



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, 2016 to January 15, 2017 for its root CAs known as Amazon Root CA 1, Amazon Root CA 2, Amazon Root CA 3, Amazon Root CA 4, Starfield Services Root Certificate Authority - G2 and other CAs listed in [Appendix A](#), ATS has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
 - [Amazon Trust Services Certificate Policy v1.0.4](#); and
 - [Amazon Trust Services Certification Practice Statement v1.0.5](#)
- 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 [Trust Service Principles and Criteria for Certification Authorities, Version 2.0](#).

ATS’ management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

We conducted our examination in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

- (1) obtaining an understanding of ATS’ key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;



- (2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
- (3) testing and evaluating the operating effectiveness of the controls; and
- (4) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

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. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

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, throughout the period January 16, 2016 to January 15, 2017, ATS management's assertion, as referred to above, is fairly stated, in all material respects, based on the Trust Service Principles and Criteria for Certification Authorities, Version 2.0.

This report does not include any representation as to the quality of ATS' services beyond those covered by the Trust Service Principles and Criteria for Certification Authorities, Version 2.0, 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.

BDO USA, LLP

Certified Public Accountants
St. Louis, Missouri
March 28, 2017



Amazon Trust Services LLC Management's Assertion

March 28, 2017

Amazon Trust Services LLC ("ATS") operates Certification Authorities ("CAs") known as Amazon Root CA 1, Amazon Root CA 2, Amazon Root CA 3, Amazon Root CA4, Starfield Services Root Certificate Authority - G2 and other CAs as listed in [Appendix A](#), and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA certification

The management of ATS is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its [website](#), 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, 2016 to January 15, 2017, ATS has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
 - [Amazon Trust Services Certificate Policy v1.0.4](#); and
 - [Amazon Trust Services Certification Practice Statement v1.0.5](#)
- 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 [Trust Service Principles and Criteria for Certification Authorities, Version 2.0](#), including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement 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 and Maintenance
- 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 and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Escrow

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

ATS did not escrow CA keys, nor did ATS provide Integrated Circuit Card Life Cycle Management or Certificate Suspension services. ATS only provided Subscriber Key Generation and Subscriber Key Storage and Recovery services when the subscriber was ATS or an affiliate of ATS.

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

APPENDIX A – IN-SCOPE CAs

Root CAs	SHA-256 Hash of Subject Public Key Information
CN=Amazon Root CA 1, O=Amazon, C=US	fbe3018031f9586bcbf41727e417b7d1c45c2f47f93be372a17b96b50757d5a2
CN=Amazon Root CA 2, O=Amazon, C=US	7f4296fc5b6a4e3b35d3c369623e364a b1af381d8fa7121533c9d6c633ea2461
CN=Amazon Root CA 3, O=Amazon, C=US	36abc32656acf645c61b71613c4bf21c787f5cabbec48348d58597803d7abc9
CN=Amazon Root CA 4, O=Amazon, C=US	f7ecded5c66047d28ed6466b543c40e0743abe81d109254dcf845d4c2c7853c5
CN=Starfield Services Root Certificate Authority - G2, O=Starfield Technologies, Inc., L=Scottsdale, ST=Arizona, C=US	2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92

Other CAs	SHA-256 Hash of Subject Public Key Information
CN=Amazon, OU=Server CA 0A, O=Amazon, C=US	b58539ecea13921ccdb80d38d34875fd e6471c5a159d9bee2fa6f99983bd611
CN=Amazon, OU=Server CA 1A, O=Amazon, C=US	64bb5bd80311fa3f53bd99404cab8762 ad6e048447d0a97f219fcec1661f37c
CN=Amazon, OU=Server CA 2A, O=Amazon, C=US	1bda5affff83781380bf708198f9f7d2d b1e067f14bb9ea7bae70aac0b0305e7b
CN=Amazon, OU=Server CA 3A, O=Amazon, C=US	7c53b5dff79135d9af6195ef6bb73ab98 c2c89950b892b192dff784db925a41c
CN=Amazon, OU=Server CA 4A, O=Amazon, C=US	17708dff2b7faec9cb1b5215ebb2421d 97b0543c936fac9d6e02b92f220e5c707

Notes: Amazon Trust Services assumed operation of Starfield Services Root Certificate Authority - G2 (SFG2) on June 10, 2015. Starfield Technologies operated SFG2 prior to June 10, 2015 and was responsible for the key generation for SFG2.