



## REPORT OF THE INDEPENDENT ACCOUNTANT

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

### Scope

We have examined ATS management’s [assertion](#) that for its Certification Authority (“CA”) operations in Dublin, Ireland, and Washington, Oregon and Virginia, in the United States of America, for its CAs as 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 Amazon Trust Services Certification Practice Statement (“CPS”) and Amazon Trust Services Certificate Policy (“CP”) enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
  - ATS’ CPS is consistent with its CP; and
  - ATS provides its services in accordance with its CP and CPS
- 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

throughout the period January 16, 2024 to January 15, 2025, based on the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

ATS does not escrow CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, integrated circuit card lifecycle management services, and certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.



## **Certification Authority's Responsibilities**

ATS' management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

## **Independent Accountant's Responsibilities**

Our responsibility is to express an opinion on management's assertion based on our examination. 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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.

## **Inherent limitations**

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

## **Independent Accountant's Opinion**

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 Dublin, Ireland, and Washington, Oregon and Virginia, in the United States of America, nor the suitability of any of ATS' services for any customer's intended purpose.



## Other Matter

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

Matter Topic		Matter Description
1	Certificate Revocation List (CRL) Encoding	Amazon Trust Services disclosed in Mozilla Bug <a href="#">#1914893</a> that one (1) Subordinate CA status CRL was not DER encoded, as required by RFC 5280.

While the ATS assertion notes all issues disclosed on Bugzilla from January 16, 2024 through the date of this report, we have only noted those instances relevant to the CAs enumerated in [Attachment B](#) and applicable to the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

## Use of the WebTrust Seal

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

April 10, 2025



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

Policy Name	Version	Effective Date
<a href="#">Amazon Trust Services Certificate Policy</a>	1.0.14	July 24, 2024
Amazon Trust Services Certificate Policy	1.0.13	July 28, 2023
<a href="#">Amazon Trust Services Certification Practices Statement</a>	1.0.15	July 24, 2024
Amazon Trust Services Certification Practices Statement	1.0.14	July 28, 2023



## ATTACHMENT B - IN-SCOPE CAs

Root CA Certificates				
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
CN = Amazon RSA 2048 Root EU M1 O = Amazon C = DE	EAFAC50C7E3E15A68F779A5E70EC2F5E9FC4A03FF69AB337B4D6C4510432395	8D935558E6A3C896330148 FFDF6A1AC0A5BFBA1AB44 545135A3B376C9A1A308D	11/14/2024	11/14/2042
CN = Amazon ECDSA 256 Root EU M1 O = Amazon C = DE	9EAD32C9285FE68BA2C5B0FE427D149B103FDFA1D0958D77C3DA0FF246E853D3	9565907725464BE0BFF44B 1232F85EE862A9A0D99DB9 71BA20344AAF41431D58	11/14/2024	11/14/2042
CN = Amazon ECDSA 384 Root EU M1 O = Amazon C = DE	8E136CE0E77C848F2D2910ABD4E3A764358BB1B7A4932202BC9B915732462D85	798FE10957E8C5A0874201 CAF09D5EF4B2E2412C47BF 991949566CB542D3AF3F	11/14/2024	11/14/2042

<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 CA Certificates				
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
CN = Amazon Root CA 4 O = Amazon C = US	543D9B7FC2A6471CD84FCA52C2CF6159DF83EBFCD88D8B08B5AF3F88737F52E6	F7ECDEDE5C66047D28ED64 66B543C40E0743ABE81D10 9254DCF845D4C2C7853C5	5/25/2015	12/31/2037

Intermediate CA Certificates				
Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN=Amazon RSA 2048 M05 O=Amazon C=US	F1D0D91BD33F9C0600B394481847FCD3069D4532FE55EFC06A12E5259DD4CE2A	3DD9C9093547E6322BB3BD ABFE67D5A929A6FDE215FE 7AE5C528A4797663BC8F	1/13/2025	1/15/2033
CN=Amazon RSA 2048 M06 O=Amazon C=US	64F0C9594F65BD69FCF82E35879827F3AEB36B9F9977726A9A9F33CB61EE7BBB	1822A8DD53E117B25D340A 18602BC2D4E6B8BB0227CE DA9933BA15DCDAB889B2	1/13/2025	1/15/2033
CN=Amazon RSA 4096 M05 O=Amazon C=US	8714CD260F39B865E4B0ADF16ECBAA748AB0ABE494980E80E196A6DB1B170B5B	69262417C64D056E5EF539 5F7BC65BD7C6D7C3122F5F 1F40E7A6CAF9980ECE8D	1/13/2025	1/15/2033
CN=Amazon ECDSA 256 M05 O=Amazon C=US	36A77659CA91702BC800B527D12A6B4FD0237D506EDBE4670FD3A56CD0AE4243	39F2551D1B91B392031FEB 7822E9587093E76640B46C F2CC546E8ACC96D62CBA	1/13/2025	1/15/2033



Intermediate CA Certificates				
Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN=Amazon ECDSA 256 M06 O=Amazon C=US	4FF1CF3F6920EEC8D5078ABBA246F198588987DC543B73CD12ABC781125CA0FE	26DC4A8860CAE0ED7D4D7 3C32B6D834AC3A74A9C13 FBBBFCB690EB59168B9429	1/13/2025	1/15/2033
CN=Amazon ECDSA 384 M05 O=Amazon C=US	36FDD1CDE845411BACF3C09E1CA09546DDC5DEA40332DE411AE56EEA349BAEBE	D4355548E497AB4C247A09 75FC6F6A22CC65C88D5346 7D0A000FA5BFC95F3B2D	1/13/2025	1/15/2033
CN=Amazon ECDSA 384 M06 O=Amazon C=US	4F2D3225BA9E26817DFA325A4FB3397FDE34DE62C41D846CE05D815A10276C3B	85DE0208B443F9F869ECA5 8C48FE7E45F1D5494FEC6B 7EE369C7736DD5B04BEB	1/13/2025	1/15/2033



## 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 and cross-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, 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' CA 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 Dublin, Ireland, and Washington, Oregon and Virginia, in the United States of America, ATS has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Amazon Trust Services Certification Practice Statement ("CPS") and Amazon Trust Services Certificate Policy ("CP") enumerated in [Attachment A](#)
- maintained effective controls to provide reasonable assurance that:
  - ATS' CPS is consistent with its CP; and
  - ATS provides its services in accordance with its CP and CPS
- 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

throughout the period January 16, 2024 to January 15, 2025, based on the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), 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 and 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

#### **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 and Cross Certificate Lifecycle Management Controls**

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

ATS does not escrow CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, integrated circuit card lifecycle management services, and certificate suspension 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.

ATS has disclosed the following matters publicly on Mozilla’s Bugzilla platform. These matters were included below due to being open during the period January 16, 2024, through the date of this report:

Bug ID	Summary	Opened	Closed	Resolution
<a href="#">#1914893</a>	Amazon Trust Services: CRL not DER-encoded	8/26/2024	9/18/2024	Fixed

*Jay Kistler*

---

Jay Kistler  
Vice President  
Amazon Trust Services, LLC

April 10, 2025

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

Policy Name	Version	Effective Date
<a href="#">Amazon Trust Services Certificate Policy</a>	1.0.14	July 24, 2024
Amazon Trust Services Certificate Policy	1.0.13	July 28, 2023
<a href="#">Amazon Trust Services Certification Practices Statement</a>	1.0.15	July 24, 2024
Amazon Trust Services Certification Practices Statement	1.0.14	July 28, 2023

## ATTACHMENT B - IN-SCOPE CAs

Root CA Certificates				
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	E35D28419ED02025CFA69038CD623962458DA5C695FBDEA3C22B0BF825897092	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
CN = Amazon RSA 2048 Root EU M1 O = Amazon C = DE	EAFFAC50C7E3E15A68F779A5E70EC2F5E9FC4A03FF69AB337B4D6C4510432395	8D935558E6A3C896330148 FFDF6A1AC0A5BFBA1AB44 545135A3B376C9A1A308D	11/14/2024	11/14/2042
CN = Amazon ECDSA 256 Root EU M1 O = Amazon C = DE	9EAD32C9285FE68BA2C5B0FE427D149B103FDA1D0958D77C3DA0FF246E853D3	9565907725464BE0BFF44B 1232F85EE862A9A0D99DB9 71BA20344AAF41431D58	11/14/2024	11/14/2042
CN = Amazon ECDSA 384 Root EU M1 O = Amazon C = DE	8E136CE0E77C848F2D2910ABD4E3A764358BB1B7A4932202BC9B915732462D85	798FE10957E8C5A0874201 CAF09D5EF4B2E2412C47BF 991949566CB542D3AF3F	11/14/2024	11/14/2042

<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 CA Certificates				
Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN = Amazon Root CA 1 O = Amazon C = US	87DCD4DC74640A322CD20552506D1BE64F12596258096544986B4850BC72706	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
CN = Amazon Root CA 4 O = Amazon C = US	543D9B7FC2A6471CD84FCA52C2CF6159DF83EBFCD88D8B08B5AF3F88737F52E6	F7ECDED5C66047D28ED64 66B543C40E0743ABE81D10 9254DCF845D4C2C7853C5	5/25/2015	12/31/2037

Intermediate CA Certificates				
Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN=Amazon RSA 2048 M05 O=Amazon C=US	F1D0D91BD33F9C0600B394481847FCD3069D4532FE55EFC06A12E5259DD4CE2A	3DD9C9093547E6322BB3BD ABFE67D5A929A6FDE215FE 7AE5C528A4797663BC8F	1/13/2025	1/15/2033
CN=Amazon RSA 2048 M06 O=Amazon C=US	64F0C9594F65BD69FCF82E35879827F3AEB36B9F9977726A9A9F33CB61EE7BBB	1822A8DD53E117B25D340A 18602BC2D4E6B88B0227CE DA9933BA15DCDAB889B2	1/13/2025	1/15/2033
CN=Amazon RSA 4096 M05 O=Amazon C=US	8714CD260F39B865E4B0ADF16ECBAA748AB0ABE494980E80E196A6DB1B170B5B	69262417C64D056E5EF539 5F7BC65BD7C6D7C3122F5F 1F40E7A6CAF9980ECE8D	1/13/2025	1/15/2033
CN=Amazon ECDSA 256 M05 O=Amazon C=US	36A77659CA91702BC800B527D12A6B4FD0237D506EDBE4670FD3A56CD0AE4243	39F2551D1B91B392031FEB 7822E9587093E76640B46C F2CC546E8ACC96D62CBA	1/13/2025	1/15/2033
CN=Amazon ECDSA 256 M06 O=Amazon C=US	4FF1CF3F6920EEC8D5078ABBA246F198588987DC543B73CD12ABC781125CA0FE	26DC4A8860CAE0ED7D4D7 3C32B6D834AC3A74A9C13 FBBBFCB690EB59168B9429	1/13/2025	1/15/2033

Intermediate CA Certificates				
Subject DN	SHA2 Thumbprint	SPKI SHA256	Valid From	Valid To
CN=Amazon ECDSA 384 M05 O=Amazon C=US	36FDD1CDE845411BACF3C09E1CA09546DDC5DEA40332DE411AE56EEA349BAEBE	D4355548E497AB4C247A09 75FC6F6A22CC65C88D5346 7D0A000FA5BFC95F3B2D	1/13/2025	1/15/2033
CN=Amazon ECDSA 384 M06 O=Amazon C=US	4F2D3225BA9E26817DFA325A4FB3397FDE34DE62C41D846CE05D815A10276C3B	85DE0208B443F9F869ECA5 8C48FE7E45F1D5494FEC6B 7EE369C7736DD5B04BEB	1/13/2025	1/15/2033