

WebTrust[®] for Certification Authorities

ILLUSTRATIVE REPORTS – ISAE 3000

Release Date 1 May 2023

Version 3.0

Document History

Version	Publication Date	Revision Summary
1.0	1 September 2017	Initial publication
2.0	1 February 2022	Updated to reflect wording changes in reporting 2018-2021, new code-signing reporting, new verified mark certificate reporting and additional reports not included in 2017 package.
3.0	1 May 2023	<p>Updated to reflect</p> <ul style="list-style-type: none"> • new Network Security reports • new S/MIME certificate reporting • changes to reporting for Code Signing reports to incorporate Principle 4 • Baseline reporting, Code Signing reporting and Verified Mark Certificate reporting once new Network Security reports are issued separately • potential use of “statement” in place of “assertion” • Changes in quality control reporting in reports effective for engagements beginning on or after December 14, 2022 • other minor corrections where applicable

Acknowledgements

This document has been prepared by the WebTrust/PKI Assurance Task Force (the “Task Force”) for use by those practitioners enrolled by CPA Canada to perform WebTrust for Certification Authorities engagements.

Members of the Task Force are:

- Timothy Crawford, *BDO USA, LLP* (co-Chair)
- Dan Adam
- Donoghue Clarke, *Ernst & Young LLP*
- Chris Czajczyc, *Deloitte LLP*
- Adam Fiock, *BDO USA, LLP*
- Eric Lin, *Ernst & Young LLP*
- Zain Shabbir, *KPMG LLP*
- Donald E. Sheehy

CPA Canada Support

- Anna-Marie Christian, Director Emerging Issues & Strategic Partnerships
- Dave Chin, Principal, WebTrust (co-Chair)
- Lilia Dubko, Manager, Assurance Programs

The Task Force would like to thank retiring long-term task force members Jeffrey Ward, *BDO USA, LLP* who also chaired the Task Force since 2016, and David Roque, *Ernst & Young LLP* for their significant contributions to the advancement of the WebTrust program during their membership on the Task Force.

Table of Contents

Document History	ii
Acknowledgements	iii
Reporting Guidance	1
Professional Standards	1
Reporting on Code-Signing Engagements	1
Reporting On Network Security Requirements	2
Public Disclosure of CA Business Practices	2
CA Facilities	2
List of Root and Subordinate CAs in Scope	3
Disclosure of Changes in Scope or Roots with no Activity	3
Reference to Applicable WebTrust Principles and Criteria	3
Date Formats	4
Reporting on Subscriber Registration Activities	4
Where external RAs are used	4
Reporting When Certain Criteria Not Applicable as Services Not Performed by CA	4
Qualified Assurance Reports	5
WebTrust for Certification Authorities	7
International Standards – ISAE 3000	7
Example IN1.1 – Unqualified opinion, attestation engagement, period of time	7
Example IN1.2 – Unqualified opinion, attestation engagement, point in time	11
Example IN1.3 – Unqualified opinion, direct engagement, period of time	15
Example IN1.4 – Qualified opinion on physical security and business continuity, attestation engagement, period of time – Assertion not modified by management	20
Example IN1.5 – Qualified opinion on physical security and business continuity, direct engagement, period of time	25
Example IN1.6 – Qualified opinion on physical security and business continuity, attestation engagement, period of time – Modified management assertion – Table presentation	31
Sample Appendix A	37
List of CAs in Scope	37
Sample CA Identifying Information for in Scope CAs	38
Management’s Assertion	39

Example MA1.1 – Management’s assertion, period of time	39
Example MA1.2 – Management’s assertion, point in time	43
Example MA1.3 – Management’s modified assertion, period of time – Accompanying qualified report	47
WebTrust for Certification Authorities – SSL Baseline with Network Security	52
Specific Reporting Guidance for SSL Baseline with Network Security	52
International Standards – ISAE 3000	54
Example IN2.1 – Unqualified opinion, attestation engagement, period of time	54
Example IN2.2 – Unqualified opinion, attestation engagement, point in time	58
Example IN2.3 – Unqualified opinion, direct engagement, period of time	62
Management’s Assertion	67
Example MA2.1 – Management’s assertion, period of time	67
Example MA2.2 – Management’s assertion, point in time	69
WebTrust for Certification Authorities – Extended Validation – SSL (“EV SSL”)	71
International Standards – ISAE 3000	71
Example IN3.1 – Unqualified opinion, attestation engagement, period of time	71
Example IN3.2 – Unqualified opinion, attestation engagement, point in time	75
Example IN3.3 – Unqualified opinion, direct engagement, period of time	78
Management’s Assertion	82
Example MA3.1 – Management’s assertion, period of time	82
Example MA3.2 – Management’s assertion, point in time	84
WebTrust for Certification Authorities – Code Signing (“CS”)	86
International Standards – ISAE 3000	86
Example CA4.1 – Unqualified opinion, attestation engagement, period of time	86
Example CA4.2 – Unqualified opinion, attestation engagement, point in time	90
Example CA4.3 – Unqualified opinion, direct engagement, period of time	94
Management’s Assertion	99
Example MA4.1 – Management’s assertion, period of time	99
Example MA4.1 – Management’s assertion, point in time	101
WebTrust for Certification Authorities – Network Security (“NS”)	103
International Standards – ISAE 3000	103

Example IN5.1 – Unqualified opinion, attestation engagement, period of time	103
Example IN5.2 – Unqualified opinion, attestation engagement, point in time	106
Example IN5.3 – Unqualified opinion, direct engagement, period of time	109
Management’s Assertion	112
Example MA5.1 – Management’s assertion, period of time	112
Example MA2.2 – Management’s assertion, point in time	113
WebTrust for Certification Authorities – S/MIME Certificates (“S/MIME”)	114
International Standards – ISAE 3000	114
Example IN6.1 – Unqualified opinion, attestation engagement, period of time	114
Example IN6.2 – Unqualified opinion, attestation engagement, point in time	118
Example IN6.3 – Unqualified opinion, direct engagement, period of time	122
Management’s Assertion	126
Example MA6.1 – Management’s assertion, period of time	126
Example MA6.2 – Management’s assertion, point in time	128
Lifecycle Reports	130
International Standards – ISAE 3000	131
Example IN7.1 – Root key generation ceremony, attestation engagement	131
Management’s Assertion	134
Example MA7.1 – Management’s assertion	134
Reporting on Life Cycle	136
International Standards – ISAE 3000	136
Example CA7.2 – Unqualified opinion, attestation engagement (for various lifecycle events), period of time	136
Management’s Assertion	142
Example MA7.2 – Management’s assertion on life cycle	142
WebTrust for Certification Authorities – Verified Mark Certificates	145
International Standards – ISAE 3000	145
Example IN8.1 – Unqualified opinion, attestation engagement, period of time	145
Example IN8.2 – Unqualified opinion, attestation engagement, point in time	149
Example IN8.3 – Unqualified opinion, direct engagement, period of time	153
Management’s Assertion	157
Example MA8.1 – Management’s assertion, period of time	157
Example MA8.2 – Management’s assertion, point in time	159

Reporting Guidance

Professional Standards

As of the time of publication, illustrative assurance reports in this document have been prepared following the guidance from, and are intended to be issued under the following professional reporting standard:

- International Standard on Assurance Engagements (ISAE) 3000 Revised, Assurance Engagements Other Than Audits or Reviews of Historical Financial Information

Assurance engagements include both attestation engagements, in which a party other than the practitioner measures or evaluates the underlying subject matter against the criteria, and direct engagements, in which the practitioner measures or evaluates the underlying subject matter against the criteria. ISAE 3000 contains requirements and application and other explanatory material specific to reasonable and limited assurance attestation engagements.

Traditionally, an attestation engagement performed under ISAE 3000 was preferred for WebTrust for CA reporting. Management's assertion was felt to be an important component of the engagement and reporting as it was a clear public demonstration of management's responsibility for the PKI operation being reported on. If there was a qualification, direct reporting was typically used.

The Task Force is of the opinion that an attestation engagement should normally be performed for WebTrust for CA reporting. Assertion-based reporting has been the traditional preference for key users of the reports (the browser community). However, the decision depends on the nature of the engagement. The practitioner will need to agree with the client in advance as to the nature of the engagement that is appropriate in the circumstances. Such agreement will need to be noted in the engagement letter.

Reporting on Code-Signing Engagements

On March 1, 2023 the CA Browser clarified the requirement that meeting the Network and Certificate System Security Requirements, as set forth by the CA/Browser, is required to meet its code-signing requirements. This requirement was clarified by reference similar to Baseline, S/MIME and Verified Mark Certificates.

As a result, WebTrust Principles and Criteria For Certification Authorities – Code Signing Baseline Requirements now included a Principle 4 for meeting the Network and Certificate System Security. The practitioner reports have been updated in this respect.

Reporting On Network Security Requirements

Certain engagements (Baseline +Network Security, Code Signing, S/MIME, and Verified Mark Certificates) by reference require that the CA Browser requirements also be met as part of meeting the respective requirements. At the present time, there is a separate principle in each with regard to network security requirements.

To avoid the need to maintain the same requirements in 3 different offerings, a separate WebTrust for Network Security was created. These criteria can be used and reported in the following manners:

1. Reporting on Baseline +Network Security, Code Signing, S/MIME and Verified Mark Certificates reporting can continue as is using the criteria in the new offering to support the principles being traditionally reported on. This should continue until the Browser Root Store reporting databases are modified to accept a separate WebTrust for Network Security.
2. Modifying the Baseline +Network Security, Code-Signing, S/MIME and Verified Mark Certificates reporting to delete the principle for Network Security once a separate WebTrust for Network Security report is issued.

The impacted reports note the amendments that would be necessary when 2 above is used.

Public Disclosure of CA Business Practices

All reports issued should list the names and version numbers of all documents used by the CA to disclose its business practices, including Certificate Policies (CP) and Certification Practice Statements (CPS).

At least one type of document (CP or CPS) is required to be “publicly available” to relying parties and should be hyperlinked within the report.

For example, a CA selling and issuing certificates to the general public would fulfil the “publicly available” requirement by publishing its CP and/or CPS documents in an unprotected and conspicuous area of its website. A CA issuing certificates within a private organisation that are only intended to be used within that organisation (for example, to authenticate to company applications) would fulfil the “publicly available” requirement by publishing its CPS and/or CPS documents in an unprotected area of the organisation’s intranet that is accessible to all organisation users.

CA Facilities

All reports issued should list the state/province, and country of all physical locations of CA facilities that were included in the scope of the engagement.

CA facilities may include data centre locations (primary and alternate sites), registration authority locations (for registration authority operations performed by the CA), and all other locations where general IT and business process controls that are relevant to CA operations in scope (including cloud and remote locations).

List of Root and Subordinate CAs in Scope

All reports issued must list all root and subordinate CAs that were in scope for the engagement. For attestation engagements, this list should match the list provided in management's assertion.

The names of the CAs should be presented in a manner consistent with how these names appear in applications that use the CA's certificate (for example, when viewing the certificate chain in a web browser). The most common method of identification would be the "Common Name (CN)" field in the "Subject" extension of each CA certificate.

For example, if the common name of the CA is "ABC Root Certification Authority - CA1", then this is how the CA should be identified in the report. Using short-forms such as "ABC Root CA" may cause ambiguity.

The list of CAs should be presented in a clear format. It is preferred that CAs be listed in a referenced appendix, although the use of a bulleted list is permissible in the assurance report.

Disclosure of Changes in Scope or Roots with no Activity

During the year, various roots may be retired and may not be in use at the end of the reporting period. In addition, certain roots that are included in scope may not have issued any certificates. This information is important to users of the report and should be included. The following is an example of what could be included in the assurance report.

The XY (*Attachment A, CA #13*), YA (*Attachment A, CA #9*), L1 (*Attachment A, CA #10*), and Y2 (*Attachment A, CA #14*) CAs did not issue certificates during the period 1 November 2020 to 31 January 202x and were maintained online to provide revocation status information only. The CA certificate for the XY CA expired on 5 January 202y and was not renewed. The CA certificate for the YA CA was revoked on 2 February 202y and was not re-issued.

Reference to Applicable WebTrust Principles and Criteria

All reports issued should make reference to the applicable WebTrust principles and criteria used, including the version number. These principles and criteria should be hyperlinked in the report (and management's assertion).

Date Formats

Dates listed in the report and management's assertion should follow a consistent format with the full name of the month spelled out (i.e., 7 May 202y, or May 7, 202y). Numerical date formats (i.e., 07/05/202y or 05/07/202y) should be avoided.

Reporting on Subscriber Registration Activities

The practitioner is required to perform testing of the relevant controls maintained at the CA level regardless of the extent of outsourcing of the over the authenticity and confidentiality of subscriber and relying party information function. In an engagement based on ISAE 3000, the use of the statement "for the registration activities performed by ABC-CA" is designed to add clarity to the limit of the assertion.

Where external RAs are used

External registration authorities are required to comply with the relevant provisions of the CA's business practices disclosures, often documented in a CPS and applicable CP(s). The functions performed by these specific groups would typically be outside the scope of the WebTrust for Certification Authorities engagement performed for the CA. In this case, management's assertion should specify those aspects of the registration process that are not handled by the CA. External RAs could be considered and reported upon through a separate engagement from the CA, using the relevant criteria contained in the relevant WebTrust Principles and Criteria for Certification Authorities Version being reported on. It is recommended that a separate paragraph be included in the assurance report when external RAs are used:

- a. ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

Reporting When Certain Criteria Not Applicable as Services Not Performed by CA

There will be situations where certain WebTrust criteria are not applicable as the CA does not perform the relevant CA service. A common example is not performing certificate rekey activities. In these scenarios, it is recommended that the practitioner note in the assurance report that the criteria were not in scope for the engagement as the CA does not perform such services. Wording such as the following could be used.

- b. ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

Qualified Assurance Reports

Under ISAE 3000, par. 77, when the statement made by the appropriate party has identified and properly described that the subject matter information is materially misstated, the practitioner shall either:

- (a) Express a qualified conclusion or adverse conclusion phrased in terms of the underlying subject matter and the applicable criteria (Sample reports 1.4 and 1.6); or
- (b) If specifically required by the terms of the engagement to phrase the conclusion in terms of a statement made by the appropriate party, express an unqualified conclusion but include an Emphasis of Matter paragraph in the assurance report referring to the statement made by the appropriate party that identifies and properly describes that the subject matter information is materially misstated.

Where the practitioner issues a qualified report, the Task Force recommends that option (a) be used to express the practitioner's conclusion. The management assertion should be amended, and attached to the assurance report. It reflects management's acknowledgement of the issues causing the qualification. The sample reports included in this package are based on option (a). No sample reports for (b) above have been included.

There are various ways in which to report a scenario where the CA does not meet the WebTrust principles and criteria.

Under ISAE 3000, depending on whether management has modified their assertion or not, the practitioner has the following options:

- 1) If Management has not modified its assertion (the assertion states they meet the criteria even though matters of non-compliance were identified)
The practitioner will assess the materiality and pervasiveness of the matter(s) of non-compliance and determine if the effects or possible effects of a matter are:
 - not so material or pervasive, then the practitioner would issue a qualified opinion (Example IN1.4: Qualified opinion)
 - material and pervasive, then the practitioner would issue an adverse opinion or disclaimer of conclusion.

This option (option 1) is not recommended by the Task Force as management appears as either not being aware of the issues that cause the assurance report qualification or not taking responsibility for such. The Task Force believes that the assertion should be modified to reflect the control issues that created the report qualification and do not meet the WebTrust principles and criteria. It reflects management's acknowledgement of the issues causing the report qualification.

- 2) If Management has modified its assertion (to state they do not meet (part of) the criteria)

The practitioner can issue:

- An unqualified opinion but include an emphasis of matter paragraph regarding the non-compliance or
- Express a qualified or adverse conclusion (based on the material and pervasive nature of the matter) with reference to management's modified assertion.

The former is only available if specifically required by the terms of the engagement. It is the opinion of the Task Force, however, that a practitioner NOT issue an unqualified report with emphasis of matter provided in a scenario where management's assertion is modified. This is felt to be too confusing to report users.

Rather, when ISAE 3000 is used for reporting, the second option should be used. This option is shown as example IN1.5.

The practitioner reports directly on the subject matter and applicable criteria since there is no management assertion provided for these engagements. When the practitioner issues a qualified report, it is referenced to the subject matter and applicable criteria. No management assertion is included in the report. This option is shown as example IN1.5.

WebTrust for Certification Authorities

International Standards – ISAE 3000

Example IN1.1 – Unqualified opinion, attestation engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope¹

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{2, 3} that for its Certification Authority (CA) operations at <LOCATION>,⁴ throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],⁵ ABC-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁶
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA’s Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]⁷
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)⁸
- 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;

1 Subheadings are optional and can be removed if desired.

2 Hyperlink to assertion.

3 Statement can be used rather than assertion throughout if desired.

4 CA processing locations as defined in the “Reporting Guidance” section.

5 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to “Reporting Guidance” section.

6 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

7 Remove bracketed text/bullet if CA has a combined CP and CPS document.

8 If CA has a combined CP/CPS then remove references to Certificate Policy.

- subscriber information is properly authenticated (for the registration activities performed by ABC-CA); 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.⁹

[(If external RAs are used) ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.]¹⁰

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.]¹¹

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,¹² 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.x.

Our independence and quality control¹³

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services, Engagements* and accordingly maintains a comprehensive system

9 Include applicable version number and hyperlink to the criteria document.

10 Remove bracketed text if external RAs are not used.

11 Modify this paragraph as appropriate to exclude certain criteria from scope. Please note that criteria can be excluded only if the CA does not provide the related service.

12 Statement can be used rather than assertion throughout if desired.

13 For engagements beginning on or after December 15, 2022 replace with "Our independence and quality management".

of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]¹⁴

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]¹⁵

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion¹⁶ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion¹⁷ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

14 Use this paragraph for engagements beginning before December 15, 2022.

15 Use this paragraph for engagements beginning on or after December 15, 2022.

16 Statement can be used rather than assertion throughout if desired.

17 Statement can be used rather than assertion throughout if desired.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,¹⁸ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's 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.]¹⁹

Firm Name

City, State/Province, Country

Report Date

18 Statement can be used rather than assertion throughout if desired.

19 Remove bracketed text if a seal is not issued.

Example IN1.2 – Unqualified opinion, attestation engagement, point in time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope²⁰

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{21, 22} that for its Certification Authority (CA) operations at <LOCATION>,²³ as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],²⁴ ABC-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]²⁵
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - [ABC-CA’s Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]²⁶
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)²⁷
- suitably designed, and placed into operation, 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 (for the registration activities performed by ABC-CA); and
 - subordinate CA certificate requests are accurate, authenticated, and approved

20 Subheadings are optional and can be removed if desired.

21 Hyperlink to assertion.

22 Statement can be used rather than assertion throughout if desired.

23 CA processing locations as defined in the “Reporting Guidance” section.

24 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to “Reporting Guidance” section.

25 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

26 Remove bracketed text/bullet if CA has a combined CP and CPS document.

27 If CA has a combined CP/CPS then remove references to Certificate Policy.

- suitably designed, and placed into operation, 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.²⁸

[(If external RAs are used) ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.]²⁹

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.]³⁰

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,³¹ 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.x.

Our independence and quality control³²

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³³

28 Include applicable version number and hyperlink to the criteria document.

29 Remove bracketed text if external RAs are not used.

30 Modify this paragraph as appropriate to exclude certain criteria from scope. Please note that criteria can be excluded only if the CA does not provide the related service.

31 Statement can be used rather than assertion throughout if desired.

32 For engagements beginning on or after December 15, 2022 replace with "Our independence and quality management".

33 Use this paragraph for engagements beginning before December 15, 2022.

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³⁴

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion³⁵ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion³⁶ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's 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. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ABC-CA's controls, individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The suitability of the design of the controls at ABC-CA 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 suitability of the design of the controls at individual subscriber and relying party locations.

34 Use this paragraph for engagements beginning on or after December 15, 2022.

35 Statement can be used rather than assertion throughout if desired.

36 Statement can be used rather than assertion throughout if desired.

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 unauthorised 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.

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,³⁷ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

³⁷ Statement can be used rather than assertion throughout if desired.

Example IN1.3 – Unqualified opinion, direct engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope³⁸

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,³⁹ whether ABC-CA

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁴⁰
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA’s Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]⁴¹
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)⁴²
- 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 (for the registration activities performed by ABC-CA); 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 authorised individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

38 Subheadings are optional and can be removed if desired.

39 CA processing locations as defined in the “Reporting Guidance” section.

40 At least one of these documents should be hyperlinked. If the CA does not have a separate CP then remove the second bullet.

41 Remove bracketed text/bullet if CA has a combined CP and CPS document.

42 If CA has a combined CP/CPS then remove references to Certificate Policy.

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope]⁴³ in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.⁴⁴

[(If external RAs are used) ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.]⁴⁵

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.]⁴⁶

Certification authority's responsibilities

ABC-CA's management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles Criteria for Certification Authorities v2.x.⁴⁷

Our independence and quality control⁴⁸

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴⁹

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive

43 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section.

44 Include applicable version number and hyperlink to the criteria document.

45 Remove bracketed text if external RAs are not used.

46 Modify this paragraph as appropriate to exclude certain criteria from scope. Please note that criteria can be excluded only if the CA does not provide the related service.

47 Include applicable version number and hyperlink to the criteria document.

48 For engagements beginning on or after December 15, 2022 replace with "Our independence and quality management".

49 Use this paragraph for engagements beginning before December 15, 2022.

system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁵⁰

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities v2.x, based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's disclosures and controls conform to the WebTrust Criteria, and, accordingly, included:

1. obtaining an understanding of ABC-CA's 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised access to systems

50 Use this paragraph for engagements beginning on or after December 15, 2022.

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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA has, in all material respects:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁵¹
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]⁵²
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)⁵³
- 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 (for the registration activities performed by ABC-CA); 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

51 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

52 Remove bracketed text/bullet if CA has a combined CP and CPS document.

53 If CA has a combined CP/CPS then remove references to Certificate Policy.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's 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.]⁵⁴

Firm Name

City, State/Province, Country

Report Date

54 Remove bracketed text if a seal is not issued.

Example IN1.4 – Qualified opinion on physical security and business continuity, attestation engagement, period of time – Assertion not modified by management

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope⁵⁵

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{56, 57} that for its Certification Authority (CA) operations at <LOCATION>,⁵⁸ throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],⁵⁹ ABC-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁶⁰
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA’s Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]⁶¹
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)⁶²
- 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 (for the registration activities performed by ABC-CA); and
 - subordinate CA certificate requests are accurate, authenticated, and approved

55 Subheadings are optional and can be removed if desired.

56 Hyperlink to assertion.

57 Statement can be used rather than assertion throughout if desired.

58 CA processing locations as defined in the “Reporting Guidance” section.

59 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to “Reporting Guidance” section.

60 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

61 Remove bracketed text / bullet if CA has a combined CP and CPS document.

62 If CA has a combined CP/CPS then remove references to Certificate Policy.

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.⁶³

[(If external RAs are used) ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.]⁶⁴

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.]⁶⁵

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,⁶⁶ 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.x.

Our independence and quality control⁶⁷

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁶⁸

63 Include applicable version number and hyperlink to the criteria document.

64 Remove bracketed text if external RAs are not used.

65 Modify this paragraph as appropriate to exclude certain criteria from scope. Please note that criteria can be excluded only if the CA does not provide the related service.

66 Statement can be used rather than assertion throughout if desired.

67 For engagements beginning on or after December 15, 2022 replace with "Our independence and quality management".

68 Use this paragraph for engagements beginning before December 15, 2022.

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁶⁹

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion⁷⁰ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion⁷¹ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised access to systems

69 Use this paragraph for engagements beginning on or after December 15, 2022.

70 Statement can be used rather than assertion throughout if desired.

71 Statement can be used rather than assertion throughout if desired.

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.

Basis for qualified opinion

During our procedures, we noted that sufficient physical and environmental security controls were not implemented at ABC-CA's data centre. Specifically:

- electronic and auditable dual-custody multi-factor entrance and exit controls to secure PKI area were not implemented;
- (other findings as applicable)

This caused WebTrust Criterion 3.4 which reads:

The CA maintains controls to provide reasonable assurance that:

- *physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control;*
- *CA facilities and equipment are protected from environmental hazards;*
- *loss, damage or compromise of assets and interruption to business activities are prevented; and*
- *compromise of information and information processing facilities is prevented.*

to not be met.

During our procedures, we noted that a sufficient disaster recovery plan was not developed and tested. Additionally, physically secure disaster recovery facilities were not available. This caused WebTrust Criterion 3.8 which reads:

The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum:

- *the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system;*
- *the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;*
- *the storage of backups of systems, data and configuration information at an alternate location; and*
- *the availability of an alternate site, equipment and connectivity to enable recovery.*

The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation or degradation of the CA's services.

to not be met.

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified section above, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,⁷² as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name

City, State/Province, Country

Report Date

⁷² Statement can be used rather than assertion throughout if desired.

Example IN1.5 – Qualified opinion on physical security and business continuity, direct engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope⁷³

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,⁷⁴ whether ABC-CA

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁷⁵
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA’s Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]⁷⁶
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)⁷⁷
- 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 (for the registration activities performed by ABC-CA); 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 authorised individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

73 Subheadings are optional and can be removed if desired.

74 CA processing locations as defined in the “Reporting Guidance” section.

75 At least one of these documents should be hyperlinked. If the CA does not have a separate CP then remove the second bullet.

76 Remove bracketed text/bullet if CA has a combined CP and CPS document.

77 If CA has a combined CP/CPS then remove references to Certificate Policy.

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope]⁷⁸ in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.⁷⁹

[(If external RAs are used) ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.]⁸⁰

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.]⁸¹ Replace with list of Root and Subordinate CAs in scope or reference to an appendix.

Certification authority's responsibilities

ABC-CA's management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles Criteria for Certification Authorities v2.x.⁸²

Our independence and quality control⁸³

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁸⁴

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive

78 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section.

79 Include applicable version number and hyperlink to the criteria document.

80 Remove bracketed text if external RAs are not used.

81 Modify this paragraph as appropriate to exclude certain criteria from scope. Please note that criteria can be excluded only if the CA does not provide the related service.

82 Include applicable version number and hyperlink to the criteria document.

83 For engagements beginning on or after December 15, 2022 replace with "Our independence and quality management".

84 Use this paragraph for engagements beginning before December 15, 2022.

system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁸⁵

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities v2.x, based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's disclosures and controls conform to the WebTrust Criteria, and, accordingly, included:

1. obtaining an understanding of ABC-CA's 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised access to systems

85 Use this paragraph for engagements beginning on or after December 15, 2022.

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.

Basis for qualified opinion

During our procedures, we noted that sufficient physical and environmental security controls were not implemented at ABC-CA's data centre. Specifically:

- electronic and auditable dual-custody multi-factor entrance and exit controls to secure PKI area were not implemented;
- (other findings as applicable)

This caused WebTrust Criterion 3.4 which reads:

The CA maintains controls to provide reasonable assurance that:

- *physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control;*
- *CA facilities and equipment are protected from environmental hazards;*
- *loss, damage or compromise of assets and interruption to business activities are prevented; and*
- *compromise of information and information processing facilities is prevented.*

to not be met.

During our procedures, we noted that a sufficient disaster recovery plan was not developed and tested. Additionally, physically secure disaster recovery facilities were not available. This caused WebTrust Criterion 3.8 which reads:

The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum:

- *the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system;*
- *the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;*
- *the storage of backups of systems, data and configuration information at an alternate location; and*
- *the availability of an alternate site, equipment and connectivity to enable recovery.*

The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation or degradation of the CA's services.

to not be met.

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified opinion section above, throughout the period <DATE> to <DATE>, ABC-CA has, in all material respects:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁸⁶
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]⁸⁷
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)⁸⁸
- 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 (for the registration activities performed by ABC-CA); 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

86 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

87 Remove bracketed text / bullet if CA has a combined CP and CPS document.

88 If CA has a combined CP/CPS then remove references to Certificate Policy.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name

City, State/Province, Country

Report Date

Example IN1.6 – Qualified opinion on physical security and business continuity, attestation engagement, period of time – Modified management assertion – Table presentation

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope⁸⁹

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{90, 91} that, except for matters described in the assertion,⁹² for its Certification Authority (CA) operations at <LOCATION>,⁹³ throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],⁹⁴ ABC-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁹⁵
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA’s Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]⁹⁶
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)⁹⁷
- 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 (for the registration activities performed by ABC-CA); and

89 Subheadings are optional and can be removed if desired.

90 Hyperlink to assertion.

91 Statement can be used rather than assertion throughout if desired.

92 Statement can be used rather than assertion throughout if desired.

93 CA processing locations as defined in the “Reporting Guidance” section.

94 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to “Reporting Guidance” section.

95 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

96 Remove bracketed text/bullet if CA has a combined CP and CPS document.

97 If CA has a combined CP/CPS then remove references to Certificate Policy.

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.⁹⁸

[(If external RAs are used) ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.]⁹⁹

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.]¹⁰⁰

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,¹⁰¹ 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.x.

Our independence and quality control¹⁰²

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]¹⁰³

98 Include applicable version number and hyperlink to the criteria document.

99 Remove bracketed text if external RAs are not used.

100 Modify this paragraph as appropriate to exclude certain criteria from scope. Please note that criteria can be excluded only if the CA does not provide the related service.

101 Statement can be used rather than assertion throughout if desired.

102 For engagements beginning on or after December 15, 2022 replace with "Our independence and quality management".

103 Use this paragraph for engagements beginning before December 15, 2022.

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]¹⁰⁴

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion¹⁰⁵ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion¹⁰⁶ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

104 Use this paragraph for engagements beginning on or after December 15, 2022.

105 Statement can be used rather than assertion throughout if desired.

106 Statement can be used rather than assertion throughout if desired.

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 unauthorised 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.

Basis for qualified opinion

During our procedures, we noted the following that caused a qualification of our opinion:

	Observation	Relevant WebTrust Criteria
1	<p>We noted that electronic and auditable dual-custody multi-factor entrance and exit controls to secure PKI area were not implemented.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.4 to not be met.</p>	<p>3.4: The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> • physical access to CA facilities and equipment is limited to authorised individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented

	Observation	Relevant WebTrust Criteria
2	<p>We noted that a sufficient disaster recovery plan was not developed and tested. Additionally, physically secure disaster recovery facilities were not available.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.8 to not be met.</p>	<p>3.8: The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum:</p> <ul style="list-style-type: none"> • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • the storage of backups of systems, data and configuration information at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery. <p>The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation or degradation of the CA's services.</p>

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified opinion section above, throughout the period <DATE> to <DATE>, ABC-CA has, in all material respects:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]¹⁰⁷
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]¹⁰⁸

107 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

108 Remove bracketed text/bullet if CA has a combined CP and CPS document.

- ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)¹⁰⁹
- 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 (for the registration activities performed by ABC-CA); 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

109 If CA has a combined CP/CPS then remove references to Certificate Policy.

Sample Appendix A

List of CAs in Scope

Root CAs

Number and List

OV SSL Issuing CAs

Number and List

EV SSL Issuing CAs

Number and List

Private Trust Issuing CAs

Number and List

Non-EV Code Signing Issuing CAs

Number and List

EV Code Signing Issuing CAs

Number and List

Secure Email (S/MIME) CAs

Number and List

Document Signing CAs

Number and List

Adobe CAs

Number and List

Timestamp CAs

Number and List

Other CAs

Number and List

Sample CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA - G1	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA - G1	6D5A3 34C1BA F569E	rsaEncryption	(4096 bit)	sha256With RSAEncryption	Mar 13 17:13:04 2017 GMT	Dec 31 17:13:04 2030 GMT	02:AE:95:D6: 52:E5:01:87: 40:AD:11:AF: DC:CD:01:EE: 69:A7:D4:77	DB:AF:00:71: 06:47:95:A5: 78:FC:FD:9F: 9E:19:63:BF: E6:D1:3D:D8: FE:8C:47: A0:7E:33:BB: 77:F9:1A:15:19
2	1	C=CA O=ABC-CA Inc. CN=ABC-CA Issuing CA - EV	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA - G1	7DAAA F3CF15 F8F45	rsaEncryption	(2048 bit)	sha256With RSAEncryption	Mar 14 01:25:41 2017 GMT	Mar 14 01:25:41 2027 GMT	92:A4:60:D4 :ED:AC:57:3 D:C2:1B:24:0 7:0D:AF:AC :DD:F1:0D:8 A:9A	DF:30:CF:75: 83:21:F7:F6:DO: 08:21:05:AB: CD:BA:A4:59: 38:B3:42:CF: 5D:10:38:27: 92:52:E8:A7: D3:3A:9F
2	2	C=CA O=ABC-CA Inc. CN=ABC-CA Issuing CA - EV	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA - G1	8FABA F6CF45 F884F	rsaEncryption	(2048 bit)	sha256With RSAEncryption	Apr 22 07:41:53 2017 GMT	Apr 22 07:41:53 2027 GMT	92:A4:60:D4 :ED:AC:57:3 D:C2:1B:24:0 7:0D:AF:AC :DD:F1:0D:8 A:9A	DC:25:7D:4E: 09:57:8E:1F: 86:E8:17:95: CA:FF:57:6C: D8:DD:AE:BD: A9:0D:30:23: 3E:24:CA:AC: B4:C6:60:B1

Management's Assertion

Example MA1.1 – Management's assertion,¹¹⁰ period of time

ABC-CA MANAGEMENT'S ASSERTION¹¹¹

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],¹¹² and provides the following CA services:¹¹³

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

The management of ABC-CA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website [or other repository location],¹¹⁴ 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 ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

110 Statement can be used rather than assertion throughout if desired.

111 Statement can be used rather than assertion throughout if desired.

112 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section.

113 This is a list of common services provided by CAs. Add and remove from this list to include the relevant services being provided.

114 Link to business practices repository location and describe location if not website (i.e., intranet).

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its Certification Authority (CA) services at <LOCATION>,¹¹⁵ throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]¹¹⁶
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]¹¹⁷
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)¹¹⁸
- 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 (for the registration activities performed by ABC-CA); 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 authorised individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x,¹¹⁹ including the following:¹²⁰

115 CA processing locations as defined in the "Reporting Guidance" section.

116 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

117 Remove bracketed text/bullet if CA has a combined CP and CPS document.

118 If CA has a combined CP/CPS then remove references to Certificate Policy.

119 Include applicable version number and hyperlink to the criteria document.

120 Remove bullets that are not applicable.

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

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services

- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our assertion¹²¹ does not extend to controls that would address those criteria.]¹²²

<Signoff Name and Title>

<Date that matches the assurance opinion date>

121 Statement can be used rather than assertion throughout if desired.

122 Modify this paragraph as appropriate to exclude certain criteria from scope.

Example MA1.2 – Management’s assertion,¹²³ point in time

ABC-CA MANAGEMENT’S ASSERTION¹²⁴

ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],¹²⁵ and provides the following CA services:¹²⁶

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

The management of ABC-CA is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its website [or other repository location],¹²⁷ 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, controls placed into operation can only provide reasonable assurance with respect to ABC-CA’s Certification Authority operations.

123 Statement can be used rather than assertion throughout if desired.

124 Statement can be used rather than assertion throughout if desired.

125 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to “Reporting Guidance” section.

126 This is a list of common services provided by CAs. Add and remove from this list to include the relevant services being provided.

127 Link to business practices repository location and describe location if not website (i.e., intranet).

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its Certification Authority (CA) services at <LOCATION>¹²⁸ as of <DATE>, ABC-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]¹²⁹
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]¹³⁰
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)¹³¹
- suitably designed, and placed into operation, 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 (for the registration activities performed by ABC-CA); and
 - subordinate CA certificate requests are accurate, authenticated, and approved
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorised individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

128 CA processing locations as defined in the "Reporting Guidance" section.

129 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

130 Remove bracketed text / bullet if CA has a combined CP and CPS document.

131 If CA has a combined CP/CPS then remove references to Certificate Policy.

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x,¹³² including the following:¹³³

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

¹³² Include applicable version number and hyperlink to the criteria document.

¹³³ Remove bullets that are not applicable.

- CA Key Escrow

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

<Signoff Name and Title>

<Date that matches the assurance opinion date>

Example MA1.3 – Management’s modified assertion,¹³⁴ period of time – Accompanying qualified report

ABC-CA MANAGEMENT’S ASSERTION¹³⁵

ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],¹³⁶ and provides the following CA services:¹³⁷

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

The management of ABC-CA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website [or other repository location],¹³⁸ 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 ABC-CA’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

134 Statement can be used rather than assertion throughout if desired.

135 Statement can be used rather than assertion throughout if desired.

136 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to “Reporting Guidance” section.

137 This is a list of common services provided by CAs. Add and remove from this list to include the relevant services being provided.

138 Link to business practices repository location and describe location if not website (i.e., intranet).

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

	Observation	Relevant WebTrust Criteria
1	<p>We noted that electronic and auditable dual-custody multi-factor entrance and exit controls to secure PKI area were not implemented.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.4 to not be met.</p>	<p>3.4: The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> • physical access to CA facilities and equipment is limited to authorised individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented
2	<p>We noted that a sufficient disaster recovery plan was not developed and tested. Additionally, physically secure disaster recovery facilities were not available.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.8 to not be met.</p>	<p>3.8: The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum:</p> <ul style="list-style-type: none"> • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • the storage of backups of systems, data and configuration information at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery. <p>The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation or degradation of the CA's services.</p>

Based on that assessment, in ABC-CA management's opinion, except for the matters described in the preceding table, in providing its Certification Authority (CA) services at <LOCATION>,¹³⁹ throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]¹⁴⁰
- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]¹⁴¹
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)¹⁴²
- 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 (for the registration activities performed by ABC-CA); 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 authorised individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

139 CA processing locations as defined in the "Reporting Guidance" section.

140 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

141 Remove bracketed text/bullet if CA has a combined CP and CPS document.

142 If CA has a combined CP/CPS then remove references to Certificate Policy.

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x,¹⁴³ including the following:¹⁴⁴

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

¹⁴³ Include applicable version number and hyperlink to the criteria document.

¹⁴⁴ Remove bullets that are not applicable.

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our assertion¹⁴⁵ does not extend to controls that would address those criteria.]¹⁴⁶

<Signoff Name and Title>

<Date that matches the assurance opinion date>

145 Statement can be used rather than assertion throughout if desired.

146 Modify this paragraph as appropriate to exclude certain criteria from scope.

WebTrust for Certification Authorities – SSL Baseline with Network Security

Specific Reporting Guidance for SSL Baseline with Network Security¹⁴⁷

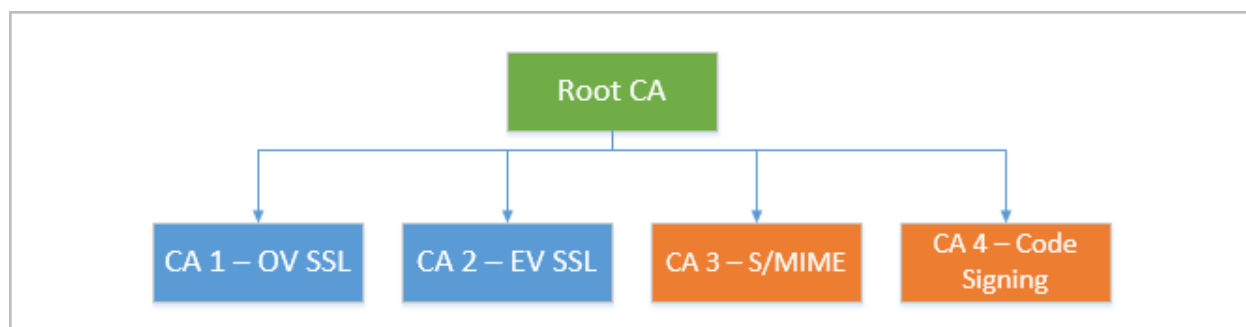
Currently, the SSL Baseline with Network Security principles and criteria incorporates two different CA/Browser Forum requirements documents:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“SSL Baseline Requirements”); and
- Network and Certificate System Security Requirements (“Network Security Requirements”)

The SSL Baseline Requirements only apply to PKI hierarchies (root and subordinate CAs) which issue publicly trusted SSL/TLS certificates intended to authenticate servers on the Internet (i.e., certificates containing the `id_kp_serverAuth` OID (1.3.6.1.5.5.7.3.1) in the `extendedKeyUsage` extension).

The Network Security Requirements apply to all CAs within a publicly trusted PKI hierarchy, even if those certificates are designed for other uses (i.e., code signing, client authentication, secure email, document signing etc.).

For example, in the following PKI hierarchy consisting of a Root CA and 4 Subordinate CAs directly underneath it:



The SSL Baseline Requirements would only apply to Root CA, CA 1, and CA 2. However, the Network Security Requirements would apply to all CAs – Root CA, CA 1, CA 2, CA 3, and CA 4.

¹⁴⁷ See discussion in introduction to document as Network security will be reported upon separately in engagements beginning on or after July 1, 2023.

The illustrative report examples in this section include language to allow the auditor to explicitly define the scope of which criteria they are opining on for which specific CAs. If the SSL Baseline Requirements and Network Security Requirements apply to all in-scope CAs, then this language can be removed. Conversely, if the engagement is only covering the Network Security Requirements for PKI hierarchies that do not issue SSL/TLS certificates, then language pertaining to the SSL Baseline Requirements can be removed.

International Standards – ISAE 3000

Example IN2.1 – Unqualified opinion, attestation engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope¹⁴⁸

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{149, 150} that for its Certification Authority (CA) operations at <LOCATION>¹⁵¹ throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for SSL Baseline Requirements [and Network Security Requirements]],^{152, 153} ABC-CA has:

- [disclosed its SSL certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],¹⁵⁴
 including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA 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 ABC-CA)
- 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

148 Subheadings are optional and can be removed if desired.

149 Hyperlink to assertion.

150 Statement can be used rather than assertion throughout if desired.

151 CA processing locations as defined in the “Reporting Guidance” section.

152 Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the SSL Baseline Requirements (and Network Security. Refer to “Reporting Guidance” section.

153 Delete if separate WebTrust for Network Security Report is issued.

154 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

[[And, for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for Network Security Requirements]]:¹⁵⁵

- 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]¹⁵⁶

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security]¹⁵⁷ v2.x.¹⁵⁸

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,¹⁵⁹ including the fairness of its presentation, and the provision of its described services in accordance with [Principle 4 of]¹⁶⁰ the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x.

Our independence and quality control¹⁶¹

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]¹⁶²

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive

155 Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the Network Security Requirements, if this is different to the CAs in scope for the SSL Baseline Requirements. If the in-scope CAs are the same for both the SSL Baseline Requirements and the Network Security Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to “Reporting Guidance” section.

156 Delete if separate WebTrust for Network Security Report is issued.

157 Delete if separate WebTrust for Network Security Report is issued.

158 Include applicable version number and hyperlink to the criteria document.

159 Statement can be used rather than assertion throughout if desired.

160 Include this bracket if only opining on the Network Security Requirements.

161 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

162 Use this paragraph for engagements beginning before December 15, 2022.

system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]¹⁶³

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion¹⁶⁴ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion¹⁶⁵ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, [and] obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum],¹⁶⁶
2. selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised access to systems

163 Use this paragraph for engagements beginning on or after December 15, 2022.

164 Statement can be used rather than assertion throughout if desired.

165 Statement can be used rather than assertion throughout if desired.

166 Delete if separate WebTrust for Network Security Report is issued.

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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,¹⁶⁷ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline [with Network Security]¹⁶⁸ v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline [with Network Security]¹⁶⁹ v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities - SSL Baseline [with Network Security]¹⁷⁰ 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.]¹⁷¹

Firm Name
City, State/Province, Country
Report Date

167 Statement can be used rather than assertion throughout if desired.

168 Delete if separate WebTrust for Network Security Report is issued.

169 Delete if separate WebTrust for Network Security Report is issued.

170 Delete if separate WebTrust for Network Security Report is issued.

171 Remove bracketed text if a seal is not issued. Seals will only be issued when the SSL Baseline Requirements are covered. Reports covering only the Network Security Requirements are not eligible for a seal.

Example IN2.2 - Unqualified opinion, attestation engagement, point in time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope¹⁷²

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{173, 174} that for its Certification Authority (CA) operations at <LOCATION>,¹⁷⁵ as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for SSL Baseline Requirements [and Network Security Requirements]],^{176, 177} ABC-CA has:

- [disclosed its SSL certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],¹⁷⁸ including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, 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 ABC-CA)
- suitably designed, and placed into operation, 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

172 Subheadings are optional and can be removed if desired.

173 Hyperlink to assertion.

174 Statement can be used rather than assertion throughout if desired.

175 CA processing locations as defined in the “Reporting Guidance” section.

176 Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the SSL Baseline Requirements (and Network Security. Refer to “Reporting Guidance” section.

177 Delete if separate WebTrust for Network Security Report is issued.

178 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

[[And, for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for Network Security Requirements]]:¹⁷⁹

- suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum¹⁸⁰

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security]¹⁸¹ v2.x.¹⁸²

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,¹⁸³ including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security]¹⁸⁴ v2.x.

Our independence and quality control¹⁸⁵

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]¹⁸⁶

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive

179 Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the Network Security Requirements, if this is different to the CAs in scope for the SSL Baseline Requirements. If the in-scope CAs are the same for both the SSL Baseline Requirements and the Network Security Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to “Reporting Guidance” section.

180 Delete if separate WebTrust for Network Security Report is issued.

181 Delete if separate WebTrust for Network Security Report is issued

182 Include applicable version number and hyperlink to the criteria document.

183 Statement can be used rather than assertion throughout if desired.

184 Delete if separate WebTrust for Network Security Report is issued.

185 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

186 Use this paragraph for engagements beginning before December 15, 2022.

system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]¹⁸⁷

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion¹⁸⁸ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion¹⁸⁹ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];¹⁹⁰
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ABC-CA's controls, individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The suitability of the design of the controls at ABC-CA 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 suitability of the design of the controls at individual subscriber and relying party locations.

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 unauthorised access to systems

187 Use this paragraph for engagements beginning on or after December 15, 2022.

188 Statement can be used rather than assertion throughout if desired.

189 Statement can be used rather than assertion throughout if desired.

190 Delete if separate WebTrust for Network Security Report is issued.

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.

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,¹⁹¹ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline [with Network Security]¹⁹² v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline [with Network Security]¹⁹³ v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

191 Statement can be used rather than assertion throughout if desired.

192 Delete if separate WebTrust for Network Security Report is issued.

193 Delete if separate WebTrust for Network Security Report is issued.

Example IN2.3 - Unqualified opinion, direct engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope¹⁹⁴

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,¹⁹⁵ whether ABC-CA has

- disclosed its SSL certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],¹⁹⁶
 including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA 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 ABC-CA)
- 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 <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for SSL Baseline Requirements and Network Security Requirements

[[And, for CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Network Security Requirements]]]:¹⁹⁷

194 Subheadings are optional and can be removed if desired.

195 CA processing locations as defined in the “Reporting Guidance” section.

196 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

197 Replace with list of Root and Subordinate CAs in scope for the Network Security Requirements or reference to an appendix, if this is different to the CAs in scope for the SSL Baseline Requirements. If the in-scope CAs are the same for both the SSL Baseline Requirements and the Network Security Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to “Reporting Guidance” section.

- 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]¹⁹⁸

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security]¹⁹⁹ v2.x.²⁰⁰

Certification authority’s responsibilities

ABC-CA’s management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security]²⁰¹ v2.x.²⁰²

Our independence and quality control²⁰³

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]²⁰⁴

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]²⁰⁵

198 Delete if separate WebTrust for Network Security Report is issued.

199 Delete if separate WebTrust for Network Security Report is issued.

200 Include applicable version number and hyperlink to the criteria document.

201 Delete if separate WebTrust for Network Security Report is issued.

202 Include applicable version number and hyperlink to the criteria document.

203 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

204 Use this paragraph for engagements beginning before December 15, 2022.

205 Use this paragraph for engagements beginning on or after December 15, 2022.

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with²⁰⁶ the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security]²⁰⁷ v2.x, based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's disclosures and controls conform to the WebTrust Criteria, and, accordingly, included:

1. obtaining an understanding of ABC-CA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];²⁰⁸
2. selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

206 Include this bracket if only opining on the Network Security Requirements.

207 Delete if separate WebTrust for Network Security Report is issued.

208 Delete if separate WebTrust for Network Security Report is issued.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA has, in all material respects:

- disclosed its SSL certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],²⁰⁹
 including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA 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 ABC-CA)
- 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

[[And, for CAs as enumerated in Attachment B are only in scope for or [list of Root and Subordinate CAs in scope for Network Security Requirements]]:²¹⁰

- 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]²¹¹

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline [with Network Security]²¹² v2.x.

209 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

210 Replace with list of Root and Subordinate CAs in scope for the Network Security Requirements or reference to an appendix, if this is different to the CAs in scope for the SSL Baseline Requirements. If the in-scope CAs are the same for both the SSL Baseline Requirements and the Network Security Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to "Reporting Guidance" section.

211 Delete if separate WebTrust for Network Security Report is issued.

212 Delete if separate WebTrust for Network Security Report is issued.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline [with Network Security]²¹³ v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities - SSL Baseline [with Network Security]²¹⁴ 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.]²¹⁵

Firm Name
City, State/Province, Country
Report Date

213 Delete if separate WebTrust for Network Security Report is issued.

214 Delete if separate WebTrust for Network Security Report is issued.

215 Remove bracketed text if a seal is not issued. Seals will only be issued when the SSL Baseline Requirements are covered. Reports covering only the Network Security Requirements are not eligible for a seal.

Management's Assertion

Example MA2.1 – Management's assertion,²¹⁶ period of time

ABC-CA MANAGEMENT'S ASSERTION²¹⁷

[ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope for SSL Baseline Requirements [and Network Security Requirements]]^{218, 219} and provides SSL CA services.]²²⁰

[ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope for Network Security Requirements]²²¹ and provides non-SSL CA services.]^{222, 223}

The management of ABC-CA is responsible for establishing and maintaining effective controls over its SSL [and non-SSL]²²⁴ CA operations, including [its network and certificate security system controls],²²⁵ its SSL CA business practices disclosure on its website [or other repository location],²²⁶ SSL key lifecycle management controls, and SSL 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 ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

216 Statement can be used rather than assertion throughout if desired.

217 Statement can be used rather than assertion throughout if desired.

218 Replace with list of Root and Subordinate CAs in scope for the SSL Baseline Requirements and Network Security Requirements or reference to an appendix. Refer to “Reporting Guidance” section.

219 Delete if separate WebTrust for Network Security Report is issued.

220 Include this introductory paragraph if all CAs are SSL CAs and therefore in scope for SSL Baseline Requirements and Network Security Requirements. Remove this paragraph if only auditing the Network Security Requirements.

221 Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the Network Security Requirements or reference to an appendix. Refer to “Reporting Guidance” section.

222 Include this introductory paragraph if there are additional non-SSL CAs that are in scope for the Network Security Requirements. Remove this paragraph if all in-scope CAs are SSL.

223 Delete if separate WebTrust for Network Security Report is issued.

224 Delete if separate WebTrust for Network Security Report is issued.

225 Delete if separate WebTrust for Network Security Report is issued.

226 Link to business practices repository location and describe location if not website (i.e. intranet).

ABC-CA management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL [and non-SSL]²²⁷ Certification Authority (CA) services at <LOCATION>,²²⁸ throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its SSL certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],²²⁹
 including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA 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 ABC-CA)
- 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]²³⁰

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security]²³¹ v2.x.²³²

<Signoff Name and Title>

<Date that matches the assurance opinion date>

227 Delete if separate WebTrust for Network Security Report is issued.

228 CA processing locations as defined in the “Reporting Guidance” section.

229 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

230 Delete if separate WebTrust for Network Security Report is issued.

231 Delete if separate WebTrust for Network Security Report is issued.

232 Include applicable version number and hyperlink to the criteria document.

Example MA2.2 – Management’s assertion,²³³ point in time

ABC-CA MANAGEMENT’S ASSERTION²³⁴

[ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope for SSL Baseline Requirements [and Network Security Requirements]]^{235, 236} and provides SSL CA services.]²³⁷

[ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope for Network Security Requirements]²³⁸ and provides non-SSL CA services.]^{239, 240}

The management of ABC-CA is responsible for establishing and maintaining effective controls over its SSL [and non-SSL]²⁴¹ CA operations, including [its network and certificate security system controls],²⁴² its SSL CA business practices disclosure on its website [or other repository location],²⁴³ SSL key lifecycle management controls, and SSL 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 ABC-CA’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its disclosures of its certificate practices [and controls over its SSL CA services. Based on that assessment, in providing its SSL [and non-SSL]²⁴⁴ Certification Authority (CA) services at <LOCATION>,²⁴⁵ as of <DATE>, ABC-CA has:

233 Statement can be used rather than assertion throughout if desired.

234 Statement can be used rather than assertion throughout if desired.

235 Replace with list of Root and Subordinate CAs in scope for the SSL Baseline Requirements and Network Security Requirements or reference to an appendix. Refer to “Reporting Guidance” section.

236 Delete if separate WebTrust for Network Security Report is issued.

237 Include this introductory paragraph if all CAs are SSL CAs and therefore in scope for SSL Baseline Requirements and Network Security Requirements. Remove this paragraph if only auditing the Network Security Requirements.

238 Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the Network Security Requirements or reference to an appendix. Refer to “Reporting Guidance” section.

239 Include this introductory paragraph if there are additional non-SSL CAs that are in scope for the Network Security Requirements. Remove this paragraph if all in-scope CAs are SSL.

240 Delete if separate WebTrust for Network Security Report is issued.

241 Delete if separate WebTrust for Network Security Report is issued.

242 Delete if separate WebTrust for Network Security Report is issued.

243 Link to business practices repository location and describe location if not website (i.e. intranet).

244 Delete if separate WebTrust for Network Security Report is issued.

245 CA processing locations as defined in the “Reporting Guidance” section.

- disclosed its SSL certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],²⁴⁶
 including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, 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 ABC-CA)
- suitably designed, and placed into operation, 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
- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum]²⁴⁷

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline [with Network Security]²⁴⁸ v2.x.²⁴⁹

<Signoff Name and Title>

<Date that matches the assurance opinion date>

246 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

247 Delete if separate WebTrust for Network Security Report is issued.

248 Delete if separate WebTrust for Network Security Report is issued.

249 Include applicable version number and hyperlink to the criteria document.

WebTrust for Certification Authorities – Extended Validation – SSL (“EV SSL”)

International Standards – ISAE 3000

Example IN3.1 – Unqualified opinion, attestation engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope²⁵⁰

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{251, 252} that for its Certification Authority (CA) operations at <LOCATION>,²⁵³ throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],²⁵⁴ ABC-CA has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]²⁵⁵
 including its commitment to provide EV SSL certificates in conformity with the CA/ Browser Forum Guidelines on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

250 Subheadings are optional and can be removed if desired.

251 Hyperlink to assertion.

252 Statement can be used rather than assertion throughout if desired.

253 CA processing locations as defined in the “Reporting Guidance” section.

254 Reference to an appendix or replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to “Reporting Guidance” section.

255 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x.²⁵⁶

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,²⁵⁷ including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x.

Our independence and quality control²⁵⁸

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]²⁵⁹

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]²⁶⁰

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion²⁶¹ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s assertion²⁶² is fairly stated, and, accordingly, included:

256 Include applicable version number and hyperlink to the criteria document.

257 Statement can be used rather than assertion throughout if desired.

258 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

259 Use this paragraph for engagements beginning before December 15, 2022.

260 Use this paragraph for engagements beginning on or after December 15, 2022.

261 Statement can be used rather than assertion throughout if desired.

262 Statement can be used rather than assertion throughout if desired.

1. obtaining an understanding of ABC-CA’s EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
2. selectively testing transactions executed in accordance with disclosed EV SSL certificate lifecycle management 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management’s assertion,²⁶³ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x.

This report does not include any representation as to the quality of ABC-CA’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x, nor the suitability of any of ABC-CA’s services for any customer’s intended purpose.

²⁶³ Statement can be used rather than assertion throughout if desired.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities - Extended Validation SSL 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.]²⁶⁴

Firm Name
City, State/Province, Country
Report Date

²⁶⁴ Remove bracketed text if a seal is not issued.

Example IN3.2 – Unqualified opinion, attestation engagement, point in time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope²⁶⁵

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{266, 267} that for its Certification Authority (CA) operations at <LOCATION>,²⁶⁸ as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],²⁶⁹ ABC-CA has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]²⁷⁰
 including its commitment to provide EV SSL certificates in conformity with the CA/ Browser Forum Guidelines on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x.²⁷¹

265 Subheadings are optional and can be removed if desired.

266 Hyperlink to assertion.

267 Statement can be used rather than assertion throughout if desired.

268 CA processing locations as defined in the “Reporting Guidance” section.

269 Reference to an appendix or replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to “Reporting Guidance” section.

270 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

271 Include applicable version number and hyperlink to the criteria document.

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,²⁷² including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x.

Our independence and quality control²⁷³

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]²⁷⁴

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]²⁷⁵

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion²⁷⁶ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s assertion²⁷⁷ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;

272 Statement can be used rather than assertion throughout if desired.

273 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

274 Use this paragraph for engagements beginning before December 15, 2022.

275 Use this paragraph for engagements beginning on or after December 15, 2022.

276 Statement can be used rather than assertion throughout if desired.

277 Statement can be used rather than assertion throughout if desired.

2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ABC-CA's controls, individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The suitability of the design of the controls at ABC-CA 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 suitability of the design of the controls at individual subscriber and relying party locations.

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 unauthorised 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.

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,²⁷⁸ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

²⁷⁸ Statement can be used rather than assertion throughout if desired.

Example IN3.3 - Unqualified opinion, direct engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. ("ABC-CA"):

Scope²⁷⁹

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,²⁸⁰ whether ABC-CA has

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]²⁸¹
 including its commitment to provide EV SSL certificates in conformity with the CA/ Browser Forum Guidelines on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

throughout the period <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope] in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.x.

Certification authority's responsibilities

ABC-CA's management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.x.²⁸²

279 Subheadings are optional and can be removed if desired.

280 CA processing locations as defined in the "Reporting Guidance" section.

281 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

282 Include applicable version number and hyperlink to the criteria document.

Our independence and quality control²⁸³

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]²⁸⁴

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]²⁸⁵

Practitioner’s responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management’s disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x (the “WebTrust Criteria”), based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s disclosures and controls conform to the WebTrust Criteria, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
2. selectively testing transactions executed in accordance with disclosed EV SSL certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

283 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

284 Use this paragraph for engagements beginning before December 15, 2022.

285 Use this paragraph for engagements beginning on or after December 15, 2022.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA has, in all significant respects:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]²⁸⁶including its commitment to provide EV SSL certificates in conformity with the CA/ Browser Forum Guidelines on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.x.

²⁸⁶ At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.x, nor the suitability of any of ABC-CA's services for any customers intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities - Extended Validation SSL 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.]²⁸⁷

Firm Name

City, State/Province, Country

Report Date

287 Remove bracketed text if a seal is not issued.

Management's Assertion

Example MA3.1 – Management's assertion,²⁸⁸ period of time

ABC-CA MANAGEMENT'S ASSERTION²⁸⁹

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],²⁹⁰ and provides Extended Validation SSL ("EV SSL") CA services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website [or other repository location],²⁹¹ EV SSL key lifecycle management controls, and EV SSL 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 ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in ABC-CA management's opinion, in providing its EV SSL Certification Authority (CA) services at <LOCATION>,²⁹² throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]²⁹³

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

288 Statement can be used rather than assertion throughout if desired.

289 Statement can be used rather than assertion throughout if desired.

290 Replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to "Reporting Guidance" section.

291 Link to business practices repository location and describe location if not website (i.e., intranet).

292 CA processing locations as defined in the "Reporting Guidance" section.

293 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.x.²⁹⁴

<Signoff Name and Title>

<Date that matches the assurance opinion date>

²⁹⁴ Include applicable version number and hyperlink to the criteria document.

Example MA3.2 - Management's assertion,²⁹⁵ point in time

ABC-CA MANAGEMENT'S ASSERTION²⁹⁶

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],²⁹⁷ and provides Extended Validation SSL ("EV SSL") CA services.

The management of ABC-CA is responsible for establishing controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website [or other repository location],²⁹⁸ EV SSL key lifecycle management controls, and EV SSL 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, controls placed into operation can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in ABC-CA management's opinion, in providing its EV SSL Certification Authority (CA) services at <LOCATION>,²⁹⁹ as of <DATE>, ABC-CA has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]³⁰⁰
 including its commitment to provide EV SSL certificates in conformity with the CA/ Browser Forum Guidelines on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and

295 Statement can be used rather than assertion throughout if desired.

296 Statement can be used rather than assertion throughout if desired.

297 Replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to "Reporting Guidance" section.

298 Link to business practices repository location and describe location if not website (i.e., intranet).

299 CA processing locations as defined in the "Reporting Guidance" section.

300 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

- EV SSL subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.x.³⁰¹

<Signoff Name and Title>

<Date that matches the assurance opinion date>

³⁰¹ Include applicable version number and hyperlink to the criteria document.

WebTrust for Certification Authorities – Code Signing (“CS”)

International Standards – ISAE 3000

Example CA4.1 – Unqualified opinion, attestation engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope³⁰²

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{303, 304} that for its Certification Authority (CA) operations at <LOCATION>,³⁰⁵ throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],³⁰⁶ ABC-CA has:

- disclosed its code signing (“CS”) certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]³⁰⁷
 including its commitment to provide CS certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.

302 Subheadings are optional and can be removed if desired.

303 Hyperlink to assertion.

304 Statement can be used rather than assertion throughout if desired.

305 CA processing locations as defined in the “Reporting Guidance” section.

306 Reference to an appendix or replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to “Reporting Guidance” section.

307 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- maintained effective controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x.³⁰⁸
- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]]³⁰⁹ maintained effective controls to provide reasonable assurance that:
 - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [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 that are incorporated by reference.³¹⁰]

In accordance with the WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements v3.x.

Certification Authority’s responsibilities

ABC-CA’s management is responsible for its assertion,³¹¹ including the fairness of its presentation, and the provision of its described services, based on [the WebTrust Principles and Criteria for Certification Authorities – Code Sign Baseline Requirements v3.x.³¹²

Our independence and quality control³¹³

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

308 Include applicable version number and hyperlink to the criteria document.

309 Replace with list of Root and Subordinate CAs in scope for the EC Code Signing Service Requirements or reference to an appendix, if this is different to the CAs in scope for the CS Requirements. If the in-scope CAs are the same for both the CS Requirements and the EV Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to “Reporting Guidance” section.

310 Delete if separate WebTrust for Network Security Report is issued.

311 Statement can be used rather than assertion throughout if desired.

312 Include applicable version number and hyperlink to the criteria document.

313 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³¹⁴

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³¹⁵

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion³¹⁶ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s assertion³¹⁷ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s CS [and EVCS]³¹⁸ certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of CS [and EVCS] certificates, CS [and EVCS] Signing Authority certificates, and CS [and EVCS] Timestamp Authority certificates [and obtaining an understanding of ABC-CA’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum];³¹⁹
2. selectively testing transactions executed in accordance with disclosed CS [and EVCS] certificate lifecycle management 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

314 Use this paragraph for engagements beginning before December 15, 2022.

315 Use this paragraph for engagements beginning on or after December 15, 2022.

316 Statement can be used rather than assertion throughout if desired.

317 Statement can be used rather than assertion throughout if desired.

318 If applicable.

319 Delete if separate WebTrust for Network Security Report is issued

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management’s assertion,³²⁰ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - Code Sign Baseline Requirements v3.x.

This report does not include any representation as to the quality of ABC-CA’s services other than its *CA operations at <LOCATION>*,³²¹ nor the suitability of any of ABC-CA’s services for any customer’s intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA’s use of the WebTrust for Certification Authorities - Code Signing 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.]³²²

Firm Name
City, State/Province, Country
Report Date

320 Statement can be used rather than assertion throughout if desired.

321 CA processing locations as defined in the “Reporting Guidance” section.

322 Remove bracketed text if a seal is not issued.

Example CA4.2 – Unqualified opinion, attestation engagement, point in time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope³²³

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{324, 325} that for its Certification Authority (CA) operations at <LOCATION>,³²⁶ throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],³²⁷ ABC-CA has:

- disclosed its code signing (“CS”) certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]³²⁸
 including its commitment to provide CS certificates in conformity with the CA/ Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - CS subscriber information is properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.
- suitably designed, and placed into operation, controls to provide reasonable that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/ Browser Forum Code Sign Working Group requirements v1.x.³²⁹

³²³ Subheadings are optional and can be removed if desired.

³²⁴ Hyperlink to assertion.

³²⁵ Statement can be used rather than assertion throughout if desired.

³²⁶ CA processing locations as defined in the “Reporting Guidance” section.

³²⁷ Reference to an appendix or replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to “Reporting Guidance” section.

³²⁸ At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

³²⁹ Include applicable version number and hyperlink to the criteria document.

- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]]³³⁰ suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - EV CS subscriber information is properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.³³¹]

In accordance with the WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing Certificates v3.x.

Certification Authority’s responsibilities

ABC-CA’s management is responsible for its assertion,³³² including the fairness of its presentation, and the provision of its described services, based on [the WebTrust Principles and Criteria for Certification Authorities – Code Sign Baseline Requirements v3.x.³³³

Our independence and quality control³³⁴

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³³⁵

330 Replace with list of Root and Subordinate CAs in scope for the EC Code Signing Service Requirements or reference to an appendix, if this is different to the CAs in scope for the CS Requirements. If the in-scope CAs are the same for both the CS Requirements and the EV Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to “Reporting Guidance” section.

331 Delete if separate WebTrust for Network Security Report is issued.

332 Statement can be used rather than assertion throughout if desired.

333 Include applicable version number and hyperlink to the criteria document.

334 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

335 Use this paragraph for engagements beginning before December 15, 2022.

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³³⁶

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion³³⁷ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s assertion³³⁸ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s CS [and EVCS]³³⁹ certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of CS [and EVCS] certificates, CS [and EVCS] Signing Authority certificates, and CS [and EVCS] Timestamp Authority certificates [and obtaining an understanding of ABC-CA’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum];³⁴⁰
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We did not perform any procedures regarding the operating effectiveness of the aforementioned controls for any period and, accordingly, do not express an opinion thereon.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The suitability of the design of the controls at ABC-CA 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 suitability of the design of the controls at individual subscriber and relying party locations.

³³⁶ Use this paragraph for engagements beginning on or after December 15, 2022.

³³⁷ Statement can be used rather than assertion throughout if desired.

³³⁸ Statement can be used rather than assertion throughout if desired.

³³⁹ If applicable.

³⁴⁰ Delete if separate WebTrust for Network Security Report is issued.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management’s assertion,³⁴¹ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – for Certification Authorities – Code Sign Baseline Requirements 32.x.

This report does not include any representation as to the quality of ABC-CA’s services other than its *CA operations at <LOCATION>*,³⁴² nor the suitability of any of ABC-CA’s services for any customer’s intended purpose.

Firm Name
City, State/Province, Country
Report Date

341 Statement can be used rather than assertion throughout if desired.

342 CA processing locations as defined in the “Reporting Guidance” section.

Example CA4.3 - Unqualified opinion, direct engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. ("ABC-CA"):

Scope³⁴³

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,³⁴⁴ whether ABC-CA has

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]³⁴⁵
 including its commitment to provide CS certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.
- maintained effective controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x.³⁴⁶
- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]]³⁴⁷ maintained effective controls to provide reasonable assurance that:
 - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;

343 Subheadings are optional and can be removed if desired.

344 CA processing locations as defined in the "Reporting Guidance" section.

345 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

346 Include applicable version number and hyperlink to the criteria document.

347 Replace with list of Root and Subordinate CAs in scope for the EC Code Signing Service Requirements or reference to an appendix, if this is different to the CAs in scope for the CS Requirements. If the in-scope CAs are the same for both the CS Requirements and the EV Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to "Reporting Guidance" section.

- The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [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 that are incorporated by reference.³⁴⁸]

throughout the period <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope] in accordance with the WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements v3.x.

Certification Authority’s responsibilities

ABC-CA’s management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements v3.x.

Our independence and quality control³⁴⁹

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³⁵⁰

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³⁵¹

Practitioner’s responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management’s disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – Authorities – Code Signing Baseline Requirements v3.x., based on our

348 Delete if separate WebTrust for Network Security Report is issued.

349 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

350 Use this paragraph for engagements beginning before December 15, 2022.

351 Use this paragraph for engagements beginning on or after December 15, 2022.

procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s disclosures and controls conform to the WebTrust Criteria, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s CS [and EVCS]³⁵² certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of CS [and EVCS] certificates, CS [and EVCS] Signing Authority certificates, and CS [and EVCS] Timestamp Authority certificates [and obtaining an understanding of ABC-CA’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum],³⁵³
2. selectively testing transactions executed in accordance with disclosed CS [and EVCS] certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA has, in all material respects:

- disclosed its code signing (“CS”) certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and

352 If applicable.

353 Delete if separate WebTrust for Network Security Report is issued.

- [name and version of certificate policy(ies) (if applicable)]³⁵⁴
including its commitment to provide CS certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.
- maintained effective controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x.³⁵⁵
- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]]³⁵⁶ maintained effective controls to provide reasonable assurance that:
 - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [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 that are incorporated by reference.³⁵⁷]

throughout the period <DATE> to <DATE> in accordance with the WebTrust Principles and Criteria for Certification Authorities - Publicly Trusted Code Signing Code Signing Baseline Requirements v3.x. This report does not include any representation as to the quality of ABC-CA's services other than its *Certification Authority (CA) operations at <LOCATION>*,³⁵⁸ nor the suitability of any of ABC-CA's services for any customer's intended purpose.

354 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

355 Include applicable version number and hyperlink to the criteria document.

356 Replace with list of Root and Subordinate CAs in scope for the EC Code Signing Service Requirements or reference to an appendix, if this is different to the CAs in scope for the CS Requirements. If the in-scope CAs are the same for both the CS Requirements and the EV Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to "Reporting Guidance" section.

357 Delete if separate WebTrust for Network Security Report is issued.

358 CA processing locations as defined in the "Reporting Guidance" section.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities - Code Signing 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.]³⁵⁹

Firm Name
City, State/Province, Country
Report Date

359 Remove bracketed text if a seal is not issued.

Management's Assertion

Example MA4.1 - Management's assertion,³⁶⁰ period of time

ABC-CA MANAGEMENT'S ASSERTION³⁶¹

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority ("CA") services for the root and other CAs in scope enumerated in Attachment A, and provides code signing ("CS") CA services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its code signing services, including [its network and certificate security system controls],³⁶² its code signing business practices disclosure on its website, code signing key lifecycle management controls, and 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 ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CS CA services. Based on that assessment, in ABC-CA management's opinion, in providing its CS CA services at <LOCATION>, throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]³⁶³

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

- maintained effective controls to provide reasonable assurance that:

³⁶⁰ Statement can be used rather than assertion throughout if desired.

³⁶¹ Statement can be used rather than assertion throughout if desired.

³⁶² Delete if separate WebTrust for Network Security Report is issued.

³⁶³ At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

- CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
- The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.
- maintained effective controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x.³⁶⁴
- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]]³⁶⁵ maintained effective controls to provide reasonable assurance that:
 - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [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 that are incorporated by reference.³⁶⁶]

throughout the period <DATE> to <DATE> in accordance with the WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements v3.x.

<Signoff Name and Title>

<Date that matches the assurance opinion date>

³⁶⁴ Include applicable version number and hyperlink to the criteria document.

³⁶⁵ Replace with list of Root and Subordinate CAs in scope for the EC Code Signing Service Requirements or reference to an appendix, if this is different to the CAs in scope for the CS Requirements. If the in-scope CAs are the same for both the CS Requirements and the EV Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to “Reporting Guidance” section.

³⁶⁶ Delete if separate WebTrust for Network Security Report is issued.

Example MA4.1 – Management’s assertion,³⁶⁷ point in time

ABC-CA MANAGEMENT’S ASSERTION³⁶⁸

ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (“CA”) services for the root and other CAs in scope enumerated in Attachment A, and provides code signing (“CS”) CA services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its code signing services, including [its network and certificate security system controls],³⁶⁹ its code signing business practices disclosure on its website, code signing key lifecycle management controls, and 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 ABC-CA’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CS CA services. Based on that assessment, in ABC-CA management’s opinion, in providing its CS CA services at <LOCATION>,³⁷⁰ as of <DATE>, ABC-CA has:

- disclosed its code signing (“CS”) certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]³⁷¹

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

- suitably designed, and placed into operation, controls to provide reasonable assurance that:

³⁶⁷ Statement can be used rather than assertion throughout if desired.

³⁶⁸ Statement can be used rather than assertion throughout if desired.

³⁶⁹ Delete if separate WebTrust for Network Security Report is issued.

³⁷⁰ CA processing locations as defined in the “Reporting Guidance” section.

³⁷¹ At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
- The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.
- suitably designed, and placed into operation, controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x
- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]]³⁷² suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.³⁷³]

throughout the period <DATE> to <DATE> in accordance with the WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements v3.x.

<Signoff Name and Title>

<Date that matches the assurance opinion date>

³⁷² Replace with list of Root and Subordinate CAs in scope for the EC Code Signing Service Requirements or reference to an appendix, if this is different to the CAs in scope for the CS Requirements. If the in-scope CAs are the same for both the CS Requirements and the EV Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to "Reporting Guidance" section.

³⁷³ Delete if separate WebTrust for Network Security Report is issued.

WebTrust for Certification Authorities – Network Security (“NS”)

International Standards – ISAE 3000

Example IN5.1 – Unqualified opinion, attestation engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope³⁷⁴

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{375, 376} that for its Certification Authority (CA) operations at <LOCATION>,³⁷⁷ throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for Network Security Requirements], ABC-CA has:

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.³⁷⁸

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,³⁷⁹ including the fairness of its presentation, and the provision of its described services in accordance the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.

374 Subheadings are optional and can be removed if desired.

375 Hyperlink to assertion.

376 Statement can be used rather than assertion throughout if desired.

377 CA processing locations as defined in the “Reporting Guidance” section.

378 Include applicable version number and hyperlink to the criteria document.

379 Statement can be used rather than assertion throughout if desired.

Our independence and quality control³⁸⁰

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³⁸¹

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³⁸²

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion³⁸³ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s assertion³⁸⁴ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
2. testing and evaluating the operating effectiveness of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

380 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

381 Use this paragraph for engagements beginning before December 15, 2022.

382 Use this paragraph for engagements beginning on or after December 15, 2022.

383 Statement can be used rather than assertion throughout if desired.

384 Statement can be used rather than assertion throughout if desired.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management’s assertion,³⁸⁵ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.

This report does not include any representation as to the quality of ABC-CA’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x, nor the suitability of any of ABC-CA’s services for any customer’s intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA’s use of the WebTrust for Certification Authorities –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.]³⁸⁶

Firm Name
City, State/Province, Country
Report Date

385 Statement can be used rather than assertion throughout if desired.

386 Remove bracketed text if a seal is not issued.

Example IN5.2 – Unqualified opinion, attestation engagement, point in time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope³⁸⁷

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion³⁸⁸ that for its Certification Authority (CA) operations at <LOCATION>,³⁸⁹ as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope Network Security Requirements], ABC-CA has:

- suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.³⁹⁰

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,³⁹¹ including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.

Our independence and quality control³⁹²

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³⁹³

387 Subheadings are optional and can be removed if desired.

388 Hyperlink to assertion.

389 CA processing locations as defined in the “Reporting Guidance” section.

390 Include applicable version number and hyperlink to the criteria document.

391 Statement can be used rather than assertion throughout if desired.

392 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

393 Use this paragraph for engagements beginning before December 15, 2022.

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]³⁹⁴

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion³⁹⁵ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s assertion³⁹⁶ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ABC-CA’s controls, individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The suitability of the design of the controls at ABC-CA 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 suitability of the design of the controls at individual subscriber and relying party locations.

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 unauthorised access to systems

394 Use this paragraph for engagements beginning on or after December 15, 2022.

395 Statement can be used rather than assertion throughout if desired.

396 Statement can be used rather than assertion throughout if desired.

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.

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,³⁹⁷ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

³⁹⁷ Statement can be used rather than assertion throughout if desired.

Example IN5.3 – Unqualified opinion, direct engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope³⁹⁸

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,³⁹⁹ whether ABC-CA has

- 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

throughout the period <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for Network Security Requirements]

Certification authority’s responsibilities

ABC-CA’s management is responsible for its controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.⁴⁰⁰

Our independence and quality control⁴⁰¹

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴⁰²

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive

398 Subheadings are optional and can be removed if desired.

399 CA processing locations as defined in the “Reporting Guidance” section.

400 Include applicable version number and hyperlink to the criteria document.

401 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

402 Use this paragraph for engagements beginning before December 15, 2022.

system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴⁰³

Practitioner’s responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management’s controls with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x, based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s controls conform to the WebTrust Criteria, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
2. testing and evaluating the operating effectiveness of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA has, in all material respects

403 Use this paragraph for engagements beginning on or after December 15, 2022.

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Network Security v1.x.

This report does not include any representation as to the quality of ABC-CA’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - Network Security v1.x, nor the suitability of any of ABC-CA’s services for any customer’s intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA’s 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.]⁴⁰⁴

Firm Name
City, State/Province, Country
Report Date

404 Remove bracketed text if a seal is not issued.

Management’s Assertion

Example MA5.1 – Management’s assertion,⁴⁰⁵ period of time

ABC-CA MANAGEMENT’S ASSERTION⁴⁰⁶

ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope for Network Security Requirements] and provides SSL [and non-SSL]⁴⁰⁷ CA services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its SSL [and non-SSL]⁴⁰⁸ CA operations, including its network and certificate security system 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 ABC-CA’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its controls over its CA services. Based on that assessment, in providing its SSL [and non-SSL]⁴⁰⁹ Certification Authority (CA) services at <LOCATION>,⁴¹⁰ throughout the period <DATE> to <DATE>, ABC-CA has:

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.⁴¹¹

<Signoff Name and Title>

<Date that matches the assurance opinion date>

405 Statement can be used rather than assertion throughout if desired.

406 Statement can be used rather than assertion throughout if desired.

407 If applicable, otherwise delete.

408 If applicable, otherwise delete.

409 If applicable, otherwise delete.

410 CA processing locations as defined in the “Reporting Guidance” section.

411 Include applicable version number and hyperlink to the criteria document.

Example MA2.2 - Management’s assertion,⁴¹² point in time

ABC-CA MANAGEMENT’S ASSERTION⁴¹³

ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope] and provides SSL [and non-SSL]⁴¹⁴ CA services.

The management of ABC-CA is responsible for establishing controls over its SSL [and non-SSL]⁴¹⁵ CA operations, including its network and certificate security system 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, controls placed into operation can only provide reasonable assurance with respect to ABC-CA’s Certification Authority operations.

ABC-CA management has assessed its controls over its CA services. Based on that assessment, in providing its SSL [and non-SSL]⁴¹⁶ Certification Authority (CA) services at <LOCATION>,⁴¹⁷ as of <DATE>, ABC-CA has:

- suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Network Security v1.x.⁴¹⁸

<Signoff Name and Title>

<Date that matches the assurance opinion date>

412 Statement can be used rather than assertion throughout if desired.

413 Statement can be used rather than assertion throughout if desired.

414 If applicable, otherwise delete.

415 If applicable, otherwise delete.

416 If applicable, otherwise delete.

417 CA processing locations as defined in the “Reporting Guidance” section.

418 Include applicable version number and hyperlink to the criteria document.

WebTrust for Certification Authorities – S/MIME Certificates (“S/MIME”)

International Standards – ISAE 3000

Example IN6.1 – Unqualified opinion, attestation engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CAs”):

Scope⁴¹⁹

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{420, 421} that for its Certification Authority (CA) operations at <LOCATION>,⁴²² throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for S/MIME Baseline Requirements [and Network Security Requirements]],⁴²³ ABC-CA has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],⁴²⁴

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

- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- maintained effective controls to provide reasonable assurance that:

419 Subheadings are optional and can be removed if desired.

420 Hyperlink to assertion.

421 Statement can be used rather than assertion throughout if desired.

422 CA processing locations as defined in the “Reporting Guidance” section.

423 Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the SSL Baseline Requirements (and Network Security. Refer to “Reporting Guidance” section.

424 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- 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 that are incorporated by reference]⁴²⁵

in accordance with the WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.x.⁴²⁶

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,⁴²⁷ including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.x.

Our independence and quality control⁴²⁸

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴²⁹

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴³⁰

425 Delete if separate WebTrust for Network Security Report is issued.

426 Include applicable version number and hyperlink to the criteria document.

427 Statement can be used rather than assertion throughout if desired.

428 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

429 Use this paragraph for engagements beginning before December 15, 2022.

430 Use this paragraph for engagements beginning on or after December 15, 2022.

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion⁴³¹ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s assertion⁴³² is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates, [and obtaining an understanding of ABC-CA’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum],⁴³³
2. selectively testing transactions executed in accordance with disclosed S/MIME certificate lifecycle management practices];⁴³⁴
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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

431 Statement can be used rather than assertion throughout if desired.

432 Statement can be used rather than assertion throughout if desired.

433 Delete if separate WebTrust for Network Security Report is issued.

434 Delete bracketed text if not covering the SSL Baseline Requirements.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management’s assertion,⁴³⁵ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.x.

This report does not include any representation as to the quality of ABC-CA’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.x, nor the suitability of any of ABC-CA’s services for any customer’s intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA’s use of the WebTrust for Certification Authorities - S/MIME Certificates 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.]⁴³⁶

Firm Name
City, State/Province, Country
Report Date

435 Statement can be used rather than assertion throughout if desired.

436 Remove bracketed text if a seal is not issued.

Example IN6.2 – Unqualified opinion, attestation engagement, point in time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope⁴³⁷

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{438, 439} that for its Certification Authority (CA) operations at <LOCATION>,⁴⁴⁰ as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope]],⁴⁴¹ ABC-CA has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],⁴⁴²

including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirement on the ABC-CA website, and provided such services in accordance with its disclosed practices

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- suitably designed, and placed into operation, 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

437 Subheadings are optional and can be removed if desired.

438 Hyperlink to assertion.

439 Statement can be used rather than assertion throughout if desired.

440 CA processing locations as defined in the “Reporting Guidance” section.

441 Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the SSL Baseline Requirements (and Network Security. Refer to “Reporting Guidance” section.

442 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.⁴⁴³]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.⁴⁴⁴

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,⁴⁴⁵ including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.

Our independence and quality control⁴⁴⁶

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴⁴⁷

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴⁴⁸

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion⁴⁴⁹ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews*

443 Delete if separate WebTrust for Network Security Report is issued.

444 Include applicable version number and hyperlink to the criteria document.

445 Statement can be used rather than assertion throughout if desired.

446 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

447 Use this paragraph for engagements beginning before December 15, 2022.

448 Use this paragraph for engagements beginning on or after December 15, 2022.

449 Statement can be used rather than assertion throughout if desired.

of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s assertion⁴⁵⁰ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA’s S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates, [and obtaining an understanding of ABC-CA’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum],⁴⁵¹
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ABC-CA’s controls, individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The suitability of the design of the controls at ABC-CA 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 suitability of the design of the controls at individual subscriber and relying party locations.

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 unauthorised 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.

Opinion

In our opinion, as of <DATE>, ABC-CA management’s assertion,⁴⁵² as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.

450 Statement can be used rather than assertion throughout if desired.

451 Delete if separate WebTrust for Network Security Report is issued.

452 Statement can be used rather than assertion throughout if desired.

This report does not include any representation as to the quality of ABC-CA’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x, nor the suitability of any of ABC-CA’s services for any customer’s intended purpose.

Firm Name
City, State/Province, Country
Report Date

Example IN6.3 – Unqualified opinion, direct engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope⁴⁵³

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,⁴⁵⁴ whether ABC-CA has

- disclosed its S/MIME certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],⁴⁵⁵
 including its commitment to provide S/MIME certificates in conformity with the CA/ Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- 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 that are incorporated by reference.⁴⁵⁶]

throughout the period <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.

453 Subheadings are optional and can be removed if desired.

454 CA processing locations as defined in the “Reporting Guidance” section.

455 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

456 Delete if separate WebTrust for Network Security Report is issued.

Certification authority’s responsibilities

ABC-CA’s management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.⁴⁵⁷

Our independence and quality control⁴⁵⁸

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴⁵⁹

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴⁶⁰

Practitioner’s responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management’s disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x, based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s disclosures and controls conform to the WebTrust Criteria, and, accordingly, included:

457 Include applicable version number and hyperlink to the criteria document.

458 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

459 Use this paragraph for engagements beginning before December 15, 2022.

460 Use this paragraph for engagements beginning on or after December 15, 2022.

1. obtaining an understanding of ABC-CA’s S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates, [and obtaining an understanding of ABC-CA’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum],⁴⁶¹
2. selectively testing transactions executed in accordance with disclosed S/MIME certificate lifecycle management 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA has, in all material respects:

- disclosed its S/MIME certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],⁴⁶²

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

⁴⁶¹ Delete if separate WebTrust for Network Security Report is issued.

⁴⁶² At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- 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 that are incorporated by reference.⁴⁶³]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.

This report does not include any representation as to the quality of ABC-CA’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x, nor the suitability of any of ABC-CA’s services for any customer’s intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA’s use of the WebTrust for Certification Authorities – S/MIME Certificates 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.]⁴⁶⁴

Firm Name
City, State/Province, Country
Report Date

⁴⁶³ Delete if separate WebTrust for Network Security Report is issued.

⁴⁶⁴ Remove bracketed text if a seal is not issued.

Management’s Assertion

Example MA6.1 – Management’s assertion,⁴⁶⁵ period of time

ABC-CA MANAGEMENT’S ASSERTION⁴⁶⁶

ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope]⁴⁶⁷ and provides S/MIME CA services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including [its network and certificate security system controls],⁴⁶⁸ its S/MIME CA business practices disclosure on its website [or other repository location, S/MIME key lifecycle management controls, and S/MIME 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 ABC-CA’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its [disclosures of its certificate practices and controls over its EV S/MIME CA services. Based on that assessment, in providing its S/MIME CA services at <LOCATION>,⁴⁶⁹ throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],⁴⁷⁰

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

- maintained effective controls to provide reasonable assurance that:

465 Statement can be used rather than assertion throughout if desired.

466 Statement can be used rather than assertion throughout if desired.

467 Replace with list of Root and Subordinate CAs in scope for the SSL Baseline Requirements and Network Security Requirements or reference to an appendix. Refer to “Reporting Guidance” section.

468 Delete if separate WebTrust for Network Security Report is issued.

469 CA processing locations as defined in the “Reporting Guidance” section.

470 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
- S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- 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 that are incorporated by reference]⁴⁷¹

in accordance with the WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.x.⁴⁷²

<Signoff Name and Title>

<Date that matches the assurance opinion date>

471 Delete if separate WebTrust for Network Security Report is issued.

472 Include applicable version number and hyperlink to the criteria document.

Example MA6.2 - Management’s assertion,⁴⁷³ point in time

ABC-CA MANAGEMENT’S ASSERTION⁴⁷⁴

ABC Certification Authority, Inc. (“ABC-CA”) operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope⁴⁷⁵ and provides S/MIME CA services.

The management of ABC-CA is responsible for establishing controls over its S/MIME CA operations, including [its network and certificate security system controls],⁴⁷⁶ its S/MIME CA business practices disclosure on its website [or other repository location],⁴⁷⁷ S/MIME key lifecycle management controls, and S/MIME 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, controls placed into operation can only provide reasonable assurance with respect to ABC-CA’s Certification Authority operations.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its S/MIME CA services. Based on that assessment, in ABC-CA management’s opinion, in providing its S/MIME Certification Authority (CA) services at <LOCATION>,⁴⁷⁸ as of <DATE>, ABC-CA has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)],⁴⁷⁹
 including its commitment to provide S/MIME certificates in conformity with the CA/ Browser Forum Requirement on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:

⁴⁷³ Statement can be used rather than assertion throughout if desired.

⁴⁷⁴ Statement can be used rather than assertion throughout if desired.

⁴⁷⁵ Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to “Reporting Guidance” section.

⁴⁷⁶ Delete if separate WebTrust for Network Security Report is issued.

⁴⁷⁷ Link to business practices repository location and describe location if not website (i.e. intranet).

⁴⁷⁸ CA processing locations as defined in the “Reporting Guidance” section.

⁴⁷⁹ At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
- S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- suitably designed, and placed into operation, 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
- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference]⁴⁸⁰

in accordance with the WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.x.⁴⁸¹

<Signoff Name and Title>

<Date that matches the assurance opinion date>

480 Delete if separate WebTrust for Network Security Report is issued.

481 Include applicable version number and hyperlink to the criteria document.

Lifecycle Reports

In addition to the reports discussed in the prior section, the Browser community, as part of their trusted root programs, are requesting reports covering key components of a root key's lifecycle. Included in this section are reports covering:

- Root Key Generation Ceremony
- key lifecycle events
 - key back up, storage and recovery
 - key usage for intended functions
 - key destruction
 - key transport

International Standards – ISAE 3000

Example IN7.1 – Root key generation ceremony, attestation engagement

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope⁴⁸²

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{483, 484} that in generating and protecting its [list of Root CAs witnessed] (collectively, “ABC-CA Root CAs”) on <DATE>⁴⁸⁵ at <LOCATION>,⁴⁸⁶ with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
ABC-CA Root CA 1	0a:4b:33:d1:f9:a8:9f:33:12:00:ab	14:2b:c7:d1
ABC-CA Root CA 2	8f:7d:c4:33:19:0a:0b:de:f1:42:11	1b:23:d4:f2

ABC-CA has:

- followed the CA key generation and protection requirements in its:
 - [name and version of certification practice statement]; and
 - [name and version of certificate policy (if applicable)]⁴⁸⁷
- included appropriate, detailed procedures and controls in its Root Key Generation Script(s):
 - [name, version number, and date of root key generation script(s). This may also include additional scripts such as server build scripts]
- maintained effective controls to provide reasonable assurance that the ABC-CA Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Script(s)

⁴⁸² Subheadings are optional and can be removed if desired.

⁴⁸³ Hyperlink to assertion.

⁴⁸⁴ Statement can be used rather than assertion throughout if desired.

⁴⁸⁵ Date of witnessing. This can be a range of dates if the ceremony spanned multiple days.

⁴⁸⁶ Location of the key generation ceremony.

⁴⁸⁷ At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- performed, during the root key generation process, all procedures required by the Root Key Generation Script(s)
- generated the CA keys in a physically secured environment as described in its CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x.⁴⁸⁸

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,⁴⁸⁹ including the fairness of its presentation, and for generating and protecting its CA keys in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control⁴⁹⁰

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴⁹¹

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁴⁹²

488 Include applicable version number and hyperlink to the criteria document.

489 Statement can be used rather than assertion throughout if desired.

490 For engagements beginning on or after December 15, 2022 replace with "Our independence and quality management".

491 Use this paragraph for engagements beginning before December 15, 2022.

492 Use this paragraph for engagements beginning on or after December 15, 2022.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion⁴⁹³ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion⁴⁹⁴ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's documented plan of procedures to be performed for the generation of the certification authority key pairs for the ABC-CA Root CAs;
2. reviewing the detailed CA key generation script(s) for conformance with industry standard practices;
3. testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;
4. physical observation of all procedures performed during the root key generation process to ensure that the procedures actually performed on <DATE> were in accordance with the Root Key Generation Script(s) for the ABC-CA Root CAs; and
5. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,⁴⁹⁵ as referred to above, is fairly stated, in all material respects, in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

493 Statement can be used rather than assertion throughout if desired.

494 Statement can be used rather than assertion throughout if desired.

495 Statement can be used rather than assertion throughout if desired.

Management's Assertion

Example MA7.1 – Management's assertion⁴⁹⁶

ABC-CA MANAGEMENT'S ASSERTION⁴⁹⁷

ABC Certification Authority, Inc. ("ABC-CA") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs known as [list of Root CAs witnessed] (collectively, "ABC-CA Root CAs"). These CA's will serve as Root CAs for client certificate services. In order to allow the CA's to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's private signing key. This helps assure the non-refutability of the integrity of the ABC-CA Root CAs' key pairs, and in particular, the private signing keys.

ABC-CA management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in ABC-CA's Certificate Policy (CP) [and/or] Certification Practice Statement (CPS), and its Root Key Generation Script(s), which are in accordance with [based on]⁴⁹⁸ CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x.⁴⁹⁹

ABC-CA management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

ABC-CA management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the ABC-CA Root CAs, and for the CA environment controls relevant to the generation and protection of its CA keys.

ABC-CA management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys for the ABC-CA Root CA's on <DATE>⁵⁰⁰ at <LOCATION>,⁵⁰¹ with the following identifying information:

496 Statement can be used rather than assertion throughout if desired.

497 Statement can be used rather than assertion throughout if desired.

498 Use "in accordance with" for Canadian and International standards. Use "based on" for US standards.

499 Include applicable version number and hyperlink to the criteria document.

500 Date of witnessing. This can be a range of dates if the ceremony spanned multiple days.

501 Location of the key generation ceremony.

Root Name	Subject Key Identifier	Certificate Serial Number
ABC-CA Root CA 1	0a:4b:33:d1:f9:a8:9f:33:12:00:ab	14:2b:c7:d1
ABC-CA Root CA 2	8f:7d:c4:33:19:0a:0b:de:f1:42:11	1b:23:d4:f2

ABC-CA has:

- followed the CA key generation and protection requirements in its:
 - [name and version of certification practice statement]; and
 - [name and version of certificate policy (if applicable)]⁵⁰²
- included appropriate, detailed procedures and controls in its Root Key Generation Script(s):
 - [name, version number, and date of root key generation script(s). This may also include additional scripts such as server build scripts]
- maintained effective controls to provide reasonable assurance that the ABC-CA Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Script(s)
- performed, during the root key generation process, all procedures required by the Root Key Generation Script(s)
- generated the CA keys in a physically secured environment as described in its CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x.⁵⁰³

<Signoff Name and Title>

<Date that matches the assurance opinion date>

502 At least of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

503 Include applicable version number and hyperlink to the criteria document.

Reporting on Life Cycle

International Standards – ISAE 3000

Example CA7.2 – Unqualified opinion, attestation engagement (for various lifecycle events), period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope⁵⁰⁴

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion⁵⁰⁵ that in managing the key lifecycle events for its Certification Authority (“CA”) private keys and/or key pairs (include if applicable keys not yet associated with a specific CA) contained on assets at <LOCATION(S)>,⁵⁰⁶ throughout the period <DATE> to <DATE> for its CA keys enumerated in Attachment A,⁵⁰⁷ ABC CA has:

- disclosed its key lifecycle management requirements in its
 - [name and version of certification practice statement(s)]; and
 - [name and version of its certificate policy(ies) (if applicable)]
 and followed such key lifecycle management requirements.

[if WTCA criteria 4.2 is applicable]⁵⁰⁸

- maintained effective controls to provide reasonable assurance that keys are backed up, stored, and recovered by authorized personnel in trusted roles using multiple person control in a physically secured environment

[if WTCA criteria 4.4 is applicable]

- maintained effective controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations

504 Subheadings are optional and can be removed if desired.

505 Statement can be used rather than assertion throughout if desired.

506 Include applicable locations based on the criteria in-scope.

507 List in-scope CA keys or other key pair identifiers.

508 Include only those criteria applicable to the current reporting.

[if WTCA criteria 4.6 is applicable]

- maintained controls to provide reasonable assurance that:
 - copies of keys that no longer serve a valid business purpose are destroyed in accordance with ABC CA's disclosed business practices; and
 - copies of keys are completely destroyed at the end of the key pair life cycle in accordance with ABC CA's disclosed business practices

[if WTCA criteria 4.8 is applicable]

- maintained effective controls to provide reasonable assurance that:
 - devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity;
 - access to CA cryptographic hardware is limited to authorized personnel in trusted roles using multiple person control; and
 - CA cryptographic hardware is functioning correctly

[if WTCA 4.10 criteria is applicable]

- maintained effective controls to provide reasonable assurance that:
 - private keys that are physically transported from one facility to another remain confidential and maintain their integrity;
 - hardware containing keys and associated activation materials are prepared for transport in a physically secure environment by authorized personnel in trusted roles using multiple person controls, and are transported within sealed tamper evident packaging;
 - keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and
 - key transportation events are logged

[if WTCA 4.11 criteria is applicable]

- maintained effective controls to provide reasonable assurance that:
 - keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration, are completed in a physically secure environment by authorized personnel in trusted roles using multiple person control;
 - hardware and software tools used during the key migration process are tested by authorized personnel in trusted roles using multiple person controls prior to the migration event; and
 - key migration events follow a documented script and are logged

in accordance with the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11⁵⁰⁹ of the WebTrust Principles and Criteria for Certification Authorities v2.x.⁵¹⁰

Certification Authority's responsibilities

ABC-CA's management is responsible for its assertion,⁵¹¹ including the fairness of its presentation, and the provision of its described services in accordance with the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11⁵¹² of the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control⁵¹³

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁵¹⁴

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁵¹⁵

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion⁵¹⁶ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance

509 Include only those criteria that are applicable to the current reporting.

510 Hyperlink to the current version of the WebTrust Principles and Criteria for Certification Authorities.

511 Statement can be used rather than assertion throughout if desired.

512 Include only those criteria that are applicable to the current reporting.

513 For engagements beginning on or after December 15, 2022 replace with "Our independence and quality management".

514 Use this paragraph for engagements beginning before December 15, 2022.

515 Use this paragraph for engagements beginning on or after December 15, 2022.

516 Statement can be used rather than assertion throughout if desired.

Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion⁵¹⁷ is fairly stated, and, accordingly, included:

- obtaining an understanding of ABC CA's documented plan of procedures to be performed for the key lifecycle management.
- reviewing the detailed key logs for conformance with industry standard practices and disclosed practices in the Certificate Policy and Certification Practice Statement.
- testing and evaluating the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the service.
- performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,⁵¹⁸ as referred to above, is fairly stated, in all material respects, in accordance with the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11⁵¹⁹ of the WebTrust Principles and Criteria for Certification Authorities v2.x.⁵²⁰

517 Statement can be used rather than assertion throughout if desired.

518 Statement can be used rather than assertion throughout if desired.

519 Include only those criteria that are applicable to the current reporting.

520 Hyperlink to the current version of the WebTrust Principles and Criteria for Certification Authorities.

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*,⁵²¹ nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

521 CA processing locations as defined in the "Reporting Guidance" section.

Attachment A - CAs in-scope for key lifecycle management activities⁵²²**CA KEYS STORED, BACKUP, AND RECOVERED IN <LOCATION(S)>⁵²³**

CA Subject Name	Subject Key Identifier	Certificate Serial Number	SHA256 Thumbprint

KEY DESTRUCTION

CA Subject Name	Subject Key Identifier	Certificate Serial Number	SHA256 Thumbprint

KEYS TRANSPORTED / MIGRATED FROM <LOCATION(S)>⁵²⁴ TO <LOCATION(S)>⁵²⁵

CA Subject Name	Subject Key Identifier	Certificate Serial Number	SHA256 Thumbprint

522 The tables below are provided as examples, but each CA should specify the level of detail they wish to disclose based on the needs of the users.

523 Include applicable location(s).

524 Include applicable location(s).

525 Include applicable location(s).

Management's Assertion⁵²⁶

Example MA7.2 – Management's assertion⁵²⁷ on life cycle

ABC-CA MANAGEMENT'S ASSERTION⁵²⁸

ABC CA, Inc. ("ABC CA") has deployed a public key infrastructure. As part of this deployment, it was necessary to implement and maintain effective key lifecycle management controls in managing the key lifecycle events of its Certification Authority ("CA") private keys and key pairs (include if applicable keys not yet associated with a specific CA) to ensure the integrity, confidentiality, and availability of private keys contained in assets at <LOCATION(S)>⁵²⁹ throughout the period January 1, 2XXX to December 31, 2XXX for its CA keys enumerated in Attachment A.⁵³⁰

The keys were managed in accordance with key lifecycle management requirements described in the Certificate Policy and Certification Practice Statement.

ABC CA management has maintained effective CA Key Lifecycle Management Controls based on the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11⁵³¹ of the WebTrust Principles and Criteria for Certification Authorities v2.x.⁵³² These controls were designed to provide reasonable assurance of adherence to these practices throughout the key lifecycle management process.

ABC CA management is responsible for establishing and maintaining procedures over its CA Key Lifecycle Management Controls, and over the integrity and confidentiality of all private keys and activation materials (including physical keys, tokens, and passwords) used in the establishment of the ABC CA keys, and for the CA environmental controls relevant to the protection of its keys.

ABC CA management has assessed the procedures and controls for the CA Key Lifecycle Management Controls. Based on that assessment, in management's opinion, in protecting its keys, ABC CA has:

- disclosed its key lifecycle management requirements in its
 - [name and version of certification practice statement(s)]; and
 - [name and version of its certificate policy(ies) (if applicable)]
 and followed such key lifecycle management requirements.

⁵²⁶ Statement can be used rather than assertion throughout if desired.

⁵²⁷ Statement can be used rather than assertion throughout if desired.

⁵²⁸ Statement can be used rather than assertion throughout if desired.

⁵²⁹ Include applicable locations based on the criteria in-scope.

⁵³⁰ List in-scope CA keys or other key pair identifiers.

⁵³¹ Include only those criteria that are applicable to the current reporting.

⁵³² Hyperlink to the current version of the WebTrust Principles and Criteria for Certification Authorities.

[if WTCA 4.2 is applicable]

- maintained effective controls to provide reasonable assurance that keys are backed up, stored, and recovered by authorized personnel in trusted roles using multiple person control in a physically secured environment

[if WTCA 4.4 is applicable]

- maintained effective controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations

[if WTCA 4.6 is applicable]

- maintained controls to provide reasonable assurance that:
 - copies of keys that no longer serve a valid business purpose are destroyed in accordance with ABC CA's disclosed business practices; and
 - copies of keys are completely destroyed at the end of the key pair life cycle in accordance with ABC CA's disclosed business practices

[if WTCA 4.8 is applicable]

- maintained effective controls to provide reasonable assurance that:
 - devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity;
 - access to CA cryptographic hardware is limited to authorized personnel in trusted roles using multiple person control; and
 - CA cryptographic hardware is functioning correctly

[if WTCA 4.10 is applicable]

- maintained effective controls to provide reasonable assurance that:
 - private keys that are physically transported from one facility to another remain confidential and maintain their integrity;
 - hardware containing keys, and associated activation materials, are prepared for transport in a physically secure environment by authorized personnel in trusted roles using multiple person controls, and are transported within sealed tamper evident packaging;
 - keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and
 - keys transportation events are logged

[if WTCA 4.11 is applicable]

- maintained effective controls to provide reasonable assurance that:
 - keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration, are completed in a physically secure environment by authorized personnel in trusted roles using multiple person control;
 - hardware and software tools used during the keys migration process are tested by authorized personnel in trusted roles using multiple person controls prior to the migration event; and
 - keys migration events follow a documented script and are logged

in accordance with the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11⁵³³ of the [WebTrust Principles and Criteria for Certification Authorities v2.x](#).⁵³⁴

<Signoff Name and Title>

<Date that matches the assurance opinion date>

533 Include only those criteria that are applicable to the current reporting.

534 Hyperlink to the current version of the WebTrust Principles and Criteria for Certification Authorities.

WebTrust for Certification Authorities – Verified Mark Certificates

International Standards – ISAE 3000

Example IN8.1 – Unqualified opinion, attestation engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope⁵³⁵

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{536, 537} that for its Certification Authority (CA) operations at <LOCATION>,⁵³⁸ throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],⁵³⁹ ABC-CA has:

- disclosed its Verified Mark (VM) certificate practices and procedures in its
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁵⁴⁰
 including its commitment to provide VM certificates in conformity with the applicable [Minimum Security Requirements for Issuance of Verified Mark Certificates](#) (VMC Guidelines), and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
 - The integrity of CA keys it manages is established and protected throughout their life cycles.

535 Subheadings are optional and can be removed if desired.

536 Hyperlink to assertion.

537 Statement can be used rather than assertion throughout if desired.

538 CA processing locations as defined in the “Reporting Guidance” section.

539 Reference to an appendix or replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to “Reporting Guidance” section.

540 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- 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 that are incorporated by reference.⁵⁴¹]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.⁵⁴²

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,⁵⁴³ including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.

Our independence and quality control⁵⁴⁴

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁵⁴⁵

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive

541 Delete if separate WebTrust for Network Security Report is issued.

542 Include applicable version number and hyperlink to the criteria document.

543 Statement can be used rather than assertion throughout if desired.

544 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

545 Use this paragraph for engagements beginning before December 15, 2022.

system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁵⁴⁶

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion⁵⁴⁷ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion⁵⁴⁸ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's VM certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of VM certificates [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];⁵⁴⁹
2. selectively testing transactions executed in accordance with disclosed VM certificate lifecycle management 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised access to systems

546 Use this paragraph for engagements beginning on or after December 15, 2022.

547 Statement can be used rather than assertion throughout if desired.

548 Statement can be used rather than assertion throughout if desired.

549 Delete if separate WebTrust for Network Security Report is issued.

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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,⁵⁵⁰ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - Verified Mark Certificates v1.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - Verified Mark Certificates v1.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities - Verified Mark Certificates 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.]⁵⁵¹

Firm Name
City, State/Province, Country
Report Date

550 Statement can be used rather than assertion throughout if desired.

551 Remove bracketed text if a seal is not issued.

Example IN8.2 - Unqualified opinion, attestation engagement, point in time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. (“ABC-CA”):

Scope⁵⁵²

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management’s assertion^{553, 554} that for its Certification Authority (CA) operations at <LOCATION>,⁵⁵⁵ as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],⁵⁵⁶ ABC-CA has:

- disclosed its Verified Mark (VM) certificate practices and procedures in its
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁵⁵⁷
 including its commitment to provide VM certificates in conformity with the applicable [Minimum Security Requirements for Issuance of Verified Mark Certificates](#) (VMC Guidelines), and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
 - The integrity of CA keys it manages is established and protected throughout their life cycles.
- suitably designed, and placed into operation, 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

552 Subheadings are optional and can be removed if desired.

553 Hyperlink to assertion.

554 Statement can be used rather than assertion throughout if desired.

555 CA processing locations as defined in the “Reporting Guidance” section.

556 Reference to an appendix or replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to “Reporting Guidance” section.

557 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.⁵⁵⁸]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.⁵⁵⁹

Certification authority’s responsibilities

ABC-CA’s management is responsible for its assertion,⁵⁶⁰ including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.

Our independence and quality control⁵⁶¹

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁵⁶²

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁵⁶³

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion⁵⁶⁴ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews*

558 Delete if separate WebTrust for Network Security Report is issued.

559 Include applicable version number and hyperlink to the criteria document.

560 Statement can be used rather than assertion throughout if desired.

561 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

562 Use this paragraph for engagements beginning before December 15, 2022.

563 Use this paragraph for engagements beginning on or after December 15, 2022.

564 Statement can be used rather than assertion throughout if desired.

of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion⁵⁶⁵ is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's VM certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of VM certificates [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];⁵⁶⁶
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ABC-CA's controls, individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The suitability of the design of the controls at ABC-CA 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 suitability of the design of the controls at individual subscriber and relying party locations.

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 unauthorised 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.

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,⁵⁶⁷ as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.

565 Statement can be used rather than assertion throughout if desired.

566 Delete if separate WebTrust for Network Security Report is issued.

567 Statement can be used rather than assertion throughout if desired.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - Verified Mark Certificates v1.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

Example IN8.3 - Unqualified opinion, direct engagement, period of time

INDEPENDENT ASSURANCE REPORT

To the management of ABC Certification Authority, Inc. ("ABC-CA"):

Scope⁵⁶⁸

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,⁵⁶⁹ whether ABC-CA has

- disclosed its Verified Mark (VM) certificate practices and procedures in its
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁵⁷⁰
 including its commitment to provide VM certificates in conformity with the applicable [Minimum Security Requirements for Issuance of Verified Mark Certificates](#) (VMC Guidelines), and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
 - The integrity of CA keys it manages is established and protected throughout their life cycles.
- 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 that are incorporated by reference.^{571]}

throughout the period <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope] in accordance with the WebTrust Principles and Criteria for Certification Authorities - Verified Mark Certificates v1.x.

568 Subheadings are optional and can be removed if desired.

569 CA processing locations as defined in the "Reporting Guidance" section.

570 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

571 Delete if separate WebTrust for Network Security Report is issued.

Certification authority’s responsibilities

ABC-CA’s management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.⁵⁷²

Our independence and quality control⁵⁷³

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

[The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁵⁷⁴

[The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]⁵⁷⁵

Practitioner’s responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management’s disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x (the “WebTrust Criteria”), based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s disclosures and controls conform to the WebTrust Criteria, and, accordingly, included:

572 Include applicable version number and hyperlink to the criteria document.

573 For engagements beginning on or after December 15, 2022 replace with “Our independence and quality management”.

574 Use this paragraph for engagements beginning before December 15, 2022.

575 Use this paragraph for engagements beginning on or after December 15, 2022.

1. obtaining an understanding of ABC-CA's VM certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of VM certificates [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];⁵⁷⁶
2. selectively testing transactions executed in accordance with disclosed VM certificate lifecycle management 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at ABC-CA 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.

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 unauthorised 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.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA has, in all significant respects:

- disclosed its Verified Mark (VM) certificate practices and procedures in its
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁵⁷⁷

including its commitment to provide VM certificates in conformity with the applicable [Minimum Security Requirements for Issuance of Verified Mark Certificates](#) (VMC Guidelines), and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:

⁵⁷⁶ Delete if separate WebTrust for Network Security Report is issued.

⁵⁷⁷ At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

- VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
- The integrity of CA keys it manages is established and protected throughout their life cycles.
- 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 that are incorporated by reference.⁵⁷⁸]

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Verified Mark Certificates v1.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - Verified Mark Certificates v1.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities - Verified Mark Certificates 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.]⁵⁷⁹

Firm Name
City, State/Province, Country
Report Date

578 Delete if separate WebTrust for Network Security Report is issued.

579 Remove bracketed text if a seal is not issued.

Management's Assertion

Example MA8.1 – Management's assertion,⁵⁸⁰ period of time

ABC-CA MANAGEMENT'S ASSERTION⁵⁸¹

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],⁵⁸² and provides Verified Mark (VM) Certificate services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its VM CA operations, including its VM CA business practices disclosure on its website [or other repository location],⁵⁸³ VM key lifecycle management controls, and VM 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 ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its VM CA services. Based on that assessment, in ABC-CA management's opinion, in providing its Certification Authority (CA) services at <LOCATION>,⁵⁸⁴ throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its Verified Mark (VM) certificate practices and procedures in its
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁵⁸⁵

including its commitment to provide VM certificates in conformity with the applicable [Minimum Security Requirements for Issuance of Verified Mark Certificates](#) (VMC Guidelines), and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:

580 Statement can be used rather than assertion throughout if desired.

581 Statement can be used rather than assertion throughout if desired.

582 Replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to "Reporting Guidance" section.

583 Link to business practices repository location and describe location if not website (i.e., intranet).

584 CA processing locations as defined in the "Reporting Guidance" section.

585 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

- VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
- The integrity of CA keys it manages is established and protected throughout their life cycles.
- 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 that are incorporated by reference.⁵⁸⁶]

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Verified Mark Certificates v1.x.⁵⁸⁷

<Signoff Name and Title>

<Date that matches the assurance opinion date>

586 Delete if separate WebTrust for Network Security Report is issued.

587 Include applicable version number and hyperlink to the criteria document.

Example MA8.2 - Management's assertion,⁵⁸⁸ point in time

ABC-CA MANAGEMENT'S ASSERTION⁵⁸⁹

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],⁵⁹⁰ and provides Verified Mark (VM) Certificate services.

The management of ABC-CA is responsible for establishing controls over its VM CA operations, including its VM CA business practices disclosure on its website [or other repository location],⁵⁹¹ VM key lifecycle management controls, and VM 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, controls placed into operation can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its VM CA services. Based on that assessment, in ABC-CA management's opinion, in providing its Certification Authority (CA) services at <LOCATION>,⁵⁹² as of <DATE>, ABC-CA has:

- disclosed its Verified Mark (VM) certificate practices and procedures in its
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁵⁹³
 including its commitment to provide VM certificates in conformity with the applicable [Minimum Security Requirements for Issuance of Verified Mark Certificates](#) (VMC Guidelines), and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;

588 Statement can be used rather than assertion throughout if desired.

589 Statement can be used rather than assertion throughout if desired.

590 Replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to "Reporting Guidance" section.

591 Link to business practices repository location and describe location if not website (i.e., intranet).

592 CA processing locations as defined in the "Reporting Guidance" section.

593 At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet.

- The integrity of CA keys it manages is established and protected throughout their life cycles.
- suitably designed, and placed into operation, 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
- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.⁵⁹⁴]

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Verified Mark Certificates v1.x.⁵⁹⁵

<Signoff Name and Title>

<Date that matches the assurance opinion date>

594 Delete if separate WebTrust for Network Security Report is issued.

595 Include applicable version number and hyperlink to the criteria document.