Starfield Technologies, Inc.

**Certificate Policy
and
Certification Practice Statement
(CP/CPS)**

Version 2.0
January 9, 2007

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.

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
Valicert 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.
Starfield 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 Gaddy brand. Issues any new CAs for different types of PKI services except those used with the Go Daddy brand..
Go Daddy 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 Gaddy brand. Issues any new CAs for different types of PKI services sold under the Go Daddy brand
Legacy Issuing CA	Starfield Secure Certification Authority	Issues SSL web server certificates to authenticated organizations and individuals.
Starfield 2048-bit Issuing CA	Starfield Class 2 Certification Authority	Issues SSL web server certificates to authenticated organizations and individuals.
Go Daddy 2048-bit Issuing CA	Go Daddy Class 2 Certification Authority	Issues Go Daddy branded SSL web server certificates to authenticated organizations and individuals.

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

Starfield CP-CPS V2.0

1.3.3 End Entities

End Entities include Subscribers and Relying Parties.

For the Starfield Root CA 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

This CP/CPS is administered by the Starfield PKI Policy Committee. Contact information is listed below:

> Starfield Technologies, Inc.
> 14455 N. Hayden Road, Suite 219
> Scottsdale, AZ 85260
> Phone: 480-505-8800
> Fax: 480-505-8865
> E-mail: practices@starfieldtech.com

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

2 General Provisions

2.1 Obligations

2.1.1 Starfield PKI Committee Obligations

Obligations of the Starfield PKI Committee in its role as Policy Authority (PA) 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:

Starfield CP-CPS V2.0

- 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 Certificate CRL, 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

- Starfield warrants that it is providing the Certificate Service with reasonable skill and care

- Starfield warrants that to the best of its knowledge there are no material misrepresentations of fact in the Certificates known to or originating from the entities approving the Certificate Applications or issuing the Certificates
- Starfield warrants that there are no informational errors in the Certificates introduced by the entities that approved the Certificate Applications or issued the Certificates as a result of failing to exercise reasonable care in managing the Certificate Applications or creating the Certificates
- Starfield warrants that their Certificates meet all of the material requirements of this CPS
- Starfield warrants that the Certificates, the revocation services and its use of a repository conform to this CPS in all material respects

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 TWO THOUSAND UNITED STATES DOLLARS ($2000.00 U.S.) ("CUMULATIVE DAMAGE LIMIT"). THIS LIMITATION 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

Starfield CP-CPS V2.0

CERTIFICATE EXCEED THE CUMULATIVE DAMAGE CAP SET FORTH IN THIS SECTION ABOVE, THE AMOUNTS AVAILABLE UNDER THE CUMULATIVE DAMAGE CAP 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 CAP 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) the Subscriber failed to stop using a Starfield Certificate after the information contained in such Starfield Certificate changed or after circumstances changed so that the information contained in such Starfield Certificate became misleading or inaccurate;

(v) 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;
(vi) the Private Key associated with the Starfield Certificate has been Compromised; or
(vii) 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, and

- The Subscriber is not using the Certificate Service in any way that infringes upon the rights of third parties.

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, to, 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, Relying party agreements disclaim, and Subscriber 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.

Starfield CP-CPS V2.0

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.

Starfield CP-CPS V2.0

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

Starfield CP-CPS V2.0

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 CA, 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.

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 examination. 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 $1 million 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 PKI 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. 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 a Distinguished Name that is in compliance with the X.500 standard for Distinguished Names. The Starfield PKI approves naming conventions for the creation of distinguished names for certificate applicants.

The Issuer and Subject Distinguished Names 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, Distinguished Names shall be meaningful.

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

Distinguished Names of Extended Validation and High Assurance certificates are to be unambiguous and unique within the Starfield CA's domain, except in the case of a single Subscriber who is permitted to have multiple active certificates with identical Subject Distinguished Names. Multiple Medium Assurance certificates containing the same Subject Distinguished Name are permitted within the Starfield CA's domain.

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   Authentication of Organization Identity

For High Assurance organizational Subscribers, Starfield verifies the following:
- the organization name represents an organization currently registered with a government authority
- the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application
- the individual requesting the certificate is associated with the organization named in the certificate

3.1.9   Authentication of Individual Identity

For High Assurance individual Subscribers, Starfield verifies the following:
- the identity of the individual named in the certificate application
- the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application

In the case of a small business/sole proprietorship that is not registered with a government authority, Starfield will optionally include the entity's "doing business as" (DBA) name in an informational, unauthenticated "organizational unit" (OU) field.

3.1.10   Medium Assurance Authentication

For Medium Assurance Subscribers, Starfield verifies the following:
- the individual requesting the certificate has access to the domain name(s) that are specified in the certificate application

3.1.11   Authentication of Corporate Identity for Extended Validation Certificates

For Extended Validation corporate Subscribers, Starfield verifies the following in accordance with the CA/Browser Forum Guidelines for Extended Validation Certificates:
- Legal Existence
- Assumed Name (optional)
- Physical Existence
- Operational Existence (if records indicate that the corporation is less than three years old)
- Main Telephone number
- Domain ownership or exclusive right to use
- Name, title, and authority of contract signer, and certificate approver

3.2   Routine Re-key

Routine re-key of CAs is performed in accordance with §4.9.

Subscribers are permitted to reuse a previous certificate request to replace an expiring or expired Certificate.

Where the Subscriber holds a valid Starfield High or Medium Assurance certificate and the initial Subscriber identification and authentication process (as described in §3.1.8, 3.1.9, and 3.1.10) has been performed within the previous 13 months, Starfield may authenticate a renewal certificate request using a shared secret. Where the Subscriber holds a valid Starfield Extended Validation certificate and the initial Subscriber identification and authentication process (as described in §3.1.11) has been performed within the previous year, Starfield may authenticate a renewal certificate request using a shared secret. In all other cases, Starfield shall re-perform the initial Subscriber identification and authentication process.

3.3   Re-key After Revocation

In the event that a Starfield CA certificate must be revoked, the CA will be re-keyed in accordance with §4.9 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 and 3.1.9.

3.4   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 in accordance with §4.9.

Certificate renewal for end-user Subscriber certificates is supported via the routine re-key process described in §3.1.11.

3.5   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 a 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.

3.6   Suspension Request

See §4.4.

3.7   Request to Release Suspension

See §4.4.

4   Operational Requirements

4.1   Certificate Application

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

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, 3.1.9, and 3.1.11 – 3.4.

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 §3.5.
- 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. Manual approval is required of all revocation requests.

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 published within seven days of the processing of an authenticated revocation request. Revoked certificates are listed in the CRL until the certificate expires.

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 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	5 years
Physical access system logs	5 years
Manual logs of physical access	5 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.

Starfield CP-CPS V2.0

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 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 Scottsdale, Arizona 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 identity verification and checks of character references, employment, education and criminal record. Starfield employees are also required to complete a drug screening.

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:
- 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, upon hire 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 certificate may also be downloaded from the Starfield repository. A 160-bit SHA-1 hash of the Starfield Root CA certificate is posted in the Starfield repository so that users may verify the authenticity of the Starfield Root CA certificate.

6.1.5   Key Sizes

Starfield CA key pairs are 1024 bit or higher RSA keys. Subscriber key pairs are 1024 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.

Subscriber key pairs are generated and stored in hardware or software. It is recommended that the Subscriber use a FIPS 140-1 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 Sub-CA certificates and CRLs.
Issuing CAs	Signing of Subscriber certificates and CRLs.
Subscriber	Server authentication, 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 2 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 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	10 years (or maximum allowed in applicable guidelines)

6.4   Activation Data

HSMs used for CA private key protection are configured to require 3 of 5 shareholders to present their assigned activation materials to activate the hardware security module as described in §6.2.2. These 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 PKI Committee. All code is verified, using digital signatures and hashing, before being deployed into the production CA environment.

Starfield CP-CPS V2.0

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	01
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 25, 1999
Valid To	June 25, 2019
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)
Extensions:	
Friendly name	ValiCert Class 2 Policy Validation Authority
Enhanced Key Usage	Secure Email, Server Authentication

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

Field	Description
Version	V3
Serial Number	00
Signature Algorithm Identifier	sha1RSA
Issuer	OU=Starfield Class 2 Certification Authority O=Starfield Technologies, Inc. C=US
Valid From	June 29, 2004
Valid To	June 29, 2034
Subject	OU=Starfield Class 2 Certification Authority O=Starfield Technologies, Inc. C=US
Subject Public Key Information	RSA (2048 bits)
Basic Constraints	Subject Type=CA Path Length Constraint=None

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

Field	Description
Version	V3
Serial Number	00
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
Valid To	June 29, 2034
Subject	OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
Subject Public Key Information	RSA (2048 bits)
Basic Constraints	Subject Type=CA Path Length Constraint=None

7.1.2 Issuing CA

The following certificate profile is used for the Starfield Issuing CA.

Field	Description
Version	V3
Serial Number	260

Field	Description
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	January 14, 2004
Valid To	January 9, 2024
Subject	E=practices@starfieldtech.com CN = Starfield Secure Certification Authority O = Starfield Technologies, Inc. OU=http://www.starfieldtech.com/repository L = Scottsdale S = Arizona C = US
Subject Public Key Information	RSA (1024 bits)
Extensions:	
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing
Basic Constraints	Subject Type=CA Path Length Constraint=None
Enhanced Key Usage	Not used.

CRL Distribution Points	CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	       URL = http://certificates.starfieldtech.com/repository/root.crl

Certificate Policies	[1]Certificate Policy:
	    Policy Identifier=2.16.840.1.113733.1.7.23.3
	    [1,1]Policy Qualifier Info:
	       Policy Qualifier Id=CPS
	       Qualifier:
	         http://www.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

The following certificate profile is used for the Go Daddy 2048-bit Issuing CA.

Starfield CP-CPS V2.0

Field	Description
Version	V3
Serial Number	03 01
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	OU = Go Daddy Class 2 Certification Authority O = The Go Daddy Group, Inc. C = US
Valid From	November 14, 2006
Valid To	November 14, 2026
Subject	CN = Go Daddy Secure Certification Authority O = GoDaddy.com, Inc. OU=http://certificates.godaddy.com/repository C (OID 2.5.4.6) = US L (OID 2.5.4.7) = Scottsdale S (OID 2.5.4.8) = Arizona serialNumber (OID 2.5.4.5) = 07969287
Subject Public Key Information	RSA (2048 bit) (OID: 1.2.840.113549.1.1.1)
Extensions:	
Key Usage	keyCertSign, cRLSign
Basic Constraints	Subject Type=CA Path Length Constraint=0

CRL Distribution Points	CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	      URL = http://certificates.godaddy.com/repository/gdroot.crl

Certificate Policies	[1]Certificate Policy:
	   Policy Identifier=anyPolicy (OID: 2 5 29 32 0)
	   [1,1]Policy Qualifier Info:
	     Policy Qualifier Id=CPS
	     Qualifier:
	      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

Authority Key Identifier	d2 c4 b0 d2 91 d4 4c 11 71 b3 61 cb 3d a1 fe dd a8 6a d4 e3
Subject Key Identifier	fd ac 61 32 93 6c 45 d6 e2 ee 85 5f 9a ba e7 76 99 68 cc e7

The following certificate profile is used for the Starfield 2048-bit Issuing CA.

Field	Description
Version	V3
Serial Number	02 01
Signature Algorithm Identifier	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	OU = Starfield Class 2 Certification Authority O = Starfield Technologies, Inc. C = US
Valid From	November 14, 2006
Valid To	November 14, 2026
Subject	CN = Starfield Secure Certification Authority O = Starfield Technologies, Inc. OU=http://certificates.starfieldtech.com/repository C (OID 2.5.4.6) = US L (OID 2.5.4.7) = Scottsdale S (OID 2.5.4.8) = Arizona serialNumber (OID 2.5.4.5) = 10688435
Subject Public Key Information	RSA (2048 bit) (OID: 1.2.840.113549.1.1.1)
Extensions:	
Key Usage	keyCertSign, cRLSign
Basic Constraints	Subject Type=CA Path Length Constraint=0

CRL Distribution Points	CRL Distribution Point
	   Distribution Point Name:
	      Full Name:
	        URL = http://certificates.starfieldtech.com/repository/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:
	        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

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

Field	Description
Subject Key Identifier	49 4b 52 27 d1 1b bc f2 a1 21 6a 62 7b 51 42 7a 8a d7 d5 56

7.1.3 Bridge CA Certificates

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	01 09
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	November 14, 2006
Valid To	November 14, 2026
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

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

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

Starfield CP-CPS V2.0

Field	Description
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	01 08
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	November 14, 2006
Valid To	November 14, 2026
Subject	OU=Starfield Class 2 Certification Authority O=Starfield Technologies, Inc. C=US
Subject Public Key Information	RSA (2048 bits)
Extensions:	
Key Usage	keyCertSign, cRLSign
Basic Constraints	Subject Type=CA

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

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

7.1.4   End Entity SSL Certificates

The following certificate profile is used for Subscriber Certificates. At a minimum, the following fields will be populated as described, in accordance with IETF RFC 2459.

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	E = practices@starfieldtech.com CN = Starfield Secure Certification Authority O = Starfield Technologies, Inc. OU=http://www.starfieldtech.com/repository L = Scottsdale S = Arizona C = US
Valid From	Date and time of Certificate issuance
Valid To	One to ten years after Certificate issuance (depending on SSL certificate type).
Subject (High Assurance Certificates	CN = domain name of Subscriber's web site (may be fully qualified or wildcard) O = Subscriber's organization or individual name OU = Subscriber's DBA entry if individual but wants company listed. L = City/town S = State C = Country
Subject (Medium Assurance Certificates	CN = domain name of Subscriber's web site (may be fully qualified or wildcard) O = domain name of Subscriber's web site (may be fully qualified or wildcard) OU = "Domain Control Verified" or similar text indicating the assurance level of the certificate.

Field	Description
Subject (Extended Validation Certificates)	CN = domain name of Subscriber's web site (may be fully qualified or wildcard) 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 jurisdictionOfIncorporationLocalityName= City/town of incorporation jurisdictionOfIncorporationStateOrProvinceName= State of incorporation jurisdictionOfIncorporationCountryName= Country of incorporation serialNumber= Registration number assigned by incorporating authority
Subject Public Key Information	RSA (1024 bits or higher)
Extensions:	
Key Usage	Digital Signature, Key Encipherment(A0)
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)

CRL Distribution Points	CRL Distribution Point
	   Distribution Point Name:
	     Full Name:
	      URL =
	http://certificates.starfieldtech.com/repository/starfieldissuing#.crl
	(where # is omitted or set to a value indicating which CRL this certificate should be using)

Certificate Policies (High Assurance Certificates)	[1]Certificate Policy:
	   Policy Identifier=2.16.840.1.[114413 for Go Daddy, 114414 for Starfield].1.7.23.2
	    [1,1]Policy Qualifier Info:
	     Policy Qualifier Id=CPS
	     Qualifier:
	      http://www.starfieldtech.com/repository

Certificate Policies (Medium Assurance Certificates)	[1]Certificate Policy:
	   Policy Identifier=2.16.840.1.[114413 for Go Daddy, 114414 for Starfield].1.7.23.1
	    [1,1]Policy Qualifier Info:
	     Policy Qualifier Id=CPS
	     Qualifier:
	      http://www.starfieldtech.com/repository

Certificate Policies	[1]Certificate Policy:

Field	Description

(Extended Validation Certificates)	Policy Identifier=2.16.840.1.[114413 for Go Daddy, 114414 for Starfield].1.7.23.3
	[1,1]Policy Qualifier Info:
	   Policy Qualifier Id=CPS
	   Qualifier:
	      http://www.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_issuing.crt

Subject Alternative Name	Optional. If included, 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=fully qualified domain name of Subscriber's site, fully qualified 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

7.2   CRL Profiles

7.2.1   Root CAs

The following CRL profile is used for the Starfield Root CA.

Field	Description
Version	V1
Signature	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
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	365 days after CRL issuance.
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 Reason Code*, indicating the reason for revocation.
CRL Entry Extensions	Not used.

The following CRL profile is used for the Starfield Class 2 Certification Authority Root CA.

Field	Description
Version	V1
Signature	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	OU=Starfield Class 2 Certification Authority O=Starfield Technologies, Inc. C=US
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	365 days after CRL issuance.
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 Reason Code*, indicating the reason for revocation.
CRL Entry Extensions	Not used.

The following CRL profile is used for the Go Daddy Class 2 Root CA.

Field	Description
Version	V1
Signature	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	365 days after CRL issuance.

Starfield CP-CPS V2.0

Field	Description
Revoked Certificates	List of information regarding revoked certificates. CRL entries include: • *Serial Number*, identifying the revoked certificate • *Revocation Date*, including the date and time of certificate revocation • *CRL Reason Code*, indicating the reason for revocation.
CRL Entry Extensions	Not used.

7.2.2   Issuing CAs

The following CRL profile is used for the Starfield Issuing CA.

Field	Description
Version	V1
Signature	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	CN = Starfield Secure Certification Authority O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	No greater than 7 days after CRL Issue.
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 Reason Code*, indicating the reason for revocation.
CRL Entry Extensions	Not used.

The following CRL profile is used for the Starfield 2048-bit Issuing CA.

Field	Description
Version	V1
Signature	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	CN = Starfield Secure Certification Authority O = Starfield Technologies, Inc.. OU=http://certificates.starfieldtech.com/repository C (OID 2.5.4.6) = US L (OID 2.5.4.7) = Scottsdale S (OID 2.5.4.8) = Arizona serialNumber (OID 2.5.4.5) = 10688435

Field	Description
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	No greater than 7 days after CRL Issue.
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 Reason Code*, indicating the reason for revocation.
CRL Entry Extensions	Not used.

The following CRL profile is used for the Go Daddy 2048-bit Issuing CA.

Field	Description
Version	V1
Signature	sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer	CN = Go Daddy Secure Certification Authority O = GoDaddy.com, Inc. OU=http://certificates.godaddy.com/repository C (OID 2.5.4.6) = US L (OID 2.5.4.7) = Scottsdale S (OID 2.5.4.8) = Arizona serialNumber (OID 2.5.4.5) = 07969287
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	No greater than 7 days after CRL Issue.
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 Reason Code*, indicating the reason for revocation.
CRL Entry Extensions	Not used.

8   Specification Administration

8.1   Specification Change Procedures

Modifications to this CP/CPS are approved by the Starfield PKI 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

- 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 section 1.3.1

- Compromise - a loss, theft, disclosure, modification, unauthorized use, or other breach of security related to a Private Key

- Distinguished Name (DN) – a globally unique identifier representing a Subscriber

- Extended Validation (EV) – certificate issued under the Guidelines for Extended Validation Certificates published by the CA/Browser Forum

- 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

- Policy Authority (PA) – the Starfield committee which creates and maintains the policies related to the Starfield Public Key Infrastructure

- 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 section 1.3.2

- 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, Inc., 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

Starfield CP-CPS V2.0