Starfield Technologies, LLC

Certificate Policy
and
Certification Practice Statement
(CP/CPS)

Version 5.01
April 1, 2024

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 TLS Server Certificates* as well as *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 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**

Note: References to Baseline Requirements sections are denoted in short form using the section number. For example [BR 3.2.2.1] denotes section 3.2.2.1 of the current revision of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates.

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 • 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

Version	Effective Date	Change Summary
4.3	May 26, 2020	• Updated section 7.2 to show both versions of CRL
4.4	June 19, 2020	• Updated section 4.9.4 in accordance to BRs
4.5	July 23, 2020	• Removed the G3 and G4 roots from 1.3.1, 3.2.2.4.9 and Appendix A
4.6	July 30, 2020	• Updated link to repository in section 2.1
4.7	August 31, 2020	• Updated section 6.3.2 to reflect 398 day maximum validity period • Updated section 2.1 to reflect updated repository link
4.8	September 30, 2020	• Updated 7.2.2.1 and 7.2.2.2 to remove reason code 6 • Updated section 3.2 to add link to agency disclosure list • Updated sections 10.4 and 10.5 to reflect SHA2 • Updates section 8.6 to acknowledge new audit requirements
4.9	October 21, 2020	• Added section 9.16.5 Force Majeure • Updated sections 1.6 and 4.9.1 to add definitions and details to revocation
4.10	April 19, 2021	• Updated section 1.5.2 with more clear instructions for Certificate Problem Report • Updated section 4.2.2 to indicate that SOD is also applicable to Code Signing • Updated section 5.4.3 to reflect the 7 years retention period for audit log
4.11	June 10, 2021	• Updated section 1.4 to indicate Code signing EOL as of May 30, 2021 • Updated section 4.9.12 to specify methods used to demonstrate private key compromise
4.12	July 9, 2021	• Updated section 1.4 to reflect Code Signing policy updates in relation to Code Signing EOL • Updated section 1.5.2 to reflect new company address • Updated section 3.2.2 header to include Domain • Added section 3.2.2.4.20 TLS Using ALPN (Ballot SC33) • Removed Code Signing references in the following sections: 1.1, 3.2, 4.2.2, 6.3.2, 7.1.6, 8.7, 10.2 • Updated section 10.5 in relation to Code Signing EOL
4.13	September 8, 2021	• Updated section 10.4 to reflect removal of OU (Ballot SC47) • Ballot SC48 clean up: o Replaced all instances of Fully Qualified with Fully-Qualified o Added and updated some definitions in 1.6.1 o Updated applicable sections under 3.2.2.4 to replace instances of label(s) with Domain Label(s) • Added subsections to 7.1.4 Name Forms: 7.1.4.1, 7.1.4.2, 7.1.4.2.1, 7.1.4.2.2, 7.1.4.3, 7.1.4.3.1. • Added 3.2.2.5 Authentication for an IP Address, and 3.2.2.6 Wildcard Domain Validation. Re-numbered Data Source Accuracy to 3.2.2.7.
4.14	October 15, 2021	• Updated sections 4.9.7, 4.9.10, 7.2.2.1, and 7.2.2.2 regarding OSCP and CRL timeframes.
4.15	November 29, 2021	• Updated sections 3.2.2.4.18 and 3.2.2.4.19 regarding redirects and Wildcard Domain Names
4.16	March 9, 2022	• Updated sections 3.2.2.4.20, 3.4, 4.2.1, 4.2.3, 4,9.2, 4.9.3, 4.9.7, 4.9.10, and 9.1.5 to account for Certainly CPS alignment. • Cleaned up formatting in sections 1.5.3, 1.6, and 8.6. • Fixed references in sections 2.3, 6.1.1, 6.1.6, and 6.2.1. • Updated section 4.9.1 and subsections, to be in-line with BR formatting, and include timeframes.
4.17	June 17, 2022	• Updated audit log retention in section 5.4.3 • Updated section 9.9 to include indemnification by Starfield • Added definition of Application Software Supplier in section 1.6
4.18	November 11, 2022	• Corrected spelling mistake in 1.3.1 • Added Certainly to 1.3.1 diagram • Increased diagram sizes for readability • Added 2 new roots to 10.1 • Added 2 new Cross CA Certs to 10.3

Version	Effective Date	Change Summary
5.0	August 1, 2023	• Added Appendices for Test Sites, adjusted formatting of appendices • Added Definitions and Acronyms in 1.6.1 to align with CA/B forum definitions as well as ensure all acronyms used are pre-defined • Updated reference URLs within this document to display the Section name as well as the section number • Introduced [BR X.XX] formatting to delineate CA/B Forum alignment sections from CP/CPS sections • Updated formatting: Section indentation, table formatting, font styling • Added new Section 3.2.2.8 CAA Records • Added text to Section 5 for BR alignment • Added References to new Section 1.6.2 • Added clarifying text to 4.2.1 • Added lastUpdate/nextUpdate clarification to 4.9.7 • Added bullet expansion to 5.4.1 for CA/B alignment • Added 1.6.3 Conventions • Added 7.2.2 text and modified 7.2.2.1 and 7.2.2.2 for CAB alignment • Added 7.3 text for CAB alignment • Updated 4.9.1.1 and 4.9.1.2 for CAB alignment
5.01	April 1, 2024	• Updated 1.3.3 to clarify when Starfield may act as a subscriber • Added definition for short lived certificate to 1.6.1 • Added RFC8954 as a reference in 1.6.2 • Updated to allow use of FIPS 140-2 or FIPS 140-3 • Updated references to the Baseline Requirements • Updated term from “Random Number” to “Random Value” in sections 3.2.2.4.10 and 3.2.2.4.18 • Updated CRL frequency to align with current business practices • Updated contact address in 1.5.2 • Updated 5.4.1 to align with BR update • Added 5.4.1.1 to align with BR update

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

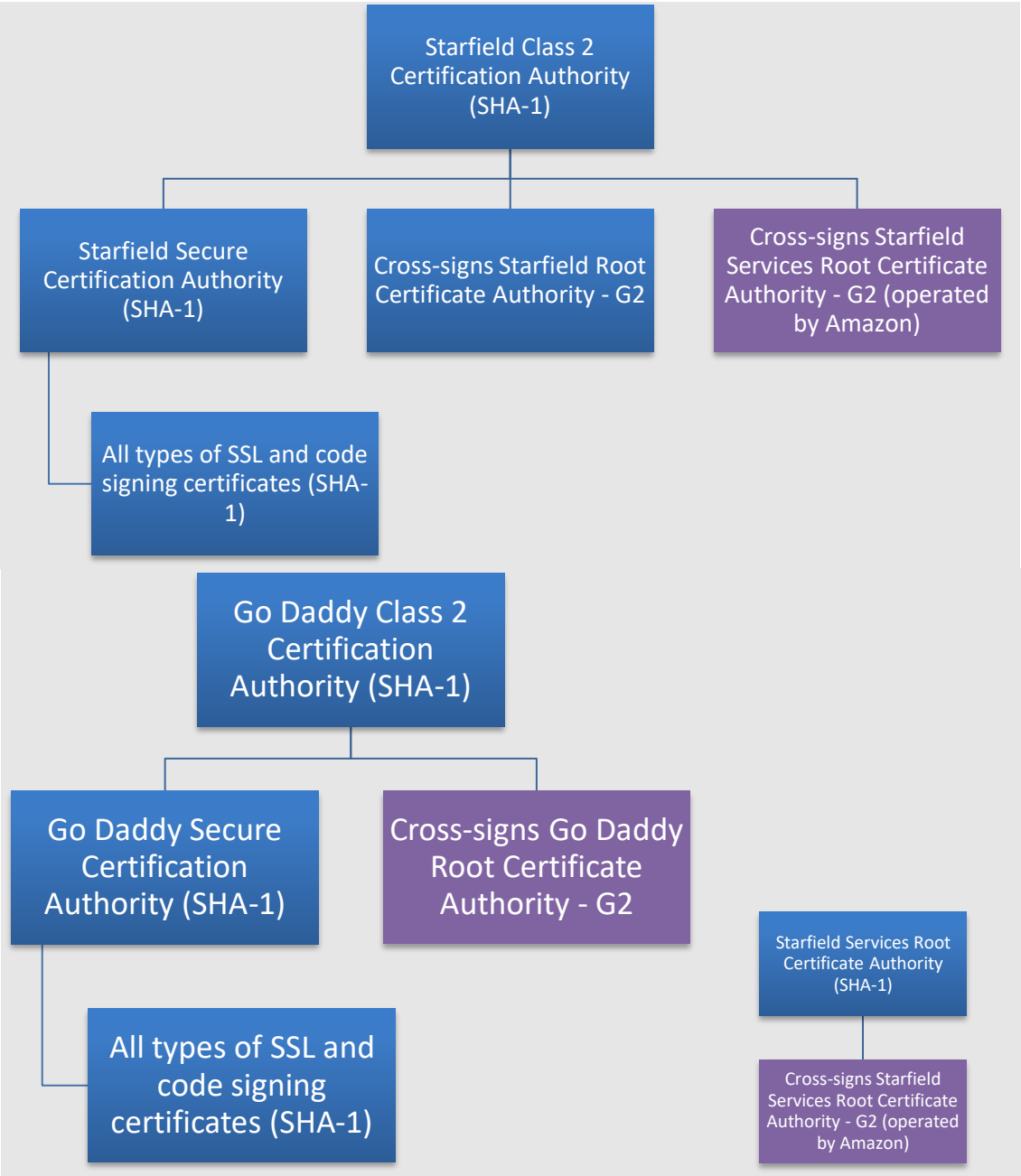
Starfield Certification Authorities (CAs) perform the following general functions:

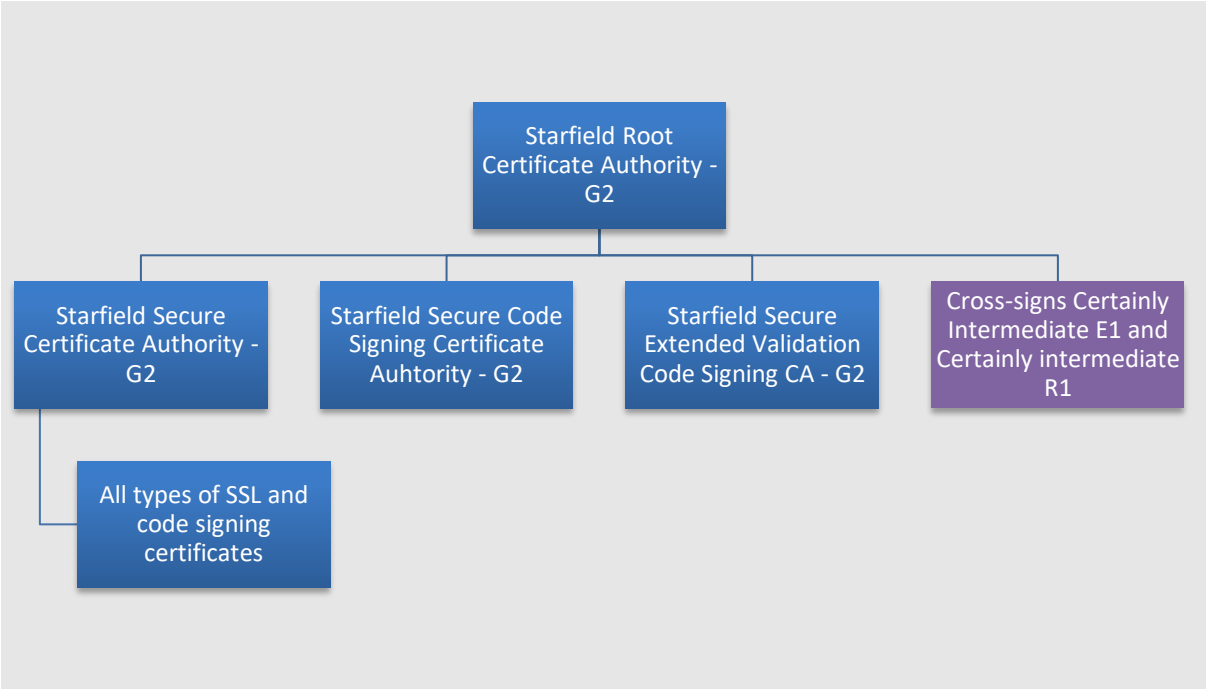
- Create and sign certificates
- Distribute certificates to the appropriate Subscribers and Relying Parties
- Revoke certificates
- Distribute certificate status information in the form of Certificate Revocation Lists (CRLs) or other mechanisms
- Provide a repository where certificates and certificate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

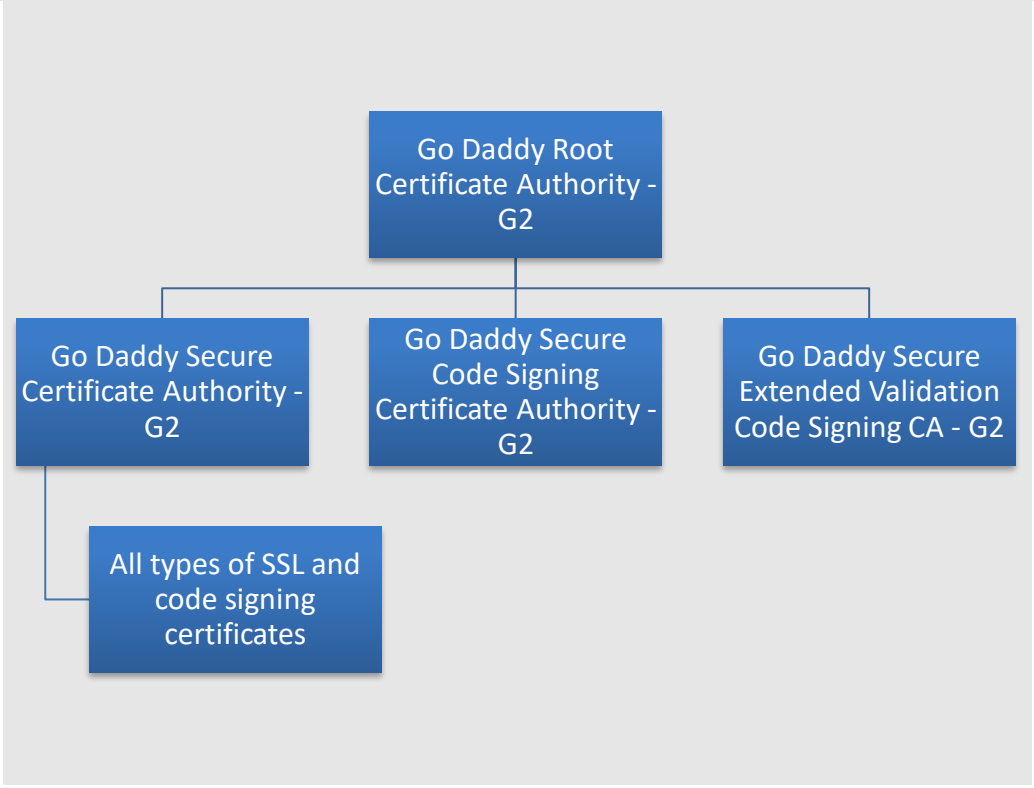
Obligations of the CAs within the Starfield PKI include:

- 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:







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. In some situations, Starfield may act as an Applicant or Subscriber, for instance, when it generates and protects a Private Key, requests a Certificate, demonstrates control of a Domain, or obtains a Certificate for its own use.

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
- 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 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)

Note: As of May 30, 2021, Starfield no longer issues High Assurance Code Signing Certificates and will no longer update this CP/CPS for Code Signing related changes to the Baseline Requirements. Code Signing references were removed in v4.12. Refer to Certificate Policy and Certification Practice Statement v4.11 in Starfield's Repository, for most recent policy containing Code Signing references.

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.

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
100 S Mill Ave, Suite 1600
Tempe, AZ 85281
Phone: 480-505-8800
E-mail: practices@starfieldtech.com

In case of a Certificate Problem Report, that concerns a key compromised certificate, a mis-issued certificate, or any other type of suspicious activity with a certificate, contact us at (480) 505-8852, or 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 a 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, Acronyms, and References

1.6.1 Definitions and Acronyms

Term	Acronym	Definition
Affiliate		A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
American Institute of Certified Public Accountants	AICPA	American Institute of Certified Public Accountants
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 been delegated authority to represent the Applicant.
Application-Layer Protocol Negotiation	ALPN	A TLS Extension that includes the protocol negotiation within the exchange of hello messages.
Application Software Supplier		A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
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.
Audit Period		In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1 Frequency or Circumstances of Assessment
Audit Report		A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
Authorization Domain Name	AND	The FQDN returned in defined processes to obtain authorization for inclusion in a Certificate.
Authorized Port		One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).

Term	Acronym	Definition
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. (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
Basic Assurance		Starfield's vetting process that verifies an Applicant's access to the domain.
Baseline Requirements	BR [BR X.X]	*Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates* published by the CA/Browser Forum. References to Baseline Requirements sections are denoted in short form using the section number. For example [BR 3.2.2.1] denotes section 3.2.2.1 of the current revision of the *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates*.
Certificate Authority Authorization	CAA	A DNS Resource Record defined further in RFC 8659.
CA Key Pair		A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).
Certificate		Digital record that contains information such as the Subscriber's distinguished name and public key, and the signer's signature and data.
Certificate Data		Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
Certificate Management Process		Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Policy	CP	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
Certificate Problem Report		Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Profile		A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 Certificate, CRL, and OCSP Profiles, e.g. a Section in a CA's CPS or a certificate template file used by CA software.
Certificate Revocation List	CRL	A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
Certificate Signing Request	CSR	A message sent to the certification authority containing the information required to issue a digital certificate.
Certification Authority	CA	Certificate Issuing entity defined further in Section 1.3.1 Certificate Authorities of this document.
Certification Practice Statement	CPS	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
Canonical Name	CNAME	A DNS resource record to provide the canonical name associated with an alias name further defined in RFC 2181 Section 10.1.
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.
Country		Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.
Country code top-level domain	ccTLD	An internet top level domain reserved for a country or dependent territory.
Cross Certificate		A certificate that is used to establish a trust relationship between two Root CAs.
Custom Certificate		A certificate profile defined for a specific, non-standard usage.
Delegated Third Party		A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
Distinguished Name	DN	A globally unique identifier representing a Subscriber.
Doing Business As	DBA	An entity name or trade name used for Subject Identity Information
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 Label		A portion of an FQDN further defined in RFC 8499 Section 2
Domain Name		An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

Term	Acronym	Definition
Domain Namespace		The set of all possible Domain Names that are subordinate to a single 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.
Domain Name Registrar		An entity that manages the reservation of internet domain names.
Domain Naming Service	DNS	An internet service used to map IP addresses to domain names.
Expiry Date		The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
Extended Validation	EV	Certificate issued under the Guidelines for the Issuance and Management of Extended Validation Certificates published by the CA/Browser Forum.
Fully-Qualified Domain Name	FQDN	An absolute Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.
Generic top-level domain	gTLD	A category of top-level domains maintained by the Internet Assigned Numbers Authority.
Government Entity		A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
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.
Internal Name		A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.
International Organization for Standardization	ISO	An independent, non-governmental international organization with a membership of 167 national standards bodies.
Internationalized Domain Name	IDN	An Internet domain name that contains at least one label displayed in software applications, in whole or in part, in non-latin script or alphabet.
Internet Assigned Numbers Authority	IANA	The organization responsible for overseeing the allocation unique names and numbers used in technical standards.
Internet Corporation for Assigned Names and Numbers	ICANN	The nonprofit organization overseeing the use of internet domains.
Internet Protocol	IP	A network layer communications protocol used for addressing and routing.
IP Address		A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication
IP Address Contact		The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.
IP Address Registration Authority		The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
Issuer		An entity that issues certificates.
Issuing CA		In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise		A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Generation Script		A documented plan of procedures for the generation of a CA Key Pair.
Key Pair		The Private Key and its associated Public Key.
LDH Label		The label form and syntax definition for host names further defined in RFC 5890 Section 2.3.1
Legal Entity		An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Medium Assurance		Starfield's vetting process that verifies access to the domain.
National Institute of Standards and Technology	NIST	US Government Department of Commerce agency for advancing measurements, science, and technology.
Non-Reserved LDH Label		Non-Reserved LDH labels are the set of valid LDH labels that do not have "--" in the third and fourth positions as defined in RFC 5890 Section 2.3.1
Object Identifier	OID	A unique identifier issued to an organization by IANA.
Onion Domain Name		A Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name.

Term	Acronym	Definition
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.
OSCP Responder		An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests.
P-Label		A XN-Label that contains valid output of the Punycode algorithm as defined in RFC 3492 Section 6.3 from the fifth and subsequent positions.
Place of Business		The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.
Policy Authority	PA	The entity responsible for identifying and maintaining requirements for a Public Key Infrastructure
Policy Authority Committee	PAC	The Starfield committee which creates and maintains the policies related to the Starfield Public Key Infrastructure. Also known as the Governance and Policy Committee (GPC).
Private Key		The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key		The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure	PKI	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
Public Suffix List	PSL	A list of usable domain suffixes as defined by ICANN.
Publicly-Trusted Certificate		A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor		A natural person or Legal Entity that meets the requirements of Section 8.2 Identity/Qualifications of Assessor.
Random Value		A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Registered Domain Name		A Domain Name that has been registered with a Domain Name Registrar.
Registration Authority	RA	Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
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.
Repository		An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Request for Comment	RFC	A publication in a series from the principal technical development and standards-setting bodies for the Internet, most prominently the Internet Engineering Task Force (IETF).
Request Token		A value, derived in a method specified by the CA which binds this demonstration of control to the certificate request.
Required Website Content		Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
Reseller		A person or organization which is given permission by Starfield to sell products to Subscribers
Reserved IP Address		An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml
Root CA		The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Term	Acronym	Definition
Root Certificate		The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
Short-lived Subscriber Certificate		For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).
Secure Socket Layer	SSL	Deprecated transport layer protocol for securing communications. Acronym is still used in lieu of TLS, the superseding protocol. In the context of this document, SSL implies TLS.
Starfield		Starfield Technologies, LLC, and its resellers.
Starfield PKI		The Starfield Public Key Infrastructure that provides Certificates for individuals and entities.
Start of Authority	SOA	A DNS resource record containing administrative information about the base DNS zone marking the start of the zone of authority.
Subject		The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Alternative Name	SAN	Optional certificate extension defined in RFC 5280.
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
Subordinate CA		A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
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.
Technically Constrained Subordinate CA Certificate		A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.
Terms of Use		Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
Trustworthy System		Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
Transport Layer Security	TLS	Protocol used for secure communications over the transport layer of networking leveraging encryption and certificates.
Unified Communications Certificate	UCC	Certificate that includes multiple Fully-Qualified Domain Names in the Subject Alternative Name extension used for unified communications.
Unregistered Domain Name		A Domain Name that is not a Registered Domain Name.
Valid Certificate		A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialist		Someone who performs the information verification duties specified by these Requirements.
Validity Period		From RFC 5280: “The period of time from notBefore through notAfter, inclusive.”
WHOIS		A query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource such as a domain name.
Wildcard Certificate		A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.
Wildcard Domain Name		A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.
XN-Label		A subset of LDH labels further defined in RFC 5890 Section 2.3.1.

1.6.2 References

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

FIPS 140-3, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, March 22, 2019.

FIPS 186-4, Federal Information Processing Standards Publication - Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, July 2013.

ISO 21188:2006, Public key infrastructure for financial services – Practices and policy framework.
Network and Certificate System Security Requirements, Version 1.7
https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Guidelines-v1.7.pdf.

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications
http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. March 1997.
RFC3492, Request for Comments: 3492, Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA). A. Costello. March 2003.
RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. S. Chokhani, et al. November 2003.
RFC3912, Request for Comments: 3912, WHOIS Protocol Specification. L. Daigle. September 2004.
RFC3986, Request for Comments: 3986, Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, et al. January 2005.
RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments. A. Deacon, et al. September 2007.
RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. D. Cooper, et al. May 2008.
RFC5890, Request for Comments: 5890, Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. J. Klensin. August 2010.
RFC5952, Request for Comments: 5952, A Recommendation for IPv6 Address Text Representation. S. Kawamura, et al. August 2010.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. S. Santesson, et al. June 2013.
RFC6962, Request for Comments: 6962, Certificate Transparency. B. Laurie, et al. June 2013.
RFC7231, Request For Comments: 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. R. Fielding, et al. June 2014.
RFC7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format. A. Newton, et al. March 2015.
RFC7538, Request For Comments: 7538, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect). J. Reschke. April 2015.
RFC8499, Request for Comments: 8499, DNS Terminology. P. Hoffman, et al. January 2019.
RFC8659, Request for Comments: 8659, DNS Certification Authority Authorization (CAA) Resource Record. P. Hallam-Baker, et al. November 2019.
RFC8738, Request for Comments: 8738, Automated Certificate Management Environment (ACME) IP Identifier Validation Extension. R.B.Shoemaker, Ed. February 2020.
RFC8954, Request for Comments: 8954, Online Certificate Status Protocol (OCSP) Nonce Extension. M. Sahni, Ed. November 2020.

WebTrust for Certification Authorities, SSL Baseline with Network Security, available at https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria.

X.509, Recommendation ITU-T X.509 (08/2005) | ISO/IEC 9594-8:2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

1.6.3 Conventions

Terms not otherwise defined in these Requirements shall be as defined in applicable agreements, user manuals, Certificate Policies and Certification Practice Statements, of Starfield.

The key words “MUST”, “MUST NOT”, "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements shall be interpreted in accordance with RFC 2119.

By convention, this document omits time and time zones when listing effective requirements such as dates. Except when explicitly specified, the associated time with a date shall be 00:00:00 UTC.

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 https://certs.secureserver.net/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. This CP/CPS is structured in accordance with RFC 3647 in alignment with the most recent published version of the CA/B Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates*.

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 Section 4.9.7 CRL Issuance Frequency and Section 4.9.10 On-line Revocation Checking Requirements.

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.

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 Section 7.1 Certificate Profile.

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 Types of Names

3.1.5 Uniqueness of Names

Refer to Sections 3.1.1 Types of Names and 3.1.6 Recognition, Authentication and Role of Trademarks.

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:

- the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application using the methods described in Section 3.2.2.4 Validation of Domain Authorization or Control.

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 Section 3.2.2.4 Validation of Domain Authorization or Control.
- the individual requesting the certificate is authorized to do so by the organization named in the certificate using the methods described in Section 3.2.5 Validation of Authority
- the organization name represents an organization validated using the methods described in Section 3.2.2 Authentication of Organization and Domain Identity.

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

Note: Effective as of 1 October 2020, before using an incorporating or registration agency for validation of an Extended Validation Certificate, that agency is disclosed publicly via https://ssltools.godaddy.com/compliance/Approved_Incorporating_and_Registration_Agencies.xlsx.
This document, Approved Incorporating and Registration Agencies, contains the name of the agency, jurisdiction(s) and website information as well as a document history including version numbers and publication dates for all edits.

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 and Domain 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.

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 Section 3.2.2.1 Identity.

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 [BR 3.2.2.6].

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 Section 4.6 Certificate Renewal.

In compliance with the CA / Browser Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server 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:

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.

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.

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.

Note: 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.

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.

Note: 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 Domain Label that begins with an underscore character.

If a Random Value is used, Starfield or Delegated Third Party SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate.

3.2.2.4.8 **IP Address**

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.

3.2.2.4.10 **TLS Using a Random Value**

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.

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**

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 Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

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.

1. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and
2. The CA 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 Value:
1. MUST be located on the Authorization Domain Name, and
2. MUST be located under the "/.well-known/pki-validation" directory, and
3. MUST be retrieved via either the "http" or "https" scheme, and
4. MUST be accessed over an Authorized Port.

If the CA follows redirects, the following apply:
1. Redirects MUST be initiated at the HTTP protocol layer.
a. For validations performed on or after December 1, 2021, redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
b. For validations performed prior to December 1, 2021, 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. CAs SHOULD limit the accepted status codes and resource URLs to those defined within 1.a.
2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
3. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:
1. The CA MUST provide a Random Value unique to the certificate request.
2. The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation.

Note:

**For Certificates issued prior to December 1, 2021, 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.*
**For Certificates issued on or after December 1, 2021, Starfield MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless Starfield performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.*

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.

Note:
**For Certificates issued prior to December 1, 2021, 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.*
**For Certificates issued on or after December 1, 2021, Starfield MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless Starfield performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.*

3.2.2.4.20 **TLS Using ALPN**

While the issuing CAs under Starfield's direct control, do not use this method of validation, Certainly issuing CAs MAY confirm the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737. The following are additive requirements to RFC 8737

Note: Once the FQDN has been validated using this method, Starfield MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless Starfield performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.5 Authentication for an IP Address

No IP address certificates are issued under this CPS.

3.2.2.6 Wildcard Domain Validation

Before issuing a Wildcard Certificate, Starfield MUST establish and follow a documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate is "registry-controlled" or is a "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public suffix", CAs MUST refuse issuance unless the Applicant proves its rightful control of the entire

Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a "public suffix list" such as the Public Suffix List (PSL), and to retrieve a fresh copy regularly.

If using the PSL, a CA SHOULD consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.

3.2.2.7 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.

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.

3.2.2.8 CAA Records

As part of the Certificate issuance process, the Starfield MUST retrieve and process CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an Onion Domain Name. If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

This stipulation does not prevent the CA from checking CAA records at any other time.

When processing CAA records, CAs MUST process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. CAs MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.

RFC 8659 requires that CAs "MUST NOT issue a certificate unless the CA determines that either (1) the certificate request is consistent with the applicable CAA RRset or (2) an exception specified in the relevant CP or CPS applies."

Note: Starfield does not issue certificates for Onion Domain Names

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 Section 3.2.2.4 Validation of Domain Authorization or Control.
- 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 Starfield 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 Cross CA Certificates for all cross certificates that identify the CA as the Subject.

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 Section 3.2 Initial Identity Validation.

3.4 Identification and Authentication for Revocation Request

Section 4.9 Certificate Revocation and Suspension describes requirements for identification and authentication of revocation requests.

When revocation is initiated by Starfield, identification and authentication is not required.

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 Section 3.2 Initial Identity Validation.

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 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server 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 may be subjected to additional verification procedures.

In cases where the certificate request does not contain all the necessary information about the Applicant, the Starfield shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant.

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 EV Certificates.

4.2.3 Time to Process Certificate Applications

Certificate applications made to CAs under Starfield's direct control may be rejected if domain validation is not completed within 45 days from certificate request. 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 Section 4.2.1 Performing Identification and Authentication Functions and Section 3.2 Initial Identity Validation.

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:

- 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.

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 Section 3.2 Initial Identity Validation) 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 Section 4.4.1 Conduct Constituting Certificate Acceptance.

4.6.6 Publication of the Renewal Certificate by the CA

As described in Section 4.4.2 Publication of the Certificate by the CA.

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 Section 4.6.3 Processing Certificate Renewal Requests).

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 Section 4.4.1 Conduct Constituting Certificate Acceptance.

4.7.6 Publication of the Re-keyed Certificate by the CA

As described in Section 4.4.2 Publication of the Certificate by the CA.

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 Section 4.6.3 Processing Certificate Renewal Requests).

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 Section 4.4.1 Conduct Constituting Certificate Acceptance.

4.8.6 Publication of the Modified Certificate by the CA

As described in Section 4.4.2 Publication of the Certificate by the CA.

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

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Starfield SHALL revoke a Certificate within 24 hours and using the corresponding CRL Reason from Section 7.2.2 CRL and CRL Entry Extensions if one or more of the following occurs:

1. The Subscriber requests in writing that Starfield, without specifying a reason, revoke the Certificate (CRLReason "**unspecified** (0)" which results in no ReasonCode extension being provided);
2. The Subscriber notifies Starfield that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason 9, **privilegeWithdrawn**);
3. Starfield obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason 1, **keyCompromise**);
4. Starfield is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate, such as a Debian weak key, see https://wiki.debian.org/SSLkeys(CRLReason 1, **keyCompromise**);
5. Starfield obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason 4, **superseded**);.

Starfield may revoke a certificate within 24 hours and will revoke a Certificate within 5 days and use the corresponding CRLReason if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Section 6.1.5 Key Sizes and Section 6.1.6 Public Key Parameters Generation and Quality Checking of this CP/CPS (CRLReason 4, **superseded**);
2. Starfield obtains evidence that the Certificate was misused (CRLReason 9, **privilegeWithdrawn**);
3. Starfield is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason 9, **privilegeWithdrawn**);
4. Starfield is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason 5, **cessationOfOperation**);
5. Starfield is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason 9, **privilegeWithdrawn**);
6. Starfield is made aware of a material change in the information contained in the Certificate (CRLReason 9, **privilegeWithdrawn**);
7. Starfield is made aware that the Certificate was not issued in accordance with these Requirements or this CP/CPS (CRLReason 4, **superseded**);
8. Starfield determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason 9, **privilegeWithdrawn**);

9. Starfield's right to issue Certificates under these Requirements expires or is revoked or terminated, unless Starfield has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "**unspecified** (0)" which results in no reasonCode extension being provided in the CRL);
10. Revocation is required by this CP/CPS for a reason that is not otherwise required to be specified by this section (CRLReason "**unspecified** (0)" which results in no reasonCode extension being provided in the CRL); or
11. Starfield is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, **keyCompromise**).

If a CRL entry is for a Certificate not subject to these Requirements and was either issued on-or-after 2020-09-30 or has a **notBefore** on-or-after 2020-09-30, the CRLReason MUST NOT be **certificateHold** (6). If a CRL entry is for a Certificate subject to these Requirements, the CRLReason MUST NOT be **certificateHold** (6).

If a **reasonCode** CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the Certificate.

CRLReason MUST be included in the **reasonCode** extension of the CRL entry corresponding to a Subscriber Certificate that is revoked after July 15, 2023, unless the CRLReason is "**unspecified** (0)". Revocation reason code entries for Subscriber Certificates revoked prior to July 15, 2023, do NOT need to be added or changed.

Only the following CRLReasons MAY be present in the CRL **reasonCode** extension for Subscriber Certificates:

keyCompromise (RFC 5280 CRLReason #1): Indicates that it is known or suspected that the Subscriber's Private Key has been compromised;
affiliationChanged (RFC 5280 CRLReason #3): Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised;
superseded (RFC 5280 CRLReason #4): Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with the Baseline Requirements or this CP/CPS;
cessationOfOperation (RFC 5280 CRLReason #5): Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate; or
privilegeWithdrawn (RFC 5280 CRLReason #9): Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The Subscriber Agreement, or an online resource referenced therein, MUST inform Subscribers about the revocation reason options listed above and provide explanation about when to choose each option. Tools that the CA provides to the Subscriber MUST allow for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason "**unspecified** (0)" which results in no reasonCode extension being provided in the CRL).

The **privilegeWithdrawn** reasonCode SHOULD NOT be made available to the Subscriber as a revocation reason option, because the use of this reasonCode is determined by the CA and not the Subscriber.

When a CA obtains verifiable evidence of Key Compromise for a Certificate whose CRL entry does not contain a **reasonCode** extension or has a reasonCode extension with a non-keyCompromise reason, the CA SHOULD update the CRL entry to enter **keyCompromise** as the CRLReason in the **reasonCode** extension. Additionally, the CA SHOULD update the revocation date in a CRL entry when it is determined that the private key of the certificate was compromised prior to the revocation date that is indicated in the CRL entry for that certificate.

Note: Backdating the revocationDate field is an exception to best practice described in RFC 5280 section 5.3.*2; however, these requirements specify the use of the revocationDate field to support TLS implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.*

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

Starfield will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing(CRLReason "**unspecified** (0)" which results in no reasonCode extension being provided in the CRL);;
2. The Subordinate CA notifies Starfield that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason 9, **privilegeWithdrawn**);
3. Starfield obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 Key Sizes and Section 6.1.6 Public Key Parameters Generation and Quality Checking of this CP/CPS (CRLReason 1, **keyCompromise**);
4. Starfield obtains evidence that the Certificate was misused(CRLReason 9, **privilegeWithdrawn**);
5. Starfield is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement(CRLReason 9, **privilegeWithdrawn**);
6. Starfield determines that any of the information appearing in the Certificate is inaccurate or misleading(CRLReason 9, **privilegeWithdrawn**);
7. Starfield or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate(CRLReason 5, **cessationOfOperation**);

8. Starfield's or the Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless Starfield has made arrangements to continue maintaining the CRL/OCSP Repository(CRLReason "**unspecified** (0)" which results in no reasonCode extension being provided in the CRL); or
9. Revocation is required by Starfield's CP/CPS(CRLReason "**unspecified** (0)" which results in no reasonCode extension being provided in the CRL).

4.9.2 Who Can Request Revocation

Subscriber certificate revocation can be initiated by the Subscriber, Starfield, the Issuing CA, or authorized Resellers. Additionally, revocation requests can be initiated by anyone who can access the ACME API endpoint that can complete the revocation procedures in Section 4.9.3 Procedure for Revocation Request.

4.9.3 Procedure for Revocation Request

Starfield maintains a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

Revocations may be requested:

- by Subscribers via their online account, which are authenticated using a shared secret; or
- by Subscribers using the appropriate ACME API endpoint, if they can sign the revocation request with the associated account private key; or
- by anyone who can access the appropriate ACME API endpoint and sign a revocation request with the private key associated with the certificate; or
- by anyone who can access appropriate ACME API endpoint and demonstrate control over all domains in the Subject.

If the revocation request cannot be authenticated using a shared secret or through the ACME endpoint, the RA must perform sufficient procedures to authenticate the revocation request 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 10 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 to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1 Reasons for Revoking a Subscriber Certificate. 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 CAs under Starfield's direct control 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 24 hours

The value of the nextUpdate field MUST NOT be more than 365 days beyond the value of the thisUpdate field for Root CAs and 10 days for Issuing CAs.

If Certainly publishes a CRL, they will do it in compliance with the CA / Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, and their CP/CPS.

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.

The following SHALL apply for communicating the status of Certificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

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

The following SHALL apply for communicating the status of Certificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

OCSP responders operated by Starfield support the HTTP GET method, as described in RFC6960 and/or RFC5019. The CA MAY process the Nonce extension (`1.3.6.1.5.5.7.48.1.2`) in accordance with RFC 8954.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates and Subordinate CA Certificates:
- Starfield OCSP responses have a validity interval between 24 and 96 hours.
- Starfield updates the information provided via an OCSP at least eight hours prior to the nextUpdate.

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 or Certificate Problem Report procedures specified above when the revocation of a Subscriber certificate is due to private key compromise.

Parties may use the following methods to demonstrate private key compromise:

- Submission of the private key
- Submission of a CSR signed by the private key
- Submission of a revoke request following the procedures defined in Section 7.6 of RFC 8555 requiring signing the revocation request with the compromised key

If a key compromise is successfully proven, Starfield will revoke the certificate according to the specifications in Section 4.9 Certificate Revocation and Suspension.

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.

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 Section 4.9 Certificate Revocation and Suspension 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

Starfield SHALL develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to Starfield by law.

The Certificate Management Process MUST include:

1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

Starfield's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that Starfield has in place to counter such threats.

Based on the Risk Assessment, Starfield SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST also take into account then-available technology and the cost of implementing the specific measures, and SHALL implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical Security 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.

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.

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 Section 6.2.2 Private Key Multi-Person Control. 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 Section 5.3 Personnel Controls.

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.

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 qualifications and background check procedures comparable to those specified in Section 5.3.1 Qualifications, Experience, and Clearance Requirements and Section 5.3.2*5.3.2* Background Check Procedures, respectively.

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:

- CA certificate and key lifecycle management events including:
  - Key generation, backup, storage, recovery, archival, and destruction;
  - Certificate requests, renewal, and re-key requests, and revocation;
  - Approval and rejection of certificate requests;
  - Cryptographic device lifecycle management events;
  - Generation of Certificate Revocation Lists;
  - Signing of OCSP Responses; and
  - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
- CA and Subscriber certificate life cycle management events
  - Requests for certificates, renewal, re-key, and revocation
  - 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; and
  - 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;
  - Installation, update, and removal of software;
  - System crashes, hardware failures, and other anomalies;
  - Relevant router and firewall activities (as described in Section 5.4.1.1 Router and firewall activities logs)
  - 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 event
- Identity of the person making the journal record (when applicable)
- Description of the event

5.4.1.1 Router and firewall activities logs

Logging of router and firewall activities MUST at a minimum include:

- Successful and unsuccessful login attempts to routers and firewalls
- Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications
- Logging of all changes made to firewall rules, including additions, modifications, and deletions
- Logging of all system events and errors, including hardware failures, software crashes, and system restarts

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	2 years after the later of the following: • the destruction of the CA Private Key; or • the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
CA system logs of certificate management activity	2 years
Operating system logs	2 years
Physical access system logs	2 years
Manual logs of physical access	2 years
Logs of all certificates, revocations and documentation relating to verification of certificate requests	2 years after the expiration of the subscriber certificate
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.

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 Section 5.4.1 Types of Events Recorded.

5.5.2 Retention Period for Archive

Starfield retention period for archives it is made in accordance with Section 5.4.3 Retention period for audit log

5.5.3 Protection of Archive

See Section 5.4.4 Protection of Audit Log.

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 Section 6.3.2 Certificate Operational Periods and Key Pair Usage Periods. 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.

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 140-2 Level 3 or FIPS 140-3 Level 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 Level 3 or FIPS 140-3 Level 3 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.

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.

6.1.5.1 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

** 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.*

6.1.5.2 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

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

**** L and N (the bit lengths of modulus p and divisor q, respectively) are described in the Digital Signature Standard, FIPS 186-4.*

6.1.5.3 Subscriber Certificates

	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.*

**** L and N (the bit lengths of modulus p and divisor q, respectively) are described in the Digital Signature Standard, FIPS 186-4.*

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 186-4 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 Section 7.1 Certificate Profile.

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 140-2 Level 3 or FIPS 140-3 Level 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 Section 6.2.1 Cryptographic Module Standards and Controls.

Once a CA has reached the end of its maximum usage period as defined in Section 6.3.2 Certificate Operational Periods and Key Pair Usage Periods, 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 Section 6.3.2 Certificate Operational Periods and Key Pair Usage Periods, 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 Section 6.2.1 Cryptographic Module Standards and Controls. 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 Section 6.2.1 Cryptographic Module Standards and Controls.

6.2.8 Method of Activating Private Keys

Hardware modules used for CA private key protection utilize an activation mechanism as described in Section 6.2.2 Private Key Multi-Person Control.

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 Section 6.2.1 Cryptographic Module Standards and Controls.

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 Section 5.5 Records Archival.

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	398 days

Subscriber Certificates	Maximum Certificate Validity Period
Basic and Medium Assurance Domain Validated SSL Server Certificate	398 days
High Assurance Organizational Validated SSL Server Certificate Subscribers	398 days
Extended Validation SSL Server Certificate Subscribers	398 days

* 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 Section 6.2.2 Private Key Multi-Person Control.

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.

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

7.1.4.1 Name Encoding

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.

7.1.4.2 Subject Information - Subscriber Certificates

By issuing the Certificate, the Starfield represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. Starfield SHALL NOT include a Domain Name or IP Address in a Subject attribute except as specified in Section 3.2.2.4 Validation of Domain Authorization or Control ..

Subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName
Required/Optional: Required
Contents: This extension MUST contain at least one entry. Each entry MUST be one of the following types:

•dNSName: The entry MUST contain either a Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with Section 3.2.2.4 Validation of Domain Authorization or Control. Wildcard Domain Names MUST be validated for consistency with Section 3.2.2.6 Wildcard Domain Validation. The entry MUST NOT contain an Internal Name.

The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry MUST be composed entirely of LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System MUST NOT be included (e.g. "example.com" MUST be encoded as "example.com" and MUST NOT be encoded as "example.com.").

Effective 2021-10-01, the Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name MUST consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels.

•IPAddress: The entry MUST contain an IPv4 or IPv6 address that the CA has validated in accordance with Section 3.2.2.5 Authentication for an IP Address. The entry MUST NOT contain a Reserved IP Address.

7.1.4.2.2 Subject Distinguished Name Fields

a. **Certificate Field**: subject:commonName (OID **2.5.4.3**)
Required/Optional: Deprecated (Discouraged, but not prohibited)
Contents: If present, this field MUST contain exactly one entry that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2.1 Subject Alternative Name Extension). The value of the field MUST be encoded as follows:
•If the value is an IPv4 address, then the value MUST be encoded as an IPv4Address as specified in RFC 3986, Section 3.2.2.
•If the value is an IPv6 address, then the value MUST be encoded in the text representation specified in RFC 5952, Section 4.
•If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value MUST be encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.

b. **Certificate Field**: subject:organizationName (OID **2.5.4.10**)
Required/Optional: Optional.
Contents: If present, the subject:organizationName field MUST contain either the Subject's name or DBA as verified under Section 3.2.2.2 DBA/Tradename. Starfield may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that Starfield documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", Starfield MAY use "Company Name Inc." or "Company Name". Because Subject name attributes for individuals (e.g. givenName

(**2.5.4.42**) and surname (**2.5.4.4**)) are not broadly supported by application software, Starfield MAY use the subject:organizationName field to convey a natural person Subject's name or DBA.

c. **Certificate Field**: subject:givenName (**2.5.4.42**) and subject:surname (**2.5.4.4**)
Required/Optional: Optional.
Contents: If present, the subject:givenName field and subject:surname field MUST contain a natural person Subject's name as verified under Section 3.2.3 Authentication of Individual Identity. A Certificate containing a subject:givenName field or subject:surname field MUST contain the (**2.23.140.1.2.3**) Certificate Policy OID.

d. **Certificate Field**: Number and street: subject:streetAddress (OID: **2.5.4.9**)
Required/Optional:
Optional if the subject:organizationName field, subject:givenName field, or subject:surname field are present.
Prohibited if the subject:organizationName field, subject:givenName, and subject:surname field are absent.
Contents: If present, the subject:streetAddress field MUST contain the Subject's street address information as verified under Section 3.2.2.1 Identity.

e. **Certificate Field**: subject:localityName (OID: **2.5.4.7**)
Required/Optional:
Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent.
Optional if the subject:stateOrProvinceName field and the subject:organizationName field, subject:givenName field, or subject:surname field are present.
Prohibited if the subject:organizationName field, subject:givenName, and subject:surname field are absent.
Contents: If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 3.2.2.1 Identity. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2 (g) Subject Distinguished Name Fields: postalCode, the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 3.2.2.1 Identity.

f. **Certificate Field**: subject:stateOrProvinceName (OID: **2.5.4.8**)
Required/Optional:
Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and subject:localityName field is absent.
Optional if the subject:localityName field and the subject:organizationName field, the subject:givenName field, or the subject:surname field are present.
Prohibited if the subject:organizationName field, the subject:givenName field, or subject:surname field are absent.
Contents: If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under Section 3.2.2.1 Identity. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2 (g) Subject Distinguished Name Fields: postalCode,

the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under Section 3.2.2.1 Identity.

g. **Certificate Field**: subject:postalCode (OID: **2.5.4.17**)
Required/Optional:
Optional if the subject:organizationName, subject:givenName field, or subject:surname fields are present.
Prohibited if the subject:organizationName field, subject:givenName field, or subject:surname field are absent.
Contents: If present, the subject:postalCode field MUST contain the Subject's zip or postal information as verified under Section 3.2.2.1 Identity.

h. **Certificate Field**: subject:countryName (OID: **2.5.4.6**)
Required/Optional:
Required if the subject:organizationName field, subject:givenName, or subject:surname field are present.
Optional if the subject:organizationName field, subject:givenName field, and subject:surname field are absent.
Contents: If the subject:organizationName field is present, the subject:countryName MUST contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1 Identity. If the subject:organizationName field is absent, the subject:countryName field MAY contain the two-letter ISO 3166-1 country code associated with the Subject as verified in accordance with Section 3.2.2.3 Verification of Country. If a Country is not represented by an official ISO 3166-1 country code, Starfield MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

i. **Certificate Field**: subject:organizationalUnitName (OID: **2.5.4.11**)
Required/Optional: Deprecated.
Prohibited if the subject:organizationName is absent or the certificate is issued on or after September 1, 2022.
Contents: Starfield SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless Starfield has verified this information in accordance with Section 3.2 Initial Identity Validation and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1 Identity.

Note: As of July 16, 2021, Starfield no longer includes the OU field on Subscriber Certificates.

j. Other Subject Attributes
Other attributes MAY be present within the subject field. If present, other attributes MUST contain information that has been verified by Starfield.

7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates

By issuing a Subordinate CA Certificate, Starfield represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1 Subject Distinguished Name Fields

a. **Certificate Field**: subject:commonName (OID **2.5.4.3**)
Required/Optional: Required
Contents: This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.

b. **Certificate Field**: subject:organizationName (OID **2.5.4.10**)
Required/Optional: **Required**
Contents: This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2 DBA/Tradename. Starfield may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that Starfield documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", Starfield MAY use "Company Name Inc." or "Company Name".

c. **Certificate Field**: subject:countryName (OID: **2.5.4.6**)
Required/Optional: **Required**
Contents: This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.

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 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

1. **reasonCode** (OID **2.5.29.21**)

   If present, this extension MUST NOT be marked critical.

   If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, this CRL entry extension MUST be present. If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements.

   The CRLReason indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, CAs MUST omit reasonCode entry extension, if allowed by the previous requirements. If a CRL entry is for a Certificate not subject to these Requirements and was either issued on-or-after 2020-09-30 or has a notBefore on-or-after 2020-09-30, the CRLReason MUST NOT be certificateHold (6). If a CRL entry is for a Certificate subject to these Requirements, the CRLReason MUST NOT be certificateHold (6).

   If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the certificate.

2. **issuingDistributionPoint** (OID **2.5.29.28**)

Effective 2023-01-15, if a CRL does not contain entries for all revoked unexpired certificates issued by the CRL issuer, then it MUST contain a critical Issuing Distribution Point extension and MUST populate the **distributionPoint** field of that extension.

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 or less 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
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 **bold** reason codes: unspecified (0) **keyCompromise (1)** cACompromise (2) **affiliationChanged (3)** **superseded (4)** **cessationOfOperation (5)** removeFromCRL (8) **privilegeWithdrawn (9)** aACompromise (10)
Invalidity Date	A GeneralizedTime denoting the effective time when the given serial number is to be considered invalid.

7.2.2.2 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	10 or less 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 **bold** reason codes: unspecified (0) **keyCompromise (1)** cACompromise (2) **affiliationChanged (3)** **superseded (4)** **cessationOfOperation (5)** 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

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the **revocationReason** field within the **RevokedInfo** of the **CertStatus** MUST be present. The **CRLReason** indicated MUST contain a value permitted for CRLs, as specified in Section 7.2.2 CRL and CRL Entry Extensions.

7.3.1 Version Number

Starfield OCSP responses conform to version 1 of RFC 6960.

7.3.2 OCSP Extensions

The **singleExtensions** of an OCSP response MUST NOT contain the **reasonCode** (OID **2.5.29.21**) CRL entry extension.

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). Starfield ensures that audit results are communicated in a manner that is compliant with [BR 8.6].

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 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 Section 2 Publication and Repository Responsibilities Starfield may change this document at any time without prior notice.

8.9 CPS Approval Procedures

See Section 8.8.1 Specification Change Procedures.

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 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.

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.

9.1.5 Refund Policy

Subscribers may request a refund directly through the entity the certificate was purchased from, and will be subject to the entity's refund policies.

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.

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 Section 9.4.1 Privacy Plan.

9.4.3 Information Not Deemed Private

See Section 9.4.1 Privacy Plan.

9.4.4 Responsibility to Protect Private Information

See Section 9.4.1 Privacy Plan.

9.4.5 Notice and Consent to Use Private Information

See Section 9.4.1 Privacy Plan.

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 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 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 document 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 Section 1.3 PKI Participants. 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 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
- **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.

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 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.

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, 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 Starfield

Starfield shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by Starfield, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by Starfield where such claim, damage, or loss was directly caused by such Application Software Supplier’s software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from Starfield online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 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.

9.9.3 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:

- 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.

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 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.

9.16.4 Enforcement

No Stipulation.

9.16.5 Force Majeure

Starfield shall not be responsible for any breach of warranty, delay, or failure in performance under this CP/CPS that results from events beyond its control including, but not limited to, acts of God, acts of war, epidemics, riots, power outages, fire, earthquakes, floods and other disasters.

9.17 Other Provisions

Not applicable.

10 APPENDIX A – CERTIFICATE PROFILES

10.1 Root CAs

10.1.1 Starfield Class 2 Certification Authority

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

10.1.2 Starfield Root Certificate Authority – G2

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
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

10.1.3 Go Daddy Class 2 Certification Authority

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
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

10.1.4 Go Daddy Root Certificate Authority – G2

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

10.1.5 Starfield Services Root Certification Authority

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

10.1.6 GoDaddy Root Certificate Authority - G5.

The following certificate profile is used for the GoDaddy Root Certificate Authority - G5.

Field	Description
Version	V3
Serial Number	13:7f:6d:56:eb:b7:14:c0:cf:c6:2d:bd:61:85:a0:42
Signature Algorithm Identifier	sha256WithRSAEncryption
Issuer	CN=Go Daddy Root Certificate Authority – G5 O=GoDaddy.com, Inc. C=US
Valid From	June 21, 2022 00:00:00 GMT
Valid To	June 21, 2042 00:00:00 GMT
Subject	CN=Go Daddy Root Certificate Authority – G5 O=GoDaddy.com, Inc. C=US
Subject Public Key Information	RSA (4096 bits)
Extensions:	
Key Usage (critical)	keyCertSign, cRLSign
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None

Field	Description
Subject Key Identifier	CF:CF:BB:19:B2:9F:F8:CB:F5:C2:9E:63:84:B1:7B:E6:17:07:31:58

10.1.7 Starfield Root Certificate Authority - G5

The following certificate profile is used for the Starfield Root Certificate Authority - G5.

Field	Description
Version	V3
Serial Number	f0:f8:38:64:b9:0f:43:32:d1:bf:cb:19:1c:ae:8a:32
Signature Algorithm Identifier	sha256WithRSAEncryption
Issuer	CN= Starfield Root Certificate Authority – G5 O= Starfield Technologies, Inc. C=US
Valid From	June 21, 2022 00:00:00 GMT
Valid To	June 21, 2042 00:00:00 GMT
Subject	CN= Starfield Root Certificate Authority – G5 O= Starfield Technologies, Inc. C=US
Subject Public Key Information	RSA (4096 bit)
Extensions:	
Key Usage (critical)	keyCertSign, CRLSign
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Subject Key Identifier	E3:11:A7:2D:79:1E:3D:11:54:C3:69:2D:6B:07:A9:F8:05:03:D9:30

10.1.8 GoDaddy Root Certificate Authority – G6

The following certificate profile is used for the GoDaddy Root Certificate Authority – G6.

Field	Description
Version	V3
Serial Number	18:3c:e3:59:e1:7c:f2:86:8c:65:a7:0a:46:e0:5c:c3
Signature Algorithm Identifier	ecdsa-with-SHA384
Issuer	CN=Go Daddy Root Certificate Authority – G6 O=GoDaddy.com, Inc. C=US
Valid From	June 21, 2022 00:00:00 GMT
Valid To	June 21, 2052 00:00:00 GMT
Subject	CN=Go Daddy Root Certificate Authority – G6 O=GoDaddy.com, Inc. C=US
Subject Public Key Information	ECC, NIST P-384
Extensions:	
Key Usage (critical)	keyCertSign, cRLSign

Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Subject Key Identifier	59:C1:AE:05:B3:82:9E:CB:31:C3:F5:9B:E3:18:BC:DD:C6:23:A9:BF

10.1.9 Starfield Root Certificate Authority - G6

The following certificate profile is used for the Starfield Root Certificate Authority - G6.

Field	**Description**
Version	V3
Serial Number	54:27:7b:51:ae:50:1f:7e:a4:51:82:3e:36:06:db:7c
Signature Algorithm Identifier	ecdsa-with-SHA384
Issuer	CN= Starfield Root Certificate Authority - G6 O= Starfield Technologies, Inc. C=US
Valid From	June 21, 2022 00:00:00 GMT
Valid To	June 21, 2052 00:00:00 GMT
Subject	CN= Starfield Root Certificate Authority - G6 O= Starfield Technologies, Inc. C=US
Subject Public Key Information	ECC, NIST P-384
Extensions:	
Key Usage (critical)	keyCertSign, CRLSign
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
Subject Key Identifier	1B:C1:8D:B1:2B:19:78:D7:FF:21:82:0C:DE:60:B8:54:0D:7A:93:CC

10.2 Issuing CAs

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

10.2.1 Starfield Issuing (subordinate) CAs

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
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
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.

10.3.1 Go Daddy Root Certificate Authority - G2 + Go Daddy Class 2 Certification Authority

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
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: 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/.

10.3.2 Starfield Root Certificate Authority - G2 + Starfield Class 2 Certification Authority

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/

Note: 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/.

10.3.3 Starfield Services Root Certificate Authority + Starfield Services Root Certificate Authority

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
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: 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/.

10.3.4 Starfield Services Root Certificate Authority - G2 + Starfield Class 2 Certification Authority

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
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: 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.

10.3.5 Certainly E1 + Starfield Services Root Certificate Authority - G2

The following certificate profile is used for the certificate which cross certifies the Certainly E1 with the Starfield Services Root Certificate Authority - G2.

Field	Description
Version	V3
Serial Number	00a207da718baba362
Signature Algorithm Identifier	sha256WithRSAEncryption
Issuer	CN = Starfield Root Certificate Authority - G2 O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Valid From	June 22, 2022 00:00:00 GMT
Valid To	June 21, 2032 23:59:59 GMT
Subject	CN = Certainly Intermediate E1 O = Certainly C = US
Subject Public Key Information	ECC, NIST P-384
Extensions:	
Basic Constraints (critical)	Subject Type=CA
Key Usage (critical)	Digital Signature, Certificate Sign, CRL Sign
Subject Key Identifier	0A:98:98:AE:4F:3A:D7:DD:67:86:E7:97:25:5A:9B:23:4F:5B:58:1D
Authority Key Identifier	keyid:7C:0C:32:1F:A7:D9:30:7F:C4:7D:68:A3:62:A8:A1:CE:AB:07:5B:27
Authority Information Access	[1]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/sfroot-g2.crt.cer
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.starfieldtech.com/sfroot-g2.crl
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.49945.1.1 Qualifier: https://certs.starfieldtech.com/repository/

10.3.6 Certainly R1 + Starfield Services Root Certificate Authority - G2

The following certificate profile is used for the certificate which cross certifies the Certainly R1 with the Starfield Services Root Certificate Authority - G2.

Field	Description
Version	V3
Serial Number	11831cde4cb573e5
Signature Algorithm Identifier	sha256WithRSAEncryption
Issuer	CN = Starfield Root Certificate Authority - G2 O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Valid From	June 22, 2022 00:00:00 GMT
Valid To	June 21, 2032 23:59:59 GMT
Subject	CN = Certainly Intermediate R1 O = Certainly C = US
Subject Public Key Information	RSA (2048 bit)
Extensions:	
Basic Constraints (critical)	Subject Type=CA
Key Usage (critical)	Digital Signature, Certificate Sign, CRL Sign
Subject Key Identifier	BD:97:9D:df:A1:D8:1B:25:99:E3:0C:04:06:89:64:12:D7:65:24:C7
Authority Key Identifier	keyid:7C:0C:32:1F:A7:D9:30:7F:C4:7D:68:A3:62:A8:a1:CE:ab:07:5B:27
Authority Information Access	[1]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/sfroot-g2.crt.cer
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.starfieldtech.com/sfroot-g2.crl
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.49945.1.1 Qualifier: https://certs.starfieldtech.com/repository/

10.4 End Entity SSL Certificates

10.4.1 Go Daddy Issuing CA: Subscriber 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	sha256RSA (OID: 1.2.840.113549.1.1.11)
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 (on certificates issued prior to July 15, 2021).
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/
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

10.4.2 Starfield Issuing CA: Subscriber Certificates

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	sha256RSA (OID: 1.2.840.113549.1.1.11)
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 (on certificates issued prior to July 15, 2021).
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=2.16.840.1.114414.1.7.23.1 [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
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

10.4.3 Go Daddy Issuing CA – G2: Subscriber Certificates

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 (on certificates issued prior to July 15, 2021).
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
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

10.4.4 Starfield Issuing CA – G2: Subscriber Certificates

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 (on certificates issued prior to July 15, 2021).
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=2.16.840.1.114414.1.7.23.1 [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
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
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

10.5.1 Go Daddy Issuing CA: Subscriber Certificates

As of May 30, 2021, Starfield no longer issues High Assurance Code Signing Certificates, however the following certificate profile was used for Go Daddy branded Subscriber Certificates issued from the Go Daddy Issuing CA. At a minimum, the following fields were 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	sha256RSA (OID: 1.2.840.113549.1.1.11)
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.
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

10.5.2 Starfield Issuing CA: Subscriber Certificates

As of May 30, 2021, Starfield no longer issues High Assurance Code Signing Certificates, however the following certificate profile was used for Starfield branded Subscriber Certificates issued from the Starfield Issuing CA. At a minimum, the following fields were 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	sha256RSA (OID: 1.2.840.113549.1.1.11)
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)
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

Field	Description
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate

10.5.3 Go Daddy Secure Certificate Authority – G2 AND Go Daddy Secure Extended Validation Code Signing CA – G2: Subscriber Certificates

As of May 30, 2021, Starfield no longer issues High Assurance Code Signing Certificates, however the following certificate profile was 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 were 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	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	Subject of corresponding Issuing CA certificate
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 (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
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

10.5.4 Starfield Secure Certificate Authority – G2 AND Starfield Secure Extended Validation Code Signing CA – G2: Subscriber Certificates

As of May 30, 2021, Starfield no longer issues High Assurance Code Signing Certificates, however the following certificate profile was 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 were 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	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	Subject of corresponding Issuing CA certificate
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 (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
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

11 APPENDIX B: TEST SITES

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
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 Services			https://expired.sfs.catest.starfieldtech.com