



KPMG LLP  
Mission Towers I  
Suite 100  
3975 Freedom Circle Drive  
Santa Clara, CA 95054

## Independent Accountant's Report

To the management of Starfield Technologies, LLC:

We have examined Starfield Technologies, LLC ("Starfield") for its Starfield and Go Daddy Certification Authority (CA) operations at Scottsdale, Arizona and Phoenix, Arizona,

- Starfield's disclosure of its SSL certificate lifecycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Starfield website
- the provision of such services in accordance its disclosed practices, Starfield Technologies, LLC Certificate Policy and Certification Practices Statement (CP/CPS), version 3.10, dated March 1, 2017
- the effectiveness of its controls over
  - key and SSL certificate integrity,
  - the authenticity and confidentiality of SSL subscriber and relying party information,
  - continuity of key and SSL certificate lifecycle management operations, and
  - development, maintenance, and operation of CA systems integrity,
  - and meeting the network and certificate system security requirements set forth by the CA/Browser Forum

throughout the period July 1, 2016 to March 31, 2017 for its CAs as enumerated in Appendix A

Starfield's management is responsible for these disclosures and for maintaining effective controls based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.1. Our responsibility is to express an opinion based on our examination.

The relative effectiveness and significance of specific controls at Starfield and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, throughout the period July 1, 2016 to March 31, 2017, for its Starfield and Go Daddy CAs, in all material respects, Starfield

- disclosed its SSL certificate lifecycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Starfield website,
- provided such services in accordance its disclosed practices,
- maintained effective controls over
  - key and SSL certificate integrity,
  - the authenticity and confidentiality of SSL subscriber and relying party information,
  - continuity of key and SSL certificate lifecycle management operations, and
  - development, maintenance, and operation of CA systems integrity,
  - and meeting the network and certificate system security requirements set forth by the CA/Browser Forum



based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.1.

Because of the nature and inherent limitations of controls, Starfield’s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

We noted the following matters that resulted in a modification of our opinion:

Matters Noted	Relevant WebTrust Criteria
<p>As disclosed by Starfield, it was noted that Starfield mis-issued 8951 certificates during the examination period due to a configuration error that resulted in the domain validation process not being completed accurately in certain circumstances.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.1, Principle 2, Criterion 4.1 and Principle 3, Criterion 7 to not be met.</p>	<p>Principle 2, Criterion 4.1 requires that the CA maintains controls to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Sections 3.2.2.4, 3.2.2.5, 3.2.2.6 and 4.2.2 related to the Fully-Qualified Domain Name(s) (including wildcard domains and new gTLDs (generic top-level domains)) and IP address(es) listed in the Certificate.</p> <p>Principle 3, Criterion 7 requires that the CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.</p>

In our opinion, except for the effects of the matters discussed in the preceding table, throughout the period July 1, 2016 to March 31, 2017, Starfield has, in all material respects:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Starfield Technologies, LLC Certificate Policy and Certification Practices Statement (CP/CPS), version 3.10, dated March 1, 2017including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Starfield website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Starfield)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity



- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.1.

This report does not include any representation as to the quality of Starfield's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.1, nor the suitability of any of Starfield's services for any customer's intended purpose.

KPMG LLP

Santa Clara, California  
August 31, 2017

## Appendix A – Starfield and Go Daddy Root and Issuing CAs

Subject CN	Serial No	Fingerprint - SHA1	Fingerprint - SHA2
Starfield Class 2 Certification Authority	00	ad7e1c28b064ef8f6003402014c3d0e3370eb58a	1465fa205397b876faa6f0a9958e5590e40fcc7faa4fb7c2c8677521fb5fb658
Starfield Root Certificate Authority - G2	00	b51c067cee2b0c3df855ab2d92f4fe39d4e70f0e	2ce1cb0bf9d2f9e102993fbe215152c3b2dd0cabde1c68e5319b839154dbb7f5
Starfield Root Certificate Authority - G3	37 97 3c 60 2b ab 78 9c 96 13 69 5b 6c b0 03 10	6dfccf5ab75115a375a1fa612a476256e95dccc2	6d7f2445b84abb082c5d092ab46177282bac96ee2ba37fea8a1c9a30a0780c1e
Starfield Root Certificate Authority - G4	00 b1 a5 d0 12 b1 61 15 59 76 5f ee d0 07 25 45 92	c52a39f20c134d862c0cb5a5ee5234a0ffcafe9f	f37b58624ff838b8f48ce17a5344a15578d7112ab49f4aa2a99212ec63605158
Starfield Secure Certification Authority	02 01	7e1874a98faa5d6d2f506a8920ff22fbd16652d9	05a6db389391df92e0be93dfa4db1e3cf53903918b8d9d85a9c396cb55df030
Starfield Secure Certificate Authority - G2	07	7edc376dcfd45e6ddf082c160df6ac21835b95d4	93a07898d89b2cca166ba6f1f8a14138ce43828e491b831926bc8247d391cc72
Starfield Secure Certificate Authority - G3	00 ab 23 ac 16 ab 89 cd be	e0e7f3eb1664cc1bf074538eb9e83186c978b814	51bd250721ce5cb9252a60dc9e7b3276399489cc4e0c901440115f617db204e6
Starfield Secure Certificate Authority - G4	16 e6 f8 de 83 0f 23 5a	a276dd454651688ebaaf967f4f939f9b2f8f27dd	f7e18a5bad661f6e24aa521de998a86e8d7d385ad278437c473c0805734a646b
Starfield Services Root Certificate Authority	00	5d003860f002ed829dea4a1868f788186d62127f	b5bd2cb79cbd1907298d6bdf4842e516d8c78fa6fc96d25f71af814e16cc245e
Go Daddy Class 2 Certification Authority	00	2796bae63f1801e277261ba0d77770028f20eee4	c3846bf24b9e93ca64274c0ec67c1ecc5e024ffcacd2d74019350e81fe546ae4
Go Daddy Root Certificate Authority - G2	00	47beabc922eae80e78783462a79f45c254fde68b	45140b3247eb9cc8c5b4f0d7b53091f73292089e6e5a63e2749dd3aca9198eda
Go Daddy Root Certificate Authority - G3	58 56 36 b7 32 66 ef 14 a9 d7 ca 42 21 75 9c d2	78254b20e40965461abf0a745f9d36955cb213e7	51a490f85232d915e3eae3df695811a74d1faebe3b47ec43a58d881d44db4371

<b>Subject CN</b>	<b>Serial No</b>	<b>Fingerprint - SHA1</b>	<b>Fingerprint - SHA2</b>
Go Daddy Root Certificate Authority - G4	00 bd 83 76 4c 96 e5 91 b1 de 1c 57 48 f5 40 a8 05	f00f0478624e179dba30 1b39394b7d46ebf940fc	c1a27ecbdf9cbb3e112cb039cb3ac9 e418b6c528d2822ffb68c9c7261850 bc41
Go Daddy Secure Certification Authority	03 01	7c4656c3061f7f4c0d67b 319a855f60ebc11fc44	09ed6e991fc3273d8fea317d339c02 041861973549cfa6e1558f411f11211 aa3
Go Daddy Secure Certificate Authority - G2	07	27ac9369faf25207bb262 7cefaccbe4ef9c319b8	973a41276ffd01e027a2aad49e34c3 7846d3e976ff6a620b6712e3383204 1aa6
Go Daddy Secure Certificate Authority - G3	00 e1 d9 c6 ba 69 1a c4 a4	c2d49a088f1ae53856d0 931f7b641774b8e0df9e	91b45fd047e5477642806d93b76e76 dd308a202c754d94633733409577af 9713
Go Daddy Secure Certificate Authority - G4	00 a5 89 b5 13 01 54 db fe	49bacbdf4d8a2969b31 32e8b1112ca61d0970eb	cb35eea6b78cefd67e7dc7fe6fa3b38 dfd601d903fa29266b34c839411541 c8c



**Assertion by Management as to  
Its Disclosure of its Business Practices and its Controls  
Over Certification Authority Operations  
throughout the period July 1, 2016 to March 31, 2017**

Starfield Technologies, LLC operates the SSL Certification Authority (CA) services known as Starfield and Go Daddy CAs, as enumerated in Appendix A.

Starfield management has assessed its disclosures of its certificate practices and controls over its CA services. During our assessment, we noted the following matters which caused the relevant criteria to not be met:

Matters Noted	Relevant WebTrust Criteria
<p>Starfield mis-issued 8951 certificates during the examination period due to a configuration error that resulted in the domain validation process not being completed accurately in certain circumstances.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.1, Principle 2, Criterion 4.1 and Principle 3, Criterion 7 to not be met</p> <p>In response to the misissuance of SSL certificates in January 2017, management took timely action to identify the cause, document the process, revoke all impacted certificates, and notify customers, browsers, and CAs. Additionally, management was careful to ensure that when the certificates in question were identified, they were revoked within 24 hours of identification. For additional investigation and remediation timelines, refer to the publicly disclosed incident report that was posted to the “mozilla.dev.security.policy” email list on 1/10/2017. Additionally, in April 2017, management formalized the automated testing process. Details of automated testing procedures have been published on the Starfield and GoDaddy repositories.</p>	<p>Principle 2, Criterion 4.1 requires that the CA maintains controls to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Sections 3.2.2.4, 3.2.2.5, 3.2.2.6 and 4.2.2 related to the Fully-Qualified Domain Name(s) (including wildcard domains and new gTLDs (generic top-level domains)) and IP address(es) listed in the Certificate.</p> <p>Principle 3, Criterion 7 requires that the CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity</p>

Based on that assessment, except for the matters described in the preceding table, in providing its SSL Certification Authority (CA) services at Scottsdale, Arizona and Phoenix, Arizona, throughout the period July 1, 2016 to March 31, 2017, Starfield has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Starfield Technologies, LLC Certificate Policy and Certification Practices Statement (CP/CPS), version 3.10, dated March 1, 2017

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Starfield website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Starfield)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.1.

Starfield Technologies, LLC

Arne Josefsberg  
Chief Information Officer  
August 31, 2017

## Appendix A – Starfield and Go Daddy Root and Issuing CAs

Subject CN	Serial No	Fingerprint - SHA1	Fingerprint - SHA2
Starfield Class 2 Certification Authority	00	ad7e1c28b064ef8f6003402014c3d0e3370eb58a	1465fa205397b876faa6f0a9958e5590e40fcc7faa4fb7c2c8677521fb5fb658
Starfield Root Certificate Authority - G2	00	b51c067cee2b0c3df855ab2d92f4fe39d4e70f0e	2ce1cb0bf9d2f9e102993fbe215152c3b2dd0cabde1c68e5319b839154dbb7f5
Starfield Root Certificate Authority - G3	37 97 3c 60 2b ab 78 9c 96 13 69 5b 6c b0 03 10	6dfccf5ab75115a375a1fa612a476256e95dccc2	6d7f2445b84abb082c5d092ab46177282bac96ee2ba37fea8a1c9a30a0780c1e
Starfield Root Certificate Authority - G4	00 b1 a5 d0 12 b1 61 15 59 76 5f ee d0 07 25 45 92	c52a39f20c134d862c0cb5a5ee5234a0ffcafe9f	f37b58624ff838b8f48ce17a5344a15578d7112ab49f4aa2a99212ec63605158
Starfield Secure Certification Authority	02 01	7e1874a98faa5d6d2f506a8920ff22fbd16652d9	05a6db389391df92e0be93fdfa4db1e3cf53903918b8d9d85a9c396cb55df030
Starfield Secure Certificate Authority - G2	07	7edc376dcfd45e6ddf082c160df6ac21835b95d4	93a07898d89b2cca166ba6f1f8a14138ce43828e491b831926bc8247d391cc72
Starfield Secure Certificate Authority - G3	00 ab 23 ac 16 ab 89 cd be	e0e7f3eb1664cc1bf074538eb9e83186c978b814	51bd250721ce5cb9252a60dc9e7b3276399489cc4e0c901440115f617db204e6
Starfield Secure Certificate Authority - G4	16 e6 f8 de 83 0f 23 5a	a276dd454651688ebaaf967f4f939f9b2f8f27dd	f7e18a5bad661f6e24aa521de998a86e8d7d385ad278437c473c0805734a646b
Starfield Services Root Certificate Authority	00	5d003860f002ed829dea41868f788186d62127f	b5bd2cb79cbd1907298d6bdf4842e516d8c78fa6fc96d25f71af814e16cc245e
Go Daddy Class 2 Certification Authority	00	2796bae63f1801e277261ba0d77770028f20eee4	c3846bf24b9e93ca64274c0ec67c1ecc5e024ffcacd2d74019350e81fe546ae4
Go Daddy Root Certificate Authority - G2	00	47beabc922eae80e78783462a79f45c254fde68b	45140b3247eb9cc8c5b4f0d7b53091f73292089e6e5a63e2749dd3aca9198eda
Go Daddy Root Certificate Authority - G3	58 56 36 b7 32 66 ef 14 a9 d7 ca 42 21 75 9c d2	78254b20e40965461abf0a745f9d36955cb213e7	51a490f85232d915e3eae3df695811a74d1fae3b47ec43a58d881d44db4371



<b>Subject CN</b>	<b>Serial No</b>	<b>Fingerprint - SHA1</b>	<b>Fingerprint - SHA2</b>
Go Daddy Root Certificate Authority - G4	00 bd 83 76 4c 96 e5 91 b1 de 1c 57 48 f5 40 a8 05	f00f0478624e179dba30 1b39394b7d46ebf940fc	c1a27ecbdf9cbb3e112cb0 39cb3ac9e418b6c528d28 22ffb68c9c7261850bc41
Go Daddy Secure Certification Authority	03 01	7c4656c3061f7f4c0d67b 319a855f60ebc11fc44	09ed6e991fc3273d8fea31 7d339c02041861973549cf a6e1558f411f11211aa3
Go Daddy Secure Certificate Authority - G2	07	27ac9369faf25207bb262 7cefaccbe4ef9c319b8	973a41276ffd01e027a2aa d49e34c37846d3e976ff6a 620b6712e33832041aa6
Go Daddy Secure Certificate Authority - G3	00 e1 d9 c6 ba 69 1a c4 a4	c2d49a088f1ae53856d0 931f7b641774b8e0df9e	91b45fd047e5477642806d 93b76e76dd308a202c754 d94633733409577af9713
Go Daddy Secure Certificate Authority - G4	00 a5 89 b5 13 01 54 db fe	49bacbddf4d8a2969b31 32e8b1112ca61d0970eb	cb35eea6b78cefd67e7dc7 fe6fa3b38dfd601d903fa29 266b34c839411541c8c