validation Certificates)	CN = domain name of Subscriber's web site O = Subscriber's full legal organization name. An assumed name or DBA may also be included L = City/town of place of business S = State of place of business C = Country of place of business serialNumber= Registration number assigned by incorporating authority or date of incorporation or registration businessCategory=vetting category used to issue certificate as defined in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates jurisdictionLocalityName= City/town of incorporation or registration (if applicable) jurisdictionStateOrProvinceName= State of incorporation or registration (if applicable) jurisdictionCountryName= Country of incorporation or registration
Subject Public Key Information	RSA (2048 bits or greater)
Extensions:	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Key Usage (critical)	Digital Signature, Key Encipherment
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = <current CRL URI> The specific URI will vary depending on certificate type and CRL scope.
Certificate Policies (Basic and Medium Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114413.1.7.23.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.2.1

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Certificate Policies (High Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114413.1.7.23.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.2.2 (OV) or 2.23.140.1.2.3 (IV)
Certificate Policies (Extended Validation Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114413.1.7.23.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.1
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.godaddy.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certificates.godaddy.com/repository/gdig2.crt
Authority Key Identifier	KeyID: 40 c2 bd 27 8e cc 34 83 30 a2 33 d7 fb 6c b3 f0 b4 2c 80 ce
Subject Alternative Name	Required, set to: 1. DNS=fully qualified domain name of the Subscriber's site, domain name remaining after removing "www." from the left hand portion of the fully qualified domain name. And/or: 2. DNS=domain name of Subscriber's site, domain name of additional sites which have undergone the following verification step as part of the authentication process: the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application (per 3.2.12)
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate
1.3.6.1.4.1.11129.2.4.2 (Extended Validation Certificates)	One or more RFC 6962 Signed Certificate Timestamps

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

The following certificate profile is used for Starfield branded Subscriber Certificates issued from the Starfield Issuing CA – G2. At a minimum, the following fields will be populated as described, in accordance with IETF RFC 5280.

Field	Description
Version	V3
Serial Number	unique value with 64-bits of entropy for each certificate issued by the Issuing CA
Signature Algorithm Identifier	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	CN = Starfield Secure Certificate Authority - G2 OU=http://certs.starfield.com/repository/ O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Valid From	Date and time of Certificate issuance
Valid To	A date up to the maximum permitted validity period at the time of issuance after Certificate issuance (depending on SSL certificate type).
Subject (Basic and Medium Assurance Certificates	CN = domain name of Subscriber's web site OU = "Domain Control Verified" or similar text indicating the assurance level of the certificate.
Subject (High Assurance Certificates	CN = domain name of Subscriber's web site O = Subscriber's organization or individual name L = City/town S = State C = Country

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Subject (Extended Validation Certificates)	CN = domain name of Subscriber's web site O = Subscriber's full legal organization name. An assumed name or DBA may also be included L = City/town of place of business S = State of place of business C = Country of place of business serialNumber= Registration number assigned by incorporating authority or date of incorporation or registration businessCategory=vetting category used to issue certificate as defined in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates jurisdictionLocalityName= City/town of incorporation or registration (if applicable) jurisdictionStateOrProvinceName= State of incorporation or registration (if applicable) jurisdictionCountryName= Country of incorporation or registration
Subject Public Key Information	RSA (2048 bits or greater)
Extensions:	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Key Usage (critical)	Digital Signature, Key Encipherment
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = <current CRL URI> The specific URI will vary depending on certificate type and CRL scope.
Certificate Policies (Basic and Medium Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.2.1

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Certificate Policies (High Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.2.2 (OV) or 2.23.140.1.2.3 (IV)
Certificate Policies (Extended Validation Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.1
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.starfieldtech.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certificates.starfieldtech.com/repository/sfig2.crt
Authority Key Identifier	KeyID: 25 45 81 68 50 26 38 3d 3b 2d 2c be cd 6a d9 b6 3d b3 66 63
Subject Alternative Name	Required, set to: 1. DNS=fully qualified domain name of the Subscriber's site, domain name remaining after removing "www." from the left hand portion of the fully qualified domain name. And/or: 2. DNS=domain name of Subscriber's site , domain name of additional sites which have undergone the following verification step as part of the authentication process: the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application (per 3.2.12)
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
1.3.6.1.4.1.11129.2.4.2 (Extended Validation Certificates)	One or more RFC 6962 Signed Certificate Timestamps

10.5 End Entity Code Signing Certificates

The following certificate profile is used for Go Daddy branded Subscriber Certificates issued from the Go Daddy Issuing CA. At a minimum, the following fields will be populated as described, in accordance with IETF RFC 5280.

Field	Description
Version	V3
Serial Number	unique value for each certificate issued by the Issuing CA
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	serialNumber = 07969287 CN = Go Daddy Secure Certification Authority OU=http://certificates.godaddy.com/repository O = GoDaddy.com, Inc. L = Scottsdale S = Arizona C = US
Valid From	Date and time of Certificate issuance
Valid To	A date up to 39 months after Certificate issuance
Subject	CN = Subscriber's organization name O = Subscriber's organization name L = City/town S = State C = Country
Subject Public Key Information	RSA (2048 bits or greater)
Extensions:	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)
Key Usage (critical)	Digital Signature
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = <current CRL URI> The specific URI will vary depending on certificate type and CRL scope.

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.840.1.114413.1.7.23.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.godaddy.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certificates.godaddy.com/repository/gd_intermediate.crt
Authority Key Identifier	fd ac 61 32 93 6c 45 d6 e2 ee 85 5f 9a ba e7 76 99 68 cc e7
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate

The following certificate profile is used for Starfield branded Subscriber Certificates issued from the Starfield Issuing CA. At a minimum, the following fields will be populated as described, in accordance with IETF RFC 5280.

Field	Description
Version	V3
Serial Number	unique value for each certificate issued by the Issuing CA
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	serialNumber = 10688435 CN = Starfield Secure Certification Authority OU=http://certificates.starfieldtech.com/repository O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Valid From	Date and time of Certificate issuance
Valid To	A date up to 39 months after Certificate issuance
Subject	CN = Subscriber's organization name O = Subscriber's organization name L = City/town S = State C = Country
Subject Public Key Information	RSA (2048 bits or greater)

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Extensions:	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)
Key Usage (critical)	Digital Signature
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = <current CRL URI> The specific URI will vary depending on certificate type and CRL scope.
Certificate Policies (High Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.starfieldtech.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certificates.starfieldtech.com/repository/sf_intermediate.crt
Authority Key Identifier	49 4b 52 27 d1 1b bc f2 a1 21 6a 62 7b 51 42 7a 8a d7 d5 56
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate

The following certificate profile is used for Go Daddy branded Subscriber Certificates issued from the Go Daddy Secure Certificate Authority – G2 or the Go Daddy Secure Extended Validation Code Signing CA – G2. At a minimum, the following fields will be populated as described, in accordance with IETF RFC 5280.

Field	Description
Version	V3
Serial Number	unique value for each certificate issued by the Issuing CA
Signature Algorithm Identifier	SHA-256
Issuer	Subject of corresponding Issuing CA certificate
Valid From	Date and time of Certificate issuance

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Valid To	A date up to 39 months after Certificate issuance
Subject	CN = Subscriber's organization name O = Subscriber's organization name L = City/town S = State C = Country
Subject (Extended Validation Certificates)	O = Subscriber's full legal organization name. An assumed name or DBA may also be included L = City/town of place of business S = State of place of business C = Country of place of business serialNumber= Registration number assigned by incorporating authority or date of incorporation or registration businessCategory=vetting category used to issue certificate as defined in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates jurisdictionLocalityName= City/town of incorporation or registration (if applicable) jurisdictionStateOrProvinceName= State of incorporation or registration (if applicable) jurisdictionCountryName= Country of incorporation or registration
Subject Public Key Information	RSA (2048 bits or greater)
Extensions:	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Code Signing (1.3.6.1.5.5.7.3.3) Optional: Kernel Mode Code Signing (1.3.6.1.4.1.311.61.1.1)
Key Usage (critical)	Digital Signature
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = <current CRL URI> The specific URI will vary depending on certificate type and CRL scope.
Certificate Policies (High Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114413.1.7.23.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository [2]Certificate Policy: Policy Identifier=2.23.140.1.4.1

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Certificate Policies (Extended Validation Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114413.1.7.24.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.3
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.godaddy.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certificates.godaddy.com/repository/gdig2.crt
Authority Key Identifier	SHA-1 hash of the public of the corresponding Issuing CA
Subject Key Identifier	SHA-1 hash of the public key contained within this certificate

The following certificate profile is used for Starfield branded Subscriber Certificates issued from the Starfield Secure Certificate Authority – G2 or the Starfield Secure Extended Validation Code Signing CA – G2. At a minimum, the following fields will be populated as described, in accordance with IETF RFC 5280.

Field	Description
Version	V3
Serial Number	unique value for each certificate issued by the Issuing CA
Signature Algorithm Identifier	SHA-256
Issuer	Subject of corresponding Issuing CA certificate
Valid From	Date and time of Certificate issuance
Valid To	A date up to39 months after Certificate issuance
Subject	CN = Subscriber's organization name O = Subscriber's organization name L = City/town S = State C = Country

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Subject (Extended Validation Certificates)	O = Subscriber's full legal organization name. An assumed name or DBA may also be included L = City/town of place of business S = State of place of business C = Country of place of business serialNumber= Registration number assigned by incorporating authority or date of incorporation or registration businessCategory=vetting category used to issue certificate as defined in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates jurisdictionLocalityName= City/town of incorporation or registration (if applicable) jurisdictionStateOrProvinceName= State of incorporation or registration (if applicable) jurisdictionCountryName= Country of incorporation or registration
Subject Public Key Information	RSA (2048 bits or greater)
Extensions:	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Code Signing (1.3.6.1.5.5.7.3.3) Optional: Kernel Mode Code Signing (1.3.6.1.4.1.311.61.1.1)
Key Usage (critical)	Digital Signature
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = <current CRL URI> The specific URI will vary depending on certificate type and CRL scope.
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.4.1
Certificate Policies (Extended Validation Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.24.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.3

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.

Field	Description
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.starfieldtech.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certificates.starfieldtech.com/repository/gdig2.crt
Authority Key Identifier	SHA-1 hash of the public of the corresponding Issuing CA
Subject Key Identifier	SHA-1 hash of the public key contained within this certificate

Copyright © 2004-2019 Starfield Technologies, LLC All rights reserved.