



## 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 various location in the United States of America, throughout the period January 16, 2019 to January 15, 2020 for its CAs enumerated in [Attachment B](#) in scope for SSL Baseline Requirements and Network Security Requirements, ATS has:

- disclosed its SSL certificate lifecycle management business practices in the applicable versions of its Certification Practice Statement and Certificate Policy enumerated in [Attachment A](#), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ATS [repository](#), 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
- 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 v2.3](#). 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.

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.

Without modifying our opinion, we noted the following other matters during our procedures:

Matter Topic		Matter Description
1	Certificate Content	ATS disclosed in <a href="#">Mozilla Bug 1525710</a> five (5) certificates were issued with a validity period set for 39 months, which exceeds the 825 day limit in the Baseline Requirements. Additionally, the issued certificates contained Subject Distinguished Name (“Subject DN”) attributes that were explicitly not allowed based on the policy identifier included in the certificate.
		ATS disclosed in <a href="#">Mozilla Bug 1574594</a> three (3) certificates were issued without a Subject Alternative Name field present.
2	Certificate Content and Revocation	ATS disclosed in <a href="#">Mozilla Bug 1569266</a> five (5) certificates were issued with no space between “Private” and “Organization” in the Subject DN. Additionally, the time period between completion of investigation and revocation of the mis-issued certificates exceeded the five (5) day timeframe permitted by the Baseline Requirements.
3	Human Log Review	Log content and integrity was reviewed when offline systems were accessed. Human reviews of application and system logs to validate the retention and integrity of offline logs were not being performed on a monthly basis during the examination period.

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



The World Health Organization classified the COVID-19 outbreak as a pandemic in March 2020. Based on the rapid increase in exposure globally, the gravity or length of the impact of the COVID-19 outbreak cannot be determined at this time.

ATS' use of the WebTrust for Certification Authorities - SSL Baseline with Network Security 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.

*BDO USA, LLP*

April 8, 2020



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

<b>Policy Name</b>	<b>Version</b>	<b>Effective Date</b>
<a href="#">Amazon Trust Services Certification Practice Statement</a>	1.0.8	December 17, 2019
Amazon Trust Services Certification Practice Statement	1.0.7	April 13, 2018
<a href="#">Amazon Trust Services Certificate Policy</a>	1.0.7	December 18, 2019
Amazon Trust Services Certificate Policy	1.0.6	April 13, 2018



## ATTACHMENT B - IN-SCOPE CAs

Root CA Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN = Amazon Root CA 1 O = Amazon C = US	8ECDE6884F3D87B1125BA31AC3FCB13D7016DE7F57CC904FE1CB97C6AE98196E	FBE3018031F9586BCBF417 27E417B7D1C45C2F47F93B E372A17B96B50757D5A2	5/25/2015	1/16/2038
CN = Amazon Root CA 2 O = Amazon C = US	1BA5B2AA8C65401A82960118F80BEC4F62304D83CEC4713A19C39C011EA46DB4	7F4296FC5B6A4E3B35D3C3 69623E364AB1AF381D8FA7 121533C9D6C633EA2461	5/25/2015	5/25/2040
CN = Amazon Root CA 3 O = Amazon C = US	18CE6CFE7BF14E60B2E347B8DFE868CB31D02EBB3ADA271569F50343B46DB3A4	36ABC32656ACFC645C61B7 1613C4BF21C787F5CABBEE 48348D58597803D7ABC9	5/25/2015	5/25/2040
CN = Amazon Root CA 4 O = Amazon C = US	E35D28419ED02025CFA69038CD623962458DA5C695FBDEA3C22B0BFB25897092	F7ECDE5C66047D28ED64 66B543C40E0743ABE81D10 9254DCF845D4C2C7853C5	5/25/2015	5/25/2040
CN = Starfield Services Root Certificate Authority - G2 <sup>1</sup> O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US	568D6905A2C88708A4B3025190EDCFEDB1974A606A13C6E5290FCB2AE63EDAB5	2B071C59A0A0AE76B0EAD B2BAD23BAD4580B69C360 1B630C2EAF0613AFA83F92	8/31/2009	12/31/2037

Cross-Signed Root CA Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN = Amazon Root CA 1 O = Amazon C = US	87DCD4DC74640A322CD205552506D1BE64F12596258096544986B4850BC72706	FBE3018031F9586BCBF417 27E417B7D1C45C2F47F93B E372A17B96B50757D5A2	5/25/2015	12/31/2037
	391220705B75BCF3ED3CD4B3631213F569D2CF8226101E170799A5354AB12861		10/21/2015	12/31/2037
CN = Amazon Root CA 2 O = Amazon C = US	8B358466D66126312120645A5875A6A57E3C81D98476A967604244254EAC00F0	7F4296FC5B6A4E3B35D3C3 69623E364AB1AF381D8FA7 121533C9D6C633EA2461	5/25/2015	12/31/2037

<sup>1</sup> ATS assumed operation of this Root CA on June 10, 2015. Starfield Technologies operated this CA prior to June 10, 2015 and was responsible for its key generation.



Cross-Signed Root CA Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN = Amazon Root CA 3 O = Amazon C = US	40C826FDB22BA32A2F9DB4F94770F72B8B1DA9C8FFDA7B11E6F27AF245C89B5E	36ABC32656ACFC645C61B7 1613C4BF21C787F5CABBEE 48348D58597803D7ABC9	5/25/2015	12/31/2037
CN = Amazon Root CA 4 O = Amazon C = US	543D9B7FC2A6471CD84FCA52C2CF6159DF83EBFCD88D8B08B5AF3F88737F52E6	F7ECDE5C66047D28ED64 66B543C40E0743ABE81D10 9254DCF845D4C2C7853C5	5/25/2015	12/31/2037

Intermediate CA Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN = Amazon OU = Server CA 0A O = Amazon C = US	DFCC775C644DB4A33AD71293433F463C8E31057CE22CB267F9D31A0353F4FC2F	B58539ECAA13921CCDB80 D38D34875FDE6471C5A159 D9BEEF2FA6F99983BD611	10/21/2015	10/18/2025
CN = Amazon OU = Server CA 1A O = Amazon C = US	39C763A9CF19D923F977D23626AB890449A444AB8B795C815EF1EF81FEBCE1E38	64BB5BD80311FA3F53BD99 404CAB8762AD6E048447D0 A97F219FCECA1661F37C	10/21/2015	10/18/2025
CN = Amazon OU = Server CA 2A O = Amazon C = US	72130E3B28900349214617F4D6F3FB85D08475EE78BF095C59458A14D1828866	1BDA5AFF83781380BF708 198F9F7D2DB1E067F14BB9 EA7BAE70AAC0B0305E7B	10/21/2015	10/18/2025
CN = Amazon OU = Server CA 3A O = Amazon C = US	205154B777EDC55A5146585A5E54E054A70BE4AAD3B85D02318DA27BF807ADF1	7C53B5DF79135D9AF6195E F6BB73AB98C2C89950B892 B192DFFD784DB925A41C	10/21/2015	10/18/2025
CN = Amazon OU = Server CA 4A O = Amazon C = US	7BED29276ACBED9F176F38BBA3A67CE5815B5CBF1522C7BB59ECD86B09E16ED2	17708DFF2B7FAEC9CB1B52 15EBB2421D97B0543C936F AC9D6E02B92F20E5C707	10/21/2015	10/18/2025



## 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](#) in scope for SSL Baseline Requirements and Network Security Requirements and provides SSL CA services.

ATS management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL CA services in the United States of America, throughout the period January 16, 2019 to January 15, 2020, ATS has:

- disclosed its SSL certificate lifecycle management business practices in the applicable versions of its Certificate Practice Statement and Certificate Policy enumerated in [Attachment A](#) including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ATS [repository](#), 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
- 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 v2.3](#).

*Jonathan Kozolchyk*

---

Jonathan Kozolchyk  
Vice President  
Amazon Trust Services, LLC

April 8, 2020

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

<b>Policy Name</b>	<b>Version</b>	<b>Effective Date</b>
<a href="#">Amazon Trust Services Certification Practice Statement</a>	1.0.8	December 17, 2019
Amazon Trust Services Certification Practice Statement	1.0.7	April 13, 2018
<a href="#">Amazon Trust Services Certificate Policy</a>	1.0.7	December 18, 2019
Amazon Trust Services Certificate Policy	1.0.6	April 13, 2018



## ATTACHMENT B - IN-SCOPE CAs

Root CA Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN = Amazon Root CA 1 O = Amazon C = US	8ECDE6884F3D87B1125BA31AC3FCB13D7016DE7F57CC904FE1CB97C6AE98196E	FBE3018031F9586BCBF417 27E417B7D1C45C2F47F93B E372A17B96B50757D5A2	5/25/2015	1/16/2038
CN = Amazon Root CA 2 O = Amazon C = US	1BA5B2AA8C65401A82960118F80BEC4F62304D83CEC4713A19C39C011EA46DB4	7F4296FC5B6A4E3B35D3C3 69623E364AB1AF381D8FA7 121533C9D6C633EA2461	5/25/2015	5/25/2040
CN = Amazon Root CA 3 O = Amazon C = US	18CE6CFE7BF14E60B2E347B8DFE868CB31D02EBB3ADA271569F50343B46DB3A4	36ABC32656ACFC645C61B7 1613C4BF21C787F5CABBEE 48348D58597803D7ABC9	5/25/2015	5/25/2040
CN = Amazon Root CA 4 O = Amazon C = US	E35D28419ED02025CFA69038CD623962458DA5C695FBDEA3C22B0BFB25897092	F7ECDED5C66047D28ED64 66B543C40E0743ABE81D10 9254DCF845D4C2C7853C5	5/25/2015	5/25/2040
CN = Starfield Services Root Certificate Authority - G2 <sup>1</sup> O = Starfield Technologies, Inc. L = Scottsdale S = Arizona C = US	568D6905A2C88708A4B3025190EDCFEDB1974A606A13C6E5290FCB2AE63EDAB5	2B071C59A0A0AE76B0EAD B2BAD23BAD4580B69C360 1B630C2EAF0613AFA83F92	8/31/2009	12/31/2037

Cross-Signed Root CA Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN = Amazon Root CA 1 O = Amazon C = US	87DCD4DC74640A322CD205552506D1BE64F12596258096544986B4850BC72706	FBE3018031F9586BCBF417 27E417B7D1C45C2F47F93B E372A17B96B50757D5A2	5/25/2015	12/31/2037
	391220705B75BCF3ED3CD4B3631213F569D2CF8226101E170799A5354AB12861		10/21/2015	12/31/2037
CN = Amazon Root CA 2 O = Amazon C = US	8B358466D66126312120645A5875A6A57E3C81D98476A967604244254EAC00F0	7F4296FC5B6A4E3B35D3C3 69623E364AB1AF381D8FA7 121533C9D6C633EA2461	5/25/2015	12/31/2037
CN = Amazon Root CA 3 O = Amazon C = US	40C826FDB22BA32A2F9DB4F94770F72B8B1DA9C8FFDA7B11E6F27AF245C89B5E	36ABC32656ACFC645C61B7 1613C4BF21C787F5CABBEE 48348D58597803D7ABC9	5/25/2015	12/31/2037

<sup>1</sup> ATS assumed operation of this Root CA on June 10, 2015. Starfield Technologies operated this CA prior to June 10, 2015 and was responsible for its key generation.

Cross-Signed Root CA Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN = Amazon Root CA 4 O = Amazon C = US	543D9B7FC2A6471CD84FCA52C2CF6159DF83EBFCD88D8B08B5AF3F88737F52E6	F7ECDEED5C66047D28ED64 66B543C40E0743ABE81D10 9254DCF845D4C2C7853C5	5/25/2015	12/31/2037

Intermediate CA Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN = Amazon OU = Server CA 0A O = Amazon C = US	DFCC775C644DB4A33AD71293433F463C8E31057CE22CB267F9D31A0353F4FC2F	B58539ECAA13921CCDB80 D38D34875FDE6471C5A159 D9BEEF2FA6F99983BD611	10/21/2015	10/18/2025
CN = Amazon OU = Server CA 1A O = Amazon C = US	39C763A9CF19D923F977D23626AB890449A444AB8B795C815EF1EF81FEBC1E38	64BB5BD80311FA3F53BD99 404CAB8762AD6E048447D0 A97F219FCECA1661F37C	10/21/2015	10/18/2025
CN = Amazon OU = Server CA 2A O = Amazon C = US	72130E3B28900349214617F4D6F3FB85D08475EE78BF095C59458A14D1828866	1BDA5AFF83781380BF708 198F9F7D2DB1E067F14BB9 EA7BAE70AAC0B0305E7B	10/21/2015	10/18/2025
CN = Amazon OU = Server CA 3A O = Amazon C = US	205154B777EDC55A5146585A5E54E054A70BE4AAD3B85D02318DA27BF807ADF1	7C53B5DF79135D9AF6195E F6BB73AB98C2C89950B892 B192DFFD784DB925A41C	10/21/2015	10/18/2025
CN = Amazon OU = Server CA 4A O = Amazon C = US	7BED29276ACBED9F176F38BBA3A67CE5815B5CBF1522C7BB59ECD86B09E16ED2	17708DFF2B7FAEC9CB1B52 15EBB2421D97B0543C936F AC9D6E02B92F20E5C707	10/21/2015	10/18/2025