



Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 S Hanley Rd, #800
St. Louis, MO 63105

REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of Amazon Trust Services, LLC ("ATS"):

We have examined ATS management's [assertion](#) that for its Certification Authority ("CA") operations in the United States of America, throughout the period January 16, 2018 to January 15, 2019 for its CAs enumerated in [Attachment B](#), ATS has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certification Practice Statement and Certificate Policy enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
 - ATS' Certification Practice Statement is consistent with its Certificate Policy; and
 - ATS provides its services in accordance with its Certificate Policy and Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated; and
 - subordinate CA certificate requests are accurate, authenticated, and approved
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities v2.1](#). ATS' management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion, based on our examination.

The relative effectiveness and significance of specific controls at ATS 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.

ATS did not escrow CA keys, did not provide certificate suspension services, and did not provide the subscriber key life cycle management services. Accordingly, our examination did not extend to controls that would address those criteria.



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 management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, ATS' 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.

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ATS' services other than its CA operations in the United States of America, nor the suitability of any of ATS' services for any customer's intended purpose.

ATS' use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

BDS USA, LLP

St. Louis, Missouri
April 8, 2019



ATTACHMENT A - IN-SCOPE CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS

Amazon Trust Services, LLC Certification Practice Statement and Certificate Policy Versions in Scope

Policy Name	Version	Date
Amazon Trust Services Certification Practice Statement	1.0.7	April 13, 2018
Amazon Trust Services Certification Practice Statement	1.0.6	January 15, 2018
Amazon Trust Services Certificate Policy	1.0.6	April 13, 2018
Amazon Trust Services Certificate Policy	1.0.5	January 15, 2018



ATTACHMENT B - IN-SCOPE CAs

Root CAs	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
CN=Amazon Root CA 1,O=Amazon,C=US	06 6c 9f cf 99 bf 8c 0a 39 e2 f0 78 8a 43 e6 96 36 5b ca	8d a7 f9 65 ec 5e fc 37 91 0f 1c 6e 59 fd c1 cc 6a 6e de 16	8e cd e6 88 4f 3d 87 b1 12 5b a3 1a c3 fc b1 3d 70 16 de 7f 57 cc 90 4f e1 cb 97 c6 ae 98 19 6e
CN=Amazon Root CA 2,O=Amazon,C=US	06 6c 9f d2 96 35 86 9f 0a 0f e5 86 78 f8 5b 26 bb 8a 37	5a 8c ef 45 d7 a6 98 59 76 7a 8c 8b 44 96 b5 78 cf 47 4b 1a	1b a5 b2 aa 8c 65 40 1a 82 96 01 18 f8 0b ec 4f 62 30 4d 83 ce c4 71 3a 19 c3 9c 01 1e a4 6d b4
CN=Amazon Root CA 3,O=Amazon,C=US	06 6c 9f d5 74 97 36 66 3f 3b 0b 9a d9 e8 9e 76 03 f2 4a	0d 44 dd 8c 3c 8c 1a 1a 58 75 64 81 e9 0f 2e 2a ff b3 d2 6e	18 ce 6c fe 7b f1 4e 60 b2 e3 47 b8 df e8 68 cb 31 d0 2e bb 3a da 27 15 69 f5 03 43 b4 6d b3 a4
CN=Amazon Root CA 4,O=Amazon,C=US	06 6c 9f d7 c1 bb 10 4c 29 43 e5 71 7b 7b 2c c8 1a c1 0e	f6 10 84 07 d6 f8 bb 67 98 0c c2 e2 44 c2 eb ae 1c ef 63 be	e3 5d 28 41 9e d0 20 25 cf a6 90 38 cd 62 39 62 45 8d a5 c6 95 fb de a3 c2 2b 0b fb 25 89 70 92
CN=Starfield Services Root Certificate Authority - G2,O=Starfield Technologies, Inc.,L=Scottsdale,ST=Arizona,C=US	00	92 5a 8f 8d 2c 6d 04 e0 66 5f 59 6a ff 22 d8 63 e8 25 6f 3f	56 8d 69 05 a2 c8 87 08 a4 b3 02 51 90 ed cf ed b1 97 4a 60 6a 13 c6 e5 29 0f cb 2a e6 3e da b5

Other CAs	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
CN=Amazon,OU=Server CA 0A,O=Amazon,C=US	06 7f 94 57 4b b7 07 5d 3e 48 96 5c 78 32 24 aa 75 4f ed	fe 19 62 07 e8 36 b7 16 72 89 cd b1 f9 12 b5 07 c5 9c 3f c1	df cc 77 5c 64 4d b4 a3 3a d7 12 93 43 3f 46 3c 8e 31 05 7c e2 2c b2 67 f9 d3 1a 03 53 f4 fc 2f
CN=Amazon,OU=Server CA 1A,O=Amazon,C=US	06 7f 94 57 50 8c 64 8c 09 ca 65 2e 71 79 18 30 e7 25 92	10 18 8c 71 0f c3 2d 05 e0 75 8a 2f 5b 70 f8 ff a8 f0 f7 77	39 c7 63 a9 cf 19 d9 23 f9 77 d2 36 26 ab 89 04 49 a4 44 ab 8b 79 5c 81 5e f1 ef 81 fe bc 1e 38
CN=Amazon,OU=Server CA 2A,O=Amazon,C=US	06 7f 94 57 55 f1 87 a9 1f 81 63 f3 e6 24 62 01 77 ff 38	1c ec 96 ae 3d 32 91 42 53 df 97 5f 82 aa e8 3c 9e 8a a3 4d	72 13 0e 3b 28 90 03 49 21 46 17 f4 d6 f3 fb 85 d0 84 75 ee 78 bf 09 5c 59 45 8a 14 d1 82 88 66
CN=Amazon,OU=Server CA 3A,O=Amazon,C=US	06 7f 94 57 58 fe 55 b9 ee 3f 75 83 1d 47 f0 7d 22 6c 8a	46 54 d1 6b fb 1f 55 16 01 0b b1 e3 a2 54 45 fd 06 d7 9f 6d	20 51 54 b7 77 ed c5 5a 51 46 58 5a 5e 54 e0 54 a7 0b e4 aa d3 b8 5d 02 31 8d a2 7b f8 07 ad f1



CN=Amazon,OU=Server CA 4A,O=Amazon,C=US	06 7f 94 57 5a 88 62 a9 07 2e 32 39 c3 7c eb a1 27 4e 18	f0 e7 a2 72 b0 b8 1d dc 46 e1 bd b7 ca 01 a6 08 58 d2 ec 85	7b ed 29 27 6a cb ed 9f 17 6f 38 bb a3 a6 7c e5 81 5b 5c bf 15 22 c7 bb 59 ec d8 6b 09 e1 6e d2
---	---	---	---

Note: Amazon Trust Services assumed operation of Starfield Services Root Certificate Authority - G2 ("SFSG2") on June 10, 2015. Starfield Technologies operated SFSG2 prior to June 10, 2015 and was responsible for the key generation for SFSG2.



Amazon Trust Services, LLC Management's Assertion

Amazon Trust Services LLC, ("ATS") operates the Certification Authority ("CA") services for the CAs enumerated in [Attachment B](#), and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of ATS is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its [repository](#), CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to ATS' Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ATS management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ATS management's opinion, in providing its CA services in the United States of America, throughout the period January 16, 2018 to January 15, 2019, ATS has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certification Practice Statement and Certificate Policy enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
 - ATS' Certification Practice Statement is consistent with its Certificate Policy; and
 - ATS provides its services in accordance with its Certificate Policy and Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;

- the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
- subscriber information is properly authenticated; and
- subordinate CA certificate requests are accurate, authenticated, and approved
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities v2.1](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certification Practice Statement (CPS) Management
- Certificate Policy (CP) Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival

- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management
- CA Key Transportation
- CA Key Migration

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

ATS did not escrow CA keys, did not provide certificate suspension services, and did not provide subscriber key life cycle management services. Accordingly, our assertion does not extend to controls that would address those criteria.

ATS did not delegate subscriber information authentication to any third parties. ATS maintained controls over subscriber information authentication for all certificates issued.

Jonathan Kozolchyk

Jonathan Kozolchyk
Vice President
Amazon Trust Services LLC

April 8, 2019

ATTACHMENT A – IN-SCOPE CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY VERSIONS

Amazon Trust Services, LLC Certification Practice Statement and Certificate Policy Versions in Scope

Policy Name	Version	Date
Amazon Trust Services Certification Practice Statement	1.0.7	April 13, 2018
Amazon Trust Services Certification Practice Statement	1.0.6	January 15, 2018
Amazon Trust Services Certificate Policy	1.0.6	April 13, 2018
Amazon Trust Services Certificate Policy	1.0.5	January 15, 2018

ATTACHMENT B – IN-SCOPE CAs

Root CAs	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
CN=Amazon Root CA 1,O=Amazon,C=US	06 6c 9f cf 99 bf 8c 0a 39 e2 f0 78 8a 43 e6 96 36 5b ca	8d a7 f9 65 ec 5e fc 37 91 0f 1c 6e 59 fd c1 cc 6a 6e de 16	8e cd e6 88 4f 3d 87 b1 12 5b a3 1a c3 fc b1 3d 70 16 de 7f 57 cc 90 4f e1 cb 97 c6 ae 98 19 6e
CN=Amazon Root CA 2,O=Amazon,C=US	06 6c 9f d2 96 35 86 9f 0a 0f e5 86 78 f8 5b 26 bb 8a 37	5a 8c ef 45 d7 a6 98 59 76 7a 8c 8b 44 96 b5 78 cf 47 4b 1a	1b a5 b2 aa 8c 65 40 1a 82 96 01 18 f8 0b ec 4f 62 30 4d 83 ce c4 71 3a 19 c3 9c 01 1e a4 6d b4
CN=Amazon Root CA 3,O=Amazon,C=US	06 6c 9f d5 74 97 36 66 3f 3b 0b 9a d9 e8 9e 76 03 f2 4a	0d 44 dd 8c 3c 8c 1a 1a 58 75 64 81 e9 0f 2e 2a ff b3 d2 6e	18 ce 6c fe 7b f1 4e 60 b2 e3 47 b8 df e8 68 cb 31 d0 2e bb 3a da 27 15 69 f5 03 43 b4 6d b3 a4
CN=Amazon Root CA 4,O=Amazon,C=US	06 6c 9f d7 c1 bb 10 4c 29 43 e5 71 7b 7b 2c c8 1a c1 0e	f6 10 84 07 d6 f8 bb 67 98 0c c2 e2 44 c2 eb ae 1c ef 63 be	e3 5d 28 41 9e d0 20 25 cf a6 90 38 cd 62 39 62 45 8d a5 c6 95 fb de a3 c2 2b 0b fb 25 89 70 92
CN=Starfield Services Root Certificate Authority - G2,O=Starfield Technologies, Inc.,L=Scottsdale,ST=Arizona,C=US	00	92 5a 8f 8d 2c 6d 04 e0 66 5f 59 6a ff 22 d8 63 e8 25 6f 3f	56 8d 69 05 a2 c8 87 08 a4 b3 02 51 90 ed cf ed b1 97 4a 60 6a 13 c6 e5 29 0f cb 2a e6 3e da b5

Other CAs	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint
CN=Amazon,OU=Server CA 0A,O=Amazon,C=US	06 7f 94 57 4b b7 07 5d 3e 48 96 5c 78 32 24 aa 75 4f ed	fe 19 62 07 e8 36 b7 16 72 89 cd b1 f9 12 b5 07 c5 9c 3f c1	df cc 77 5c 64 4d b4 a3 3a d7 12 93 43 3f 46 3c 8e 31 05 7c e2 2c b2 67 f9 d3 1a 03 53 f4 fc 2f
CN=Amazon,OU=Server CA 1A,O=Amazon,C=US	06 7f 94 57 50 8c 64 8c 09 ca 65 2e 71 79 18 30 e7 25 92	10 18 8c 71 0f c3 2d 05 e0 75 8a 2f 5b 70 f8 ff a8 f0 f7 77	39 c7 63 a9 cf 19 d9 23 f9 77 d2 36 26 ab 89 04 49 a4 44 ab 8b 79 5c 81 5e f1 ef 81 fe bc 1e 38
CN=Amazon,OU=Server CA 2A,O=Amazon,C=US	06 7f 94 57 55 f1 87 a9 1f 81 63 f3 e6 24 62 01 77 ff 38	1c ec 96 ae 3d 32 91 42 53 df 97 5f 82 aa e8 3c 9e 8a a3 4d	72 13 0e 3b 28 90 03 49 21 46 17 f4 d6 f3 fb 85 d0 84 75 ee 78 bf 09 5c 59 45 8a 14 d1 82 88 66
CN=Amazon,OU=Server CA 3A,O=Amazon,C=US	06 7f 94 57 58 fe 55 b9 ee 3f 75 83 1d 47 f0 7d 22 6c 8a	46 54 d1 6b fb 1f 55 16 01 0b b1 e3 a2 54 45 fd 06 d7 9f 6d	20 51 54 b7 77 ed c5 5a 51 46 58 5a 5e 54 e0 54 a7 0b e4 aa d3 b8 5d 02 31 8d a2 7b f8 07 ad f1

CN=Amazon,OU=Server CA 4A,O=Amazon,C=US	06 7f 94 57 5a 88 62 a9 07 2e 32 39 c3 7c eb a1 27 4e 18	f0 e7 a2 72 b0 b8 1d dc 46 e1 bd b7 ca 01 a6 08 58 d2 ec 85	7b ed 29 27 6a cb ed 9f 17 6f 38 bb a3 a6 7c e5 81 5b 5c bf 15 22 c7 bb 59 ec d8 6b 09 e1 6e d2
---	---	--	---

Note: Amazon Trust Services assumed operation of Starfield Services Root Certificate Authority - G2 ("SFSG2") on June 10, 2015. Starfield Technologies operated SFSG2 prior to June 10, 2015 and was responsible for the key generation for SFSG2.