Starfield Technologies, LLC

Certificate Policy
and
Certification Practice Statement
(CP/CPS)

Version 3.10
March 1, 2017

Table of Contents

1 Introduction

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

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

1.1 Overview

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

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

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

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

1.2 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.

1.3 Community and Applicability

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).

Within the Starfield PKI, there are two general types of CAs: Root and Issuing CAs. Currently, the Starfield PKI hierarchy consists of the following CAs:

CA Type	CA Name	Description of Function
Root CA	ValiCert Class 2 Policy Validation Authority (also referred to as the "Starfield Root CA")[1]	Serves as the legacy "trust anchor" for the Starfield PKI hierarchy.
Issuing CA	Starfield Secure Certification Authority (1024-bit)	Issued SSL web server certificates to authenticated organizations and individuals. No longer issuing certificates.
Root CA	Starfield Class 2 Certification Authority	Serves as the "trust anchor" for the Starfield PKI hierarchy for any certificates other than those sold under the Go Daddy brand.
Issuing CA	Starfield Secure Certification Authority (2048-bit)	Issues certificates to authenticated organizations and individuals.
Root CA	Starfield Root Certificate Authority – G2	Second Generation (G2) Starfield Root CA. Serves as the default "trust anchor" for the Starfield PKI hierarchy for any certificates other than those sold under the Go Daddy brand. Issues any new CAs for different types of PKI services except those used with the Go Daddy brand. Serves as a trusted root for time stamping certificates.
Issuing CA	Starfield Secure Certificate Authority - G2	Issues certificates to authenticated organizations and individuals.
Issuing CA	Starfield Secure Code Signing Certificate Authority - G2	Reserved for future use.
Issuing CA	Starfield Secure Extended Validation Code Signing CA – G2	Issues Extended Validation Code Signing certificates to authenticated entities.

[1] Starfield acquired the ValiCert Class 2 Policy Validation Authority from ValiCert, Inc. in June 2003.

Root CA	Starfield Root Certificate Authority – G3	Reserved for future use (4096-bit).
Issuing CA	Starfield Secure Certificate Authority – G3	Reserved for future use (4096-bit).
Issuing CA	Starfield Secure Code Signing Certificate Authority – G3	Reserved for future use (4096-bit).
Issuing CA	Starfield Secure Extended Validation Code Signing CA – G3	Reserved for future use (4096-bit).
Root CA	Starfield Root Certificate Authority – G4	Reserved for future use (ECDSA).
Issuing CA	Starfield Secure Certificate Authority – G4	Reserved for future use (ECDSA).
Issuing CA	Starfield Secure Code Signing Certificate Authority – G4	Reserved for future use (ECDSA).
Issuing CA	Starfield Secure Extended Validation Code Signing CA – G4	Reserved for future use (ECDSA).
Root CA	Go Daddy Class 2 Certification Authority	Serves as the "trust anchor" for the Starfield PKI hierarchy for any certificates sold under the Go Daddy brand.
Issuing CA	Go Daddy Secure Certification Authority	Issues GoDaddy branded certificates to authenticated organizations and individuals.
Root CA	Go Daddy Root Certificate Authority – G2	Second Generation (G2) Go Daddy Root CA. Serves as the default "trust anchor" for the Starfield PKI hierarchy for any certificates sold under the Go Daddy brand. Issues any new CAs for different types of PKI services sold under the Go Daddy brand.
Issuing CA	Go Daddy Secure Certificate Authority - G2	Issues GoDaddy branded certificates to authenticated organizations and individuals.

Issuing CA	Go Daddy Secure Code Signing Certificate Authority - G2	Reserved for future use.
Issuing CA	Go Daddy Secure Extended Validation Code Signing CA – G2	Issues GoDaddy branded Extended Validation Code Signing certificates to authenticated entities.
Root CA	Go Daddy Root Certificate Authority – G3	Reserved for future use (4096-bit).
Issuing CA	Go Daddy Secure Certificate Authority – G3	Reserved for future use (4096-bit).
Issuing CA	Go Daddy Secure Code Signing Certificate Authority – G3	Reserved for future use (4096-bit).
Issuing CA	Go Daddy Secure Extended Validation Code Signing CA – G3	Reserved for future use (4096-bit).
Root CA	Go Daddy Root Certificate Authority – G4	Reserved for future use (ECDSA).
Issuing CA	Go Daddy Secure Certificate Authority – G4	Reserved for future use (ECDSA).
Issuing CA	Go Daddy Secure Code Signing Certificate Authority – G4	Reserved for future use (ECDSA).
Issuing CA	Go Daddy Secure Extended Validation Code Signing CA – G4	Reserved for future use (ECDSA).
Root CA	Starfield Services Root Certificate Authority	Serves as a trusted root for time stamping certificates. Also reserved for general purpose usage in the future.
Root CA	Starfield Services Root Certificate Authority – G2	As of June 10, 2015 this root is operated by Amazon Web Services, Inc.; however, it remains cross-certified by both the Starfield Services Root Certificate Authority and the Starfield Class 2 Certification Authority

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.

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 End Entities

End Entities include Subscribers and Relying Parties.

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

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.

1.3.4 Applicability

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.

1.4 Contact Details

1.4.1 Organization Administering the Document

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

1.4.2 Contact Person

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

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

1.5 Policy Administration

See §1.4

2 General Provisions

2.1 Obligations

2.1.1 Starfield Governance and Policy Committee Obligations

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.

2.1.2 Certification Authority Obligations

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.

2.1.3 Repository Obligations

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.

2.1.4 Registration Authority Obligations

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.

2.1.5 Subscriber Obligations

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.

2.1.6 Relying Party Obligations

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.

2.2 Liability

2.2.1 Warranties and Limitations on Warranties

The warranties, disclaimers of warranty, and limitations of liability among Starfield, its Resellers, and their respective Customers within the Starfield PKI are set forth and governed by the agreements among them. This CPS 2.2.1 relates only to the warranties that certain CAs (Starfield CAs) must make to end-Subscribers receiving Certificates from them and to Relying Parties, the disclaimers of warranties they shall make to those Subscribers and Relying Parties, and the limitations of liability they can place on those Subscribers and Relying Parties.

Starfield uses, and (where required) Resellers shall use, Subscriber agreements and Relying party agreements in accordance with CPS 2. 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.

2.2.1.1 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.

2.2.1.2 Loss Limitations

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) ZERO UNITED STATES DOLLARS ($0.00) FOR EACH BASIC ASSURANCE CERTIFICATE ("BASIC ASSURANCE CUMULATIVE DAMAGE LIMIT"); (B) ONE HUNDRED THOUSAND UNITED STATES DOLLARS ($100,000.00) FOR EACH MEDIUM ASSURANCE CERTIFICATE ("MEDIUM ASSURANCE CUMULATIVE DAMAGE LIMIT"); (C) TWO HUNDRED FIFTY THOUSAND UNITED STATES DOLLARS ($250,000.00) FOR EACH HIGH ASSURANCE CERTIFICATE ("HIGH ASSURANCE CUMULATIVE DAMAGE LIMIT"); OR (D) ONE MILLION UNITED STATES DOLLARS ($1,000,000.00) 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.

In addition, Starfield is not liable for any loss:

- of CA or RA services due to war, natural disasters or other uncontrollable forces;
- incurred between the time a certificate is revoked and the next scheduled issuance of a CRL;
- due to unauthorized use of certificates issued by the Starfield PKI, or use of certificates beyond the prescribed use defined by this CP/CPS;
- arising from the negligent or fraudulent use of certificates or CRLs issued by the Starfield PKI; or
- due to disclosure of personal information contained within certificates.

2.2.1.3 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.

2.2.1.4 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.

2.2.2 Disclaimer 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 EXCEPT THE LIMITED WARRANTY IN SECTION 2.2.1.1, 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.

2.2.3 Subscriber Liability

2.2.3.1 Subscriber 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.

2.2.3.2 Private Key Compromise

The Subscriber Agreements provide that if Subscribers fail to meet the PKI requirements and their private key is compromised, they are solely responsible for any loss or damage resulting from such failure.

2.2.4 Other Exclusions

No stipulation.

2.3 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.

2.3.1 Indemnification by Subscribers and Relying Parties

2.3.1.1 Indemnification by Subscribers

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

- Any false statement, omission or misrepresentation of fact that the Subscriber has put on the Subscriber's Certificate Application,

- Any modification made by the Subscriber to the information contained in a Starfield Certificate,

- The use of a Starfield Certificate other than as permitted by the Starfield CPS, the Subscription agreement, any Relying Party agreement, and applicable law,

- The Subscriber's failure to use a secure system, protect the Subscriber's private key, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or

- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

2.3.1.2 Indemnification by Relying Parties

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

- 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.

2.3.2 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.

2.3.3 Administrative Processes

No stipulation.

2.4 Interpretation and Enforcement

2.4.1 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 2.4.1 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.

2.4.2 Severability, Survival, Merger and Notice

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.

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.

2.4.3 Dispute Resolution Procedures

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.

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

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

2.5.2 Certificate Access Fees

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

2.5.3 Status Information Access or Revocation Fees

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

2.5.4 Fees for Other Services Such as Policy Information

Starfield does not charge a fee for accessing this CPS or the CP. However, any use of the CPS for purposes other than viewing the document, including reproduction, redistribution, modification, or creation of derivative works, may be subject to a license agreement with the entity holding the copyright to the document.

2.5.5 Refund Policy

The following refund policy is in effect:

Starfield employs strict practices and policies in its certification operations and in issuing certificates. If for any reason a Subscriber is not completely satisfied with the certificate that has been issued to the Subscriber, the Subscriber may ask Starfield to revoke the certificate within 45 days of issuance for a refund, minus any fees. Following the initial 45 day period, a Subscriber may ask Starfield to revoke the certificate and provide a refund if Starfield has breached a warranty or other material obligation under this CPS relating to the Subscriber or the subscriber's certificate. After Starfield revokes the subscriber's certificate, Starfield will promptly credit the Subscriber's credit card account (if the certificate was paid for via credit card) or otherwise reimburse the Subscriber via check, for the full amount minus fees, of the amount paid for the certificate. To request a refund, please call customer service at +1 (480) 505-8855. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

2.6 Publication and Repository

2.6.1 Publication of CA Information

This CP/CPS is published in the Starfield repository at http://www.starfieldtech.com/repository/ in accordance with the provisions of §8 of this CPS.

2.6.2 Frequency of Publication

This CP/CPS is published in accordance with §2.6.1. CRLs are published in accordance with §4.4.9.

2.6.3 Access Controls

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.

2.6.4 Repositories

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.

Starfield also maintains a database of issued certificates and CRLs to which access is restricted to authorized Starfield PKI personnel.

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

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit

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.

2.7.2 Identity/Qualifications of Auditor

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.

2.7.3 Auditor's Relationship to Audited Party

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

2.7.4 Topics Covered by Audit

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.

2.7.5 Actions Taken as a Result of an Audit 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.

2.7.6 Communication of Results

Compliance audit results are communicated to Starfield Management and others deemed appropriate by Starfield Management.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

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

2.8.2 Types of Information not Considered Confidential

This CP/CPS and Certificates and CRLs issued by Starfield are not considered confidential.

2.8.3 Disclosure of Certificate Revocation Information

Subscriber certificate status information is made available to Relying Parties through the use of CRLs and OCSP. The transactional records and other information leading up to a certificate revocation are considered confidential information.

2.8.4 Release to Law Enforcement Officials

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.

2.8.5 Release as Part of Civil Discovery

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.

2.8.6 Disclosure Upon Owner's Request

No stipulation.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights

Intellectual Property Rights among Starfield PKI Participants other than Subscribers and Relying Parties are governed by the applicable agreements among such Starfield PKI Participants. The following subsections of CPS 2.9 apply to Intellectual Property Rights in relation to Subscribers and Relying Parties.

2.9.1. 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.

2.9.2 Property Rights in the Agreement

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

2.9.3 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.

2.9.4 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

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

All certificate holders require either a Distinguished Name in the Subject field that is in compliance with the X.500 standard for Distinguished Names, or a set of Subject Alternative Name values in the Subject Alternative Name extension. In the case where subject identity information is contained solely in the Subject Alternative Name extension, the Subject field of

the certificate shall be empty. The Starfield PKI approves naming conventions for the creation of distinguished names and Subject Alternative Name values for certificate applicants.

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

3.1.2 Need for Names to be Meaningful

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

3.1.3 Rules for Interpreting Various Name Forms

Name forms are interpreted in accordance with §3.1.1 and 3.1.2.

3.1.4 Uniqueness of Names

No stipulation.

3.1.5 Name Claim Dispute Resolution Procedure

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.

3.1.6 Recognition, Authentication and Role of Trademarks

See §3.1.5.

3.1.7 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.

3.1.8 Domain Name Access Verification

Domain names included in the Subject Common Name or Subject Alternative Name fields of an End Entity Certificate may be fully qualified or wildcard. Certificates issued prior to November 1, 2015 may also contain internal names or IP addresses.

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 is performed when a Subscriber requests the renewal of a certificate in accordance with §3.10.

For Subscriber Certificates issued prior to August 8, 2011 at 0700 UTC:
Once a certificate has been issued, no further verification of the domain name(s) within the certificate is performed during the validity period of the issued certificate.

For Subscriber Certificates issued on or after August 8, 2011 at 0700 UTC:
Once a certificate has been issued, re-verification of domain name access is conducted in accordance with §3.10.

3.1.9 Basic and Medium Assurance Authentication

For Basic and Medium Assurance Subscribers, Starfield verifies the following:

- the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application using the methods described in section 3.2.

3.1.10 High Assurance Authentication for Individual Subscribers

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.
- the identity of the individual named in the certificate application using the methods described in section 3.3.5.

3.1.11 High Assurance Authentication for Organizational Subscribers

For High Assurance Organizational 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.
- the individual requesting the certificate is authorized to do so by the organization named in the certificate using the methods described in section 3.3.4.
- the organization name represents an organization validated using the methods described in sections 3.3.2 and 3.3.3.

3.1.12 High Assurance Authentication for Code Signing Subscribers

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

- the individual requesting the certificate is authorized to do so by the organization named in the certificate using the methods described in section 3.3.4.
- the organization name represents an organization currently validated using the methods described in sections 3.3.2 and 3.3.3.

3.1.13 Unified Communications Certificate Authentication

The individual requesting the certificate is confirmed to have access to every domain name included in the Subject Common Name or Subject Alternative Name fields of a UCC certificate.

Only one Individual (as described in §3.1.10) or one Organization (as described in §3.1.11) is authenticated for each High Assurance UCC certificate.

3.1.14 Extended Validation Authentication

For Extended Validation Subscribers, Starfield verifies the following in accordance with the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates:

- Legal Existence and Identity
- Assumed Name (optional)
- Physical Existence
- Operational Existence (if records indicate that the organization is less than three years old)
- Domain ownership or exclusive right to use
- Name, title, and authority of contract signer, and certificate approver

3.1.15 Custom Certificate Authentication

Starfield may issue certificates designed for use in a specific peer-to-peer application. These certificates are designed for use only in that application and steps are taken to ensure that they will not function for standard uses such as SSL or code signing. For certificates issued for a specialized usage, Starfield verifies the following:

- information contained in the certificate that identifies a person or organization has been validated
- the requestor possesses a valid license key for the product on which the certificate will be used

3.2 Authorization by Domain Name Registrant

In compliance with the CA / Browser Forum Baseline Requirements, 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:

1. 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.
2. 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. 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.
4. 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.

5. Relying upon a Domain Authorization Document provided by the Domain Name Registrar or private registration service provider.
6. 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.
7. Having the Applicant demonstrate practical control over the FQDN by confirming the presence of a Random Value generated by Starfield in a DNS TXT or CAA record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

3.3 Verification of Subject Identity Information

In compliance with the CA / Browser Forum Baseline Requirements, Starfield verifies Subject identity information using the following processes:

3.3.1 Authorization by Domain Name Registrant

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 methods described in section 3.2.

3.3.2 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.

3.3.3 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 CA determines to be reliable.

3.3.4 Authenticity of Certificate Request

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.
Starfield use the sources listed in section 3.3.1 to verify the Reliable Method of Communication.
Using a Reliable Method of Communication, Starfield establishes the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.
In addition, Starfield has a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then Starfield does not accept any certificate requests that are outside this specification. Starfield will provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.3.5 Verification of Individual Applicant

If an Applicant is a natural person, then Starfield will verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.
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 will inspect the copy for any indication of alteration or falsification.
Starfield verifies the Applicant's address using a form of identification that Starfield determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. Starfield may rely on the same government issued ID that was used to verify the Applicant's name.
Starfield also verifies the certificate request with the Applicant using a Reliable Method of Communication.

3.3.6 Verification of Country

If the subject:countryName field is present, then Starfield verifies the country associated with the Subject using a method identified in Section 3.3.2.

3.3.7 Age of Certificate Data

Starfield will not use documents and data to verify certificate information if Starfield obtained the data or document more than thirty-nine (39) months prior to issuing the Certificate.

3.3.8 Denied List

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.

3.3.9 High Risk Requests

Starfield maintains a database used to identify high risk Certificate requests prior to the Certificate's approval and subjects these requests to additional verification procedures.

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

3.3.10 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.

3.4 Routine Re-key

Routine re-key of CAs is performed in accordance with §4.8.

Subscribers are permitted to submit an unlimited number of requests to re-key any valid Certificate during the validity period of the Certificate.

Prior to September 3, 2013, Starfield performed no additional verification on Subscriber re-key requests and did not modify the expiration timestamp of the certificate.

After September 3, 2013, Starfield re-keys Basic, Medium, and High Assurance Subscriber certificates in accordance with sections 3.6 and 6.3.2. Re-keys of Extended Validation Subscriber certificates require no additional verification in accordance with section 11.13.4 of the Guidelines for the Issuance and Management of Extended Validation Certificates.

3.5 Re-key After Revocation

In the event that a Starfield CA certificate must be revoked, the CA will be re-keyed in accordance with §4.8 or terminated in accordance with §4.10.

The process for re-key after revocation of a Subscriber certificate is complete re-enrollment, which requires the generation of a new Subscriber key pair and the re-performance of the initial Subscriber identification and authentication procedures specified in §3.1.8 -- 3.1.15.

3.6 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.

Subscribers are permitted to reuse a previous certificate request to replace an expiring or expired Certificate. Where the Subscriber holds a Certificate and the initial Subscriber identification and authentication process (as described in §3.1.8 -- 3.1.15) has been performed within the previous 39 months, Starfield may authenticate a renewal certificate request using a shared secret.

3.7 Revocation Request

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

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

3.8 Suspension Request

See §4.4.

3.9 Request to Release Suspension

See §4.4.

3.10 Re-Verification of Subscriber Information

This §3.10 only applies to Subscriber Certificates issued on or after August 8, 2011 at 0700 UTC.

For Subscriber Certificates with a validity period of thirty-nine (39) months or less, no re-verification of any Subscriber information is performed during the validity period of the Certificate.

For Subscriber Certificates with a validity period of more than thirty-nine (39) months, all Subscriber information that is required for the issuance of the Certificate will be re-verified at least every thirty-nine (39) months during the validity period of the Certificate.

If any required Subscriber information has not been verified within the past thirty-nine (39) months, the (end-entity, non-CA) Certificate(s) relying on that information will be revoked.

4 Operational Requirements

4.1 Certificate Application

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

4.1.1 CAA Record Processing

At the time of publication of this version of the CP-CPS, Starfield does not process RFC 6844 Certificate Authority Authorization records. Starfield reserves the right to begin processing these records at any time in the future.

4.2 Certificate Issuance

Certificates are generated, issued and published only after the RA performs the required identification and authentication steps in accordance with §3.1.8 -- 3.1.15.

4.3 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 Certificate Suspension and Revocation

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

4.4.1 Circumstances for Revocation

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

- The Subscriber or authorized Reseller on behalf of the Subscriber requests certificate revocation in accordance with §3.7.
- The certificate subject can be shown to have violated the stipulations of this CP/CPS, or compromise the security or integrity of the Starfield PKI.
- The Subscriber can be shown to have violated the stipulations of the Subscriber Agreement.
- Compromise of the Subscriber's private key is known or suspected.
- The authenticated organization or individual name in the Subject field of the Subscriber's certificate changes before the certificate expires.
- The Subscriber fails to pay any invoice from Starfield within forty-five (45) days of receiving it.

4.4.2 Who Can Request Revocation

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

4.4.3 Procedure for Revocation Request

Subscriber certificate revocation requests are authenticated using a shared secret or in accordance with Starfield's revocation request processing procedures.

4.4.4 Revocation Request Grace Period

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

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

4.4.5 Circumstances for Suspension

Not applicable.

4.4.6 Who Can Request Suspension

Not applicable.

4.4.7 Procedure for Suspension Request

Not applicable.

4.4.8 Limits on Suspension Period

Not applicable.

4.4.9 CRL Issuance Frequency

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

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

4.4.10 CRL Checking Requirements

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

4.4.11 Online Revocation/Status Checking Availability

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

CA Type	OCSP Update Frequency
Root CAs	Every 365 days or less and upon certificate revocation if OCSP is enabled for the Root CA
Issuing CAs	Every 4 days or less

4.4.12 Online Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements for Key Compromise

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

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

4.5 Certificate Problem Reporting and Response

4.5.1 Reporting

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

4.5.2 Investigation

Starfield will begin investigation of all certificate problem reports within twenty-four (24) hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:
(i) The nature of the alleged problem;
(ii) Number of Certificate Problem Reports received about a particular EV Certificate or website;
(iii) The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
(iv) Relevant legislation in force.

4.5.3 Response

Starfield maintains a continuous 24/7 ability to respond to any high priority certificate problem reports and to revoke certificates in accordance with §4.4 and/or report the problem to law enforcement officials.

4.6 Security Audit Procedures

4.6.1 Types of Events Recorded

The Starfield PKI logs the following events:

- Significant CA key life cycle management events including CA key generation backup, storage, archival, and destruction and other cryptographic device lifecycle management events
- CA and Subscriber certificate life cycle management events
  - Requests for certificates, renewal, re-key, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of certificates
  - Revocation of certificates
  - Issuance of CRLs and generation of OCSP entries
  - All verification activities required by applicable guidelines
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls
- Security-sensitive operating system events
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from CA facility
- CA facility entry/exit.
- Separation of validation duties between multiple RAs for Extended Validation certificates

4.6.2 Required Data Elements

All audit logs include, at a minimum:

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

4.6.3 Frequency of Processing Log

Audit logs are reviewed on an as-needed basis.

4.6.4 Retention Period for Audit Log

Audit logs are retained as follows:

Log Type	Retention Period
Logs of CA key management activity	30 years
CA system logs of certificate management activity	30 years
Operating system logs	7 years
Physical access system logs	7 years
Manual logs of physical access	7 years
Video recording of CA facility access	90 days

4.6.5 Protection of Audit Log

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

4.6.6 Audit Log Backup Procedures

Audit logs are backed up on a periodic basis.

4.6.7 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.

4.6.8 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.

4.6.9 Vulnerability Assessments

Starfield performs periodic vulnerability assessments of its PKI environment. The results of such assessments are used to enhance the security of the environment.

4.7 Records Archival

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

4.7.1 Types of Event Recorded

Starfield maintains an archive of logs that include the recorded events specified in §4.6.1.

4.7.2 Retention Period for Archive

Starfield archives and retains audit logs in accordance with §4.6.4.

4.7.3 Protection of Archive

See §4.6.5.

4.7.4 Archive Backup Procedures

Starfield maintains copies of its archived records at separate locations.

4.7.5 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.

4.7.6 Archive Collection System (Internal or External)

No stipulation.

4.7.7 Procedures to Obtain and Verify Archive Information

No stipulation.

4.8 Key Changeover

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

4.9 Compromise and Disaster Recovery

To enable the recovery its PKI operations in the event of a disaster, Starfield has implemented the following:

- Secure storage of backup cryptographic hardware modules containing copies of the Starfield CA private keys at an alternate location
- Secure storage of the requisite activation materials at an alternate location
- Secure storage of backups of system, data, and configuration information
- Secured disaster recovery site where operations can be restored in the event of a disaster at Starfield's primary location
- Disaster recovery plan
- Periodic disaster recovery plan testing.

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.

4.10 CA 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.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Starfield PKI systems are hosted and managed using secure facilities in the Phoenix, Arizona metropolitan area 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 facility has 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 Offsite Backup

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

5.1.8 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.

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 §6.2.2. Other operations may require only one trusted individual.

5.2.3 Identification and Authentication for Each Role

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

5.3 Personnel Controls

5.3.1 Background, 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

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 as necessary. 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.

5.3.7 Contracting Personnel Requirements

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

5.3.8 Documentation Supplied to Personnel

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

6 Technical Security Controls

6.1 Key Pair Generation

6.1.1 Key Pair Generation

CA key pair generation uses cryptographic modules that meet the requirements of §6.2.1 and requires the participation of multiple trusted employees.

Subscriber key pair generation is performed by the Subscriber.

6.1.2 Private Key Delivery to Entity

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 Users

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 160-bit SHA-1 hash and/or a 256-bit SHA-256 hash of the Starfield Root CA certificates are 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 are 1024 bit or higher RSA keys. In addition, CA key pairs used to issue certificates after January 1, 2012 are 2048 bit or higher RSA keys. Subscriber key pairs are 1024 bit or higher RSA keys. In addition, Subscriber key pairs in certificates issued after January 1, 2012 are 2048 bit or higher RSA keys.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

6.1.7 Hardware/Software Key Generation

Starfield CA key pairs are generated in and protected by hardware security modules certified to FIPS 140-1 level 3 or FIPS 140-2 level 3.

Subscriber key pairs are generated and stored in hardware or software. It is recommended that the Subscriber use a FIPS 140-2 certified cryptographic module for key generation.

6.1.8 Key Usage Purposes

Key pairs may be used as follows:

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

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

6.2 CA Private Key Protection

6.2.1 Standards for Cryptographic Module

The Starfield PKI uses cryptographic modules that are certified to FIPS 140-1 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). This is enforced by:

- requiring 3 of 5 shareholders to present their assigned activation materials to activate the hardware security module
- requiring 3 individuals to physically access the hardware security module
- requiring 1 or more individuals with sufficient CA system privileges

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). This is enforced by:

- requiring 3 of 8 shareholders to present their assigned activation materials to activate the hardware security module
- requiring 2 individuals to physically access the online HSM

- requiring 3 individuals to physically access activation materials required (for CA key backup and 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 and Archival

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

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

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

6.2.5 Private Key Entry into Cryptographic Module

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

6.2.6 Method of Activating Private Keys

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

Subscriber private keys should be protected with a pass phrase.

6.2.7 Method of Deactivating Private Key

CA private keys are de-activated by ending the session with the HSM device.

6.2.8 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.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Copies of CA and Subscriber certificates are archived in accordance with §4.7.

6.3.2 Usage periods for the Public and Private Keys

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	5 years (or maximum allowed in applicable guidelines)**

* 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.

** Prior to August 9, 2013, the maximum validity period for Subscriber certificates was 10 years.

6.4 Activation Data

HSMs used for CA private key protection are configured to require multiple key shareholders as described in §6.2.2. The activation materials are used only when needed and stored in a secure site when not in use.

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.

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 Starfield Software Development Lifecycle processes. Approvals are required at all stages of development by the Starfield Governance and Policy Committee. 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 Ratings

No stipulations

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 Cryptographic Module Engineering Controls

The Starfield PKI uses cryptographic modules that meet the requirements of §6.2.1.

7 Certificate and CRL Profiles

7.1 Certificate Profiles

7.1.1 Root CAs

The following certificate profile is used for the Starfield ValiCert Root CA.

Field	Description
Version	V1
Serial Number	1 (0x1)
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	E = info@valicert.com CN = http://www.valicert.com/ OU = ValiCert Class 2 Policy Validation Authority O = ValiCert, Inc. L = ValiCert Validation Network
Valid From	June 26, 1999 00:19:54 GMT
Valid To	June 26, 2019 00:19:54 GMT

Field	Description
Subject	E = info@valicert.com CN = http://www.valicert.com/ OU = ValiCert Class 2 Policy Validation Authority O = ValiCert, Inc. L = ValiCert Validation Network
Subject Public Key Information	RSA (1024 bits)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.1.2 Issuing CA

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

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

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

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

7.1.3 Bridge CA Certificates

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

The following certificate profile is used for the certificate which cross certifies the Go Daddy Class 2 Certification Authority with the ValiCert Class 2 Policy Validation Authority root.

Field	Description
Version	V3
Serial Number	269 (0x10D)
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)

Field	Description
Issuer	E = info@valicert.com CN = http://www.valicert.com/ OU = ValiCert Class 2 Policy Validation Authority O = ValiCert, Inc. L = ValiCert Validation Network
Valid From	June 29, 2004 17:06:20 GMT
Valid To	June 29, 2024 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:	
Key Usage	keyCertSign, cRLSign
Basic Constraints	Subject Type=CA Path Length Constraint=None
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = http://certificates.godaddy.com/repository/root.crl
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
Certificate Policies	[1]Certificate Policy: Policy Identifier=anyPolicy (OID: 2 5 29 32 0) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.godaddy.com/repository
Authority Key Identifier	Certificate Issuer: Directory Address: E = info@valicert.com CN = http://www.valicert.com/ OU = ValiCert Class 2 Policy Validation Authority O = ValiCert, Inc. L = ValiCert Validation Network Certificate SerialNumber=01
Subject Key Identifier	d2 c4 b0 d2 91 d4 4c 11 71 b3 61 cb 3d a1 fe dd a8 6a d4 e3

The following certificate profile is used for the certificate which cross certifies the Starfield Class 2 Certification Authority with the ValiCert Class 2 Policy Validation Authority root.

Field	Description
Version	V3
Serial Number	268 (0x10C)
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	E = info@valicert.com CN = http://www.valicert.com/ OU = ValiCert Class 2 Policy Validation Authority O = ValiCert, Inc. L = ValiCert Validation Network
Valid From	June 29, 2004 17:39:16 GMT
Valid To	June 29, 2024 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:	
Key Usage (critical)	keyCertSign, cRLSign
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=None
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL = http://certificates.starfieldtech.com/repository/root.crl
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
Certificate Policies	[1]Certificate Policy: Policy Identifier=anyPolicy (OID: 2 5 29 32 0) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository
Authority Key Identifier	Certificate Issuer: Directory Address: E = info@valicert.com CN = http://www.valicert.com/ OU = ValiCert Class 2 Policy Validation Authority O = ValiCert, Inc. L = ValiCert Validation Network Certificate SerialNumber=01

Field	Description
Subject Key Identifier	bf 5f b7 d1 ce dd 1f 86 f4 5b 55 ac dc d7 10 c2 0e a9 88 e7

The following certificate profile is used for the 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

Field	Description
Certificate Policies	[1]Certificate Policy: Policy Identifier=anyPolicy (OID: 2 5 29 32 0) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://certs.godaddy.com/repository/

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

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

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

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

Field	Description
Version	V3
Serial Number	30 dc a9
Signature Algorithm Identifier	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	CN=Starfield Services Root Certificate Authority OU=http://certificates.starfieldtech.com/repository/ O = Starfield Technologies, Inc. L=Scottsdale S=Arizona C = US
Valid From	January 1, 2014 07:00:00 GMT
Valid To	May 30, 2031 07:00:00 GMT
Subject	CN = Starfield Services Root Certificate Authority - G2 O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Subject Public Key Information	RSA (2048 bit) (OID: 1.2.840.113549.1.1.1)
Extensions:	
Basic Constraints (critical)	Subject Type=CA
Key Usage (critical)	keyCertSign, cRLSign

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

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

Field	Description
Version	V3
Serial Number	00 d8 c9 33 43 fe 5d 39 29
Signature Algorithm Identifier	sha256RSA (OID: 1.2.840.113549.1.1.11)
Issuer	OU=Starfield Class 2 Certification Authority O = Starfield Technologies, Inc. C = US
Valid From	September 2, 2009 00:00:00 GMT
Valid To	June 28, 2034 18:00:00 GMT
Subject	CN = Starfield 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:	

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

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	August 30, 2009 00:00:00 GMT
Valid To	June 28, 2034 17:39:16 GMT

Field	Description
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	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)

7.1.4 End Entity SSL Certificates

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

Field	Description
Version	V3
Serial Number	unique value with 64-bits of entropy for each certificate issued by the Issuing CA
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)

Field	Description
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 five years (39 months after April 1, 2015) after Certificate issuance (depending on SSL certificate type).
Subject (Medium Assurance Certificates	CN = domain name of Subscriber's web site OU = "Domain Control Verified" or similar text indicating the assurance level of the certificate.
Subject (High Assurance Certificates	CN = domain name of Subscriber's web site O = Subscriber's organization or individual name L = City/town S = State C = Country
Subject (Extended Validation Certificates)	CN = domain name of Subscriber's web site O = Subscriber's full legal organization name. An assumed name or DBA may also be included L = City/town of place of business S = State of place of business C = Country of place of business serialNumber= Registration number assigned by incorporating authority or date of incorporation or registration businessCategory=vetting category used to issue certificate as defined in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates jurisdictionLocalityName= City/town of incorporation or registration (if applicable) jurisdictionStateOrProvinceName= State of incorporation or registration (if applicable) jurisdictionCountryName= Country of incorporation or registration
Subject Public Key Information	RSA (2048 bits or greater)
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

Field	Description
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

Field	Description
	individual requesting the certificate has access to the domain name(s) that are specified in the certificate application (per §3.1.13)
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate
1.3.6.1.4.1.11129.2.4.2 (Extended Validation Certificates)	One or more RFC 6962 Signed Certificate Timestamps

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

Field	Description
Version	V3
Serial Number	unique value with 64-bits of entropy for each certificate issued by the Issuing CA
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	serialNumber = 10688435 CN = Starfield Secure Certification Authority OU=http://certificates.starfieldtech.com/repository O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
Valid From	Date and time of Certificate issuance
Valid To	A date up to five years (39 months after April 1, 2015) after Certificate issuance (depending on SSL certificate type).
Subject (Medium Assurance Certificates	CN = domain name of Subscriber's web site OU = "Domain Control Verified" or similar text indicating the assurance level of the certificate.
Subject (High Assurance Certificates	CN = domain name of Subscriber's web site O = Subscriber's organization or individual name L = City/town S = State C = Country

Field	Description
Subject (Extended Validation Certificates)	CN = domain name of Subscriber's web site O = Subscriber's full legal organization name. An assumed name or DBA may also be included L = City/town of place of business S = State of place of business C = Country of place of business serialNumber= Registration number assigned by incorporating authority or date of incorporation or registration businessCategory=vetting category used to issue certificate as defined in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates jurisdictionLocalityName= City/town of incorporation or registration (if applicable) jurisdictionStateOrProvinceName= State of incorporation or registration (if applicable) jurisdictionCountryName= Country of incorporation or registration
Subject Public Key Information	RSA (2048 bits or greater)
Extensions:	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Key Usage (critical)	Digital Signature, Key Encipherment
CRL Distribution Points	CRL Distribution Point Distribution Point Name: Full Name: URL =<current CRL URI> The specific URI will vary depending on certificate type and CRL scope.
Certificate Policies (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	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.3

Field	Description
Validation Certificates)	[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 §3.1.13)
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate
1.3.6.1.4.1.11129.2.4.2 (Extended Validation Certificates)	One or more RFC 6962 Signed Certificate Timestamps

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

Field	Description
Version	V3
Serial Number	unique value with 64-bits of entropy for each certificate issued by the Issuing CA

Field	Description
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 five years (39 months after April 1, 2015) after Certificate issuance (depending on SSL certificate type).
Subject (Basic and Medium Assurance Certificates	CN = domain name of Subscriber's web site OU = "Domain Control Verified" or similar text indicating the assurance level of the certificate.
Subject (High Assurance Certificates	CN = domain name of Subscriber's web site O = Subscriber's organization or individual name L = City/town S = State C = Country
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

Field	Description
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."

Field	Description
	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 §3.1.13)
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate
1.3.6.1.4.1.11129.2.4.2 (Extended Validation Certificates)	One or more RFC 6962 Signed Certificate Timestamps

The following certificate profile is used for 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 five years (39 months after April 1, 2015) after Certificate issuance (depending on SSL certificate type).
Subject (Basic and Medium Assurance Certificates	CN = domain name of Subscriber's web site OU = "Domain Control Verified" or similar text indicating the assurance level of the certificate.
Subject (High Assurance Certificates	CN = domain name of Subscriber's web site O = Subscriber's organization or individual name L = City/town S = State C = Country

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

Field	Description
Certificate Policies (High Assurance Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.2.2 (OV) or 2.23.140.1.2.3 (IV)
Certificate Policies (Extended Validation Certificates)	[1]Certificate Policy: Policy Identifier=2.16.840.1.114414.1.7.23.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://certificates.starfieldtech.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.1
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.starfieldtech.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certificates.starfieldtech.com/repository/sfig2.crt
Authority Key Identifier	KeyID: 25 45 81 68 50 26 38 3d 3b 2d 2c be cd 6a d9 b6 3d b3 66 63
Subject Alternative Name	Required, set to: 1. DNS=fully qualified domain name of the Subscriber's site, domain name remaining after removing "www." from the left hand portion of the fully qualified domain name. And/or: 2. DNS=domain name of Subscriber's site , domain name of additional sites which have undergone the following verification step as part of the authentication process: the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application (per §3.1.13)
Subject Key Identifier	160-bit SHA1 hash of the public key contained within this certificate

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

7.1.5 End Entity Code Signing Certificates

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.2 CRL Profiles

CRLs MAY be either V1 or V2. When a V2 CRL is issued, additional fields may be present as shown in the tables below.

7.2.1 Root CAs

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

Field	Description
Version	V1 or V2 (0x1)
Signature	SHA-1 or SHA-256
Issuer	Subject of the corresponding root certificate
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	365 days after This Update.
CRL extensions (V2 only)	
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 (V2 only and optional for any given CRL entry)	

Field	Description

CRL Reason Code	One of the following reason codes:
	`unspecified (0)`
	`keyCompromise (1)`
	`cACompromise (2)`
	`affiliationChanged (3)`
	`superseded (4)`
	`cessationOfOperation (5)`
	`certificateHold (6)`
	`removeFromCRL (8)`
	`privilegeWithdrawn (9)`
	`aACompromise (10)`

Invalidity Date	A GeneralizedTime denoting the effective time when the given serial number is to be considered invalid.

7.2.2 Issuing CAs

The following CRL profile is used for Starfield Issuing CAs.

Field	Description
Version	V1 or V2 (0x1)
Signature	SHA-1 or SHA-256
Issuer	Subject of the corresponding Issuing CA certificate
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	365 days after This Update.
CRL extensions (V2 only)	
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 (V2 only and optional for any given CRL entry)	
CRL Reason Code	One of the following reason codes: unspecified (0) keyCompromise (1) cACompromise (2) affiliationChanged (3) superseded (4) cessationOfOperation (5) certificateHold (6) removeFromCRL (8) privilegeWithdrawn (9) aACompromise (10)
Invalidity Date	A GeneralizedTime denoting the effective time when the given serial number is to be considered invalid.

8 Specification Administration

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.

8.2 Publication and Notification Policies

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

8.3 CPS Approval Procedures

See §8.1.

9 Definitions

- Applicant - the natural person or legal entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber.
- Applicant Representative - a natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.
- Attestation Letter - a letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
- Authorization Domain Name - the Domain Name used to obtain authorization for certificate issuance for a given FQDN.
- Authorized Port - one of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).
- Base Domain Name - the portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix.
- Basic Assurance – Starfield's vetting process that verifies access to the domain
- Certificate - digital record that contains information such as the Subscriber's distinguished name and public key, and the signer's signature and data
- Certificate Revocation List (CRL) – periodically published listing of all certificates that have been revoked for use by Relying Parties
- Certificate Signing Request (CSR) – a message sent to the certification authority containing the information required to issue a digital certificate
- Certification Authority (CA) – see §1.3.1
- Code Signing Certificate – a certificate issued to an organization for the purpose of digitally signing software
- Compromise - a loss, theft, disclosure, modification, unauthorized use, or other breach of security related to a Private Key
- Custom Certificate – a certificate profile defined for a specific, non-standard usage

- Distinguished Name (DN) – a globally unique identifier representing a Subscriber
- Domain Authorization Document - documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar attesting to the authority of an Applicant to request a Certificate for a specific domain namespace.
- Domain Contact - the Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record
- Domain Name - the label assigned to a node in the Domain Name System.
- Domain Name Registrant - sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
- Domain Name Registrar: a person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
- Extended Validation (EV) – certificate issued under the Guidelines for the Issuance and Management of Extended Validation Certificates published by the CA/Browser Forum (http://www.cabforum.org)
- Fully-Qualified Domain Name (FQDN) - a Domain Name that includes the labels of all superior nodes in the Internet Domain Name System
- Governance and Policy Committee (GPC) – the Starfield committee which creates and maintains the policies related to the Starfield Public Key Infrastructure. Also known as the Policy Authority Committee (PAC)
- Hardware Security Module (HSM) –a specialized computer hardware system designed to securely store encryption keys
- High Assurance – Starfield's vetting process that verifies the identity of the individual or organization that requested the certificate and access to the domain
- Medium Assurance – Starfield's vetting process that verifies access to the domain
- Online Certificate Status Protocol (OCSP) – A standardized query/response protocol whereby a client can request the status of a given Certificate and be given a response that will indicate whether the Certificate is valid or revoked.
- Policy Authority Committee – See Governance and Policy Committee
- Private Key – a confidential encrypted electronic data file that interfaces with a Public Key using the same encryption algorithm, in order to verify Digital Signatures and encrypt files or messages
- Public Key – an encrypted electronic data file that is publicly available for interfacing with a Private Key

- Registration Authority (RA) – see §1.3.2
- 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
- Reseller – a person or organization which is given permission by Starfield to sell products to Subscribers
- Starfield – Starfield Technologies, LLC, and its resellers
- Starfield PKI - the Starfield Public Key Infrastructure that provides Certificates for individuals and entities.
- Subscriber – the individual or entity that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate
- Subscriber Agreement – an agreement which specifies the stipulations under which a person or organization acts as a Subscriber
- Subject Identity Information - information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.
- Unified Communications Certificate (UCC) – certificate that includes multiple fully qualified domain names in the Subject Alternative Name extension.