CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Webtrust® for Certification Authorities

ILLUSTRATIVE REPORTS – ISAE 3000

Release Date 1 February 2022

Version 2.0

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.

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:

- Jeffrey Ward, BDO USA, LLP (Chair)
- Donald E. Sheehy (Vice-Chair)
- Chris Czajczyc, Deloitte LLP
- David Roque, Ernst & Young LLP
- Zain Shabbir, KPMG LLP

Significant support has been provided by:

- Timothy Crawford, BDO USA, LLP
- Daniel J. Adam, Deloitte & Touche LLP
- Donoghue Clarke, Ernst & Young LLP
- Eric Lin, Ernst & Young LLP

CPA Canada Support

- Kaylynn Pippo, Principal, Research, Guidance and Support
- Gord Beal, Vice President, Research, Guidance and Support
- Anna-Marie Christian, Director Emerging Issues & Strategic Partnerships
- Janet Treasure, Vice President, Member Development and Support
- Bryan Walker, Consultant

Table of Contents

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.

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 parities 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.

If 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 IN1.6.

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"):

Scope[1]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[2] that for its Certification Authority (CA) operations at <LOCATION>[3], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][4], 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][5]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][6]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[7]
- 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 CA processing locations as defined in the "Reporting Guidance" section.

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

5 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.

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

7 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[8].

[(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.][9]

[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.][10]

Certification authority's responsibilities
ABC-CA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control
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

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

9 Remove bracketed text if external RAs are not used.

10 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.

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

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion 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 assertion 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 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, 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.][11]

Firm Name
City, State/Province, Country
Report Date

11 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"):

Scope[12]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[13] that for its Certification Authority (CA) operations at <LOCATION>[14], as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][15], 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][16]
- 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)][17]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[18]
- 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

12 Subheadings are optional and can be removed if desired.

13 Hyperlink to assertion.

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

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

16 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.

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

18 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[19].

[(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.][20]

[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.][21]

Certification authority's responsibilities
ABC-CA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control
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.

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

20 Remove bracketed text if external RAs are not used.

21 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.

Practitioner's responsibilities
Our responsibility is to express an opinion on management's assertion 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 assertion 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.

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, 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

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

INDEPENDENT ASSURANCE REPORT

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

Scope[22]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[23], 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)][24]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][25]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[26]
- 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

22 Subheadings are optional and can be removed if desired.

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

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

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

26 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][27] 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 disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles Criteria for Certification Authorities v2.x.[31]

Our independence and quality control
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.

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

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

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 Include applicable version number and hyperlink to the criteria document.

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 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][32]

32 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:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][33]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[34]
- 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.

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.][35]

Firm Name
City, State/Province, Country
Report Date

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

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

35 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"):

Scope[36]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[37] that for its Certification Authority (CA) operations at <LOCATION>[38], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][39], 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)][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

36 Subheadings are optional and can be removed if desired.

37 Hyperlink to assertion.

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

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

40 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.

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.

- 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[43].

[(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.][44]

[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.][45]

Certification authority's responsibilities
ABC-CA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control
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.

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

44 Remove bracketed text if external RAs are not used.

45 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.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion 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 assertion 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 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, 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

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"):

Scope[46]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[47], 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)][48]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][49]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[50]
- 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

46 Subheadings are optional and can be removed if desired.

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

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

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

50 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][51]in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x[52].

[(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.][53]

[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.][54] 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.[55]

Our independence and quality control
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.

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*

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

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

53 Remove bracketed text if external RAs are not used.

54 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.

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

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 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][56]

56 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:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][57]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[58]
- 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

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

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

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"):

Scope[59]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[60] that, except for matters described in the assertion, for its Certification Authority (CA) operations at <LOCATION>[61], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][62], 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)][63]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][64]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[65]
- 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

59 Subheadings are optional and can be removed if desired.

60 Hyperlink to assertion.

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

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

63 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.

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

65 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[66].

[(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.][67]

[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.][68]

Certification authority's responsibilities
ABC-CA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control
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.

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

67 Remove bracketed text if external RAs are not used.

68 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.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion 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 assertion 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 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	We noted that electronic and auditable dual-custody multi-factor entrance and exit controls to secure PKI area were not implemented. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.4 to not be met.	3.4: The CA maintains controls to provide reasonable assurance that: • 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	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 Principles and Criteria for Certification Authorities v2.0, Criterion 3.8 to not be met.	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: • 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 minimised as a result of the cessation or degradation of the CA's services.

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)][69]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][70]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[71]
- 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

69 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.

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

71 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:D0: 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, period of time

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][72], and provides the following CA services[73]:

- 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][74], 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.

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

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

74 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>[75], 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]][76]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]][77]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[78]
- 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[79], including the following[80]:

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

76 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.

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

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

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

80 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 assertion does not extend to controls that would address those criteria.][81]

<Signoff Name and Title>
<Date that matches the assurance opinion date>

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

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

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][82], and provides the following CA services[83]:

- 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][84], 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.

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>[85], as of <DATE>, ABC-CA has:

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

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

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

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

- 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]
- 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)][87]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[88]
- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x[89], including the following[90]:

CA Business Practices Disclosure

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

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.

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

90 Remove bullets that are not applicable.

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

<Signoff Name and Title>
<Date that matches the assurance opinion date>

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

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][91], and provides the following CA services[92]:

- 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][93], 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.

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

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

93 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	We noted that electronic and auditable dual-custody multi-factor entrance and exit controls to secure PKI area were not implemented. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.4 to not be met.	3.4: The CA maintains controls to provide reasonable assurance that: • 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	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 Principles and Criteria for Certification Authorities v2.0, Criterion 3.8 to not be met.	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: • 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 minimised as a result of the cessation or degradation of the CA's services.

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>[94], 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)][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
  - 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

94 CA processing locations as defined in the "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.

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x[98], including the following[99]:

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

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

99 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 assertion does not extend to controls that would address those criteria.][100]

<Signoff Name and Title>
<Date that matches the assurance opinion date>

100 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 Security

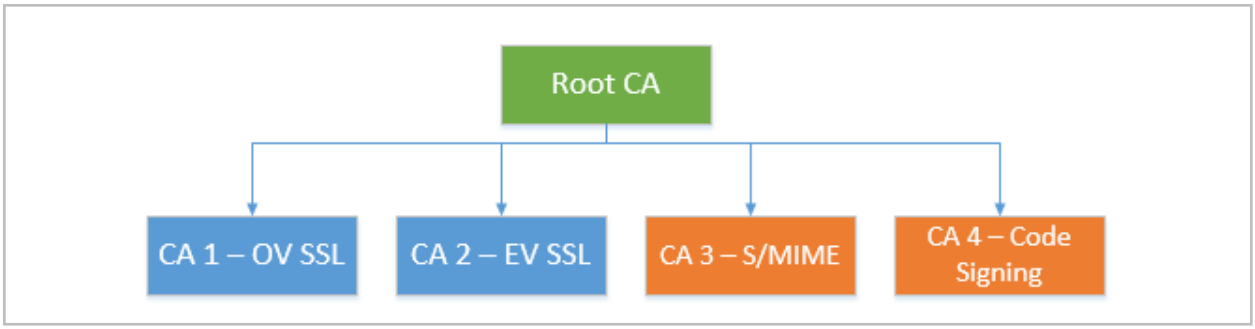
Currently, the SSL Baseline with Network Security principles and criteria incorporates two different CA/Browser Forum requirements documents:

- 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:



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.

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"):

Scope[101]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[102] that for its Certification Authority (CA) operations at <LOCATION>[103], 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]][104], 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)][105],

  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][106]

101 Subheadings are optional and can be removed if desired.

102 Hyperlink to assertion.

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

104 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.

105 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.

106 The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the Network Security Requirements

[And, for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for Network Security Requirements]][107]:

- 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 [Principle 4 of][108] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x [109].

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with [Principle 4 of][110] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x.

Our independence and quality control

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.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion 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 assertion is fairly stated, and, accordingly, included:

107 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.

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

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

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

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][111] obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
2. [selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices][112];
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, as referred to above, is fairly stated, in all material respects, in accordance with [Principle 4 of][113] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by [Principle 4 of][114] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

111 Delete bracketed text if not covering the SSL Baseline Requirements.

112 Delete bracketed text if not covering the SSL Baseline Requirements.

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

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

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.][115]

Firm Name
City, State/Province, Country
Report Date

115 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"):

Scope[116]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[117] that for its Certification Authority (CA) operations at <LOCATION>[118], 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]][119], 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)][120],

  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][121]

116 Subheadings are optional and can be removed if desired.

117 Hyperlink to assertion.

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

119 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.

120 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.

121 The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the Network Security Requirements.

[And, for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for Network Security Requirements]][122]:

- 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 [Principle 4 of][123] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x [124].

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with [Principle 4 of][125] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x.

Our independence and quality control

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.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion 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 assertion is fairly stated, and, accordingly, included:

122 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.

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

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

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

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][126] 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 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, as referred to above, is fairly stated, in all material respects, in accordance with [Principle 4 of][127] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by [Principle 4 of][128] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 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

126 Delete bracketed text if not covering the SSL Baseline Requirements.

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

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

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

INDEPENDENT ASSURANCE REPORT

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

Scope[129]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[130], whether ABC-CA has

a. 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)][131],

   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

b. 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)

c. 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][132]

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,

129 Subheadings are optional and can be removed if desired.

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

131 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.

132 The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the 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]]][133]:

d. 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

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 [Principle 4 of][134] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x.[135]

Our independence and quality control

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.

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with [Principle 4 of][136] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 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:

133 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.

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

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

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

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][137] obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
2. [selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices][138];
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 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)][139],

  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

137 Delete bracketed text if not covering the SSL Baseline Requirements.

138 Delete bracketed text if not covering the SSL Baseline Requirements.

139 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 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][140]

in accordance with [Principle 4 of][141] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x.

[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]]][142]:

- 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

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by [Principle 4 of][143] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

140 The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the Network Security Requirements.

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

142 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.

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

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.][144]

Firm Name
City, State/Province, Country
Report Date

144 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, period of time

ABC-CA MANAGEMENT'S ASSERTION

[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][145] and provides SSL CA services.][146]

ABC-CA management has assessed its [disclosures of its certificate practices and][147] controls over its EV SSL CA services. Based on that assessment, in providing its SSL [and non-SSL] Certification Authority (CA) services at <LOCATION>[148], 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)][149],

  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][150]

145 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.

146 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.

147 Include if SSL Baseline Requirements are in scope. Remove if only Network Security Requirements are in scope.

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

149 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.

150 The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the Network Security Requirements.

- 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 [Principle 4 of][151] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x [152].

<Signoff Name and Title>
<Date that matches the assurance opinion date>

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

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

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

ABC-CA MANAGEMENT'S ASSERTION

[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][153] and provides SSL CA services.][154]ABC-CA management has assessed its [disclosures of its certificate practices and][155] controls over its EV SSL CA services. Based on that assessment, in providing its SSL [and non-SSL] Certification Authority (CA) services at <LOCATION>[156], as of <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)][157],

  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][158]

153 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.

154 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.

155 Include if SSL Baseline Requirements are in scope. Remove if only Network Security Requirements are in scope.

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

157 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.

158 The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the Network Security Requirements.

- 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 [Principle 4 of][159] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x [160].

<Signoff Name and Title>
<Date that matches the assurance opinion date>

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

160 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"):

Scope[161]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[162] that for its Certification Authority (CA) operations at <LOCATION>[163], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][164], 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][165]

  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)

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x[166].

161 Subheadings are optional and can be removed if desired.

162 Hyperlink to assertion.

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

164 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.

165 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.

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

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

Our independence and quality control
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.

Practitioner's responsibilities
Our responsibility is to express an opinion on management's assertion 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 assertion 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;
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, 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.

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.][167]

Firm Name
City, State/Province, Country
Report Date

167 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"):

Scope[168]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[169] that for its Certification Authority (CA) operations at <LOCATION>[170], as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][171], 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][172]

  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[173].

Certification authority's responsibilities

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

168 Subheadings are optional and can be removed if desired.

169 Hyperlink to assertion.

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

171 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.

172 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.

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

Our independence and quality control

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.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion 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 assertion 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;
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, 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

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

INDEPENDENT ASSURANCE REPORT

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

Scope[174]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[175], 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)][176]

  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[177].

174 Subheadings are optional and can be removed if desired.

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

176 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.

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

Our independence and quality control
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.

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.

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][178]

  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)

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.

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.

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.][179]

Firm Name
City, State/Province, Country
Report Date

179 Remove bracketed text if a seal is not issued.

Management's Assertion

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

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][180], 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][181], 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>[182], 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][183]

  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

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

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

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

183 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 [based on][184] the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x[185].

<Signoff Name and Title>
<Date that matches the assurance opinion date>

184 Use ‘in accordance with’ for Canadian and International standards. Use ‘based on’ for US standards.

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

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

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][186], 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][187], 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>[188], 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][189]

  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)

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

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

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

189 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 [based on][190] the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x[191].

<Signoff Name and Title>
<Date that matches the assurance opinion date>

190 Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards.

191 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"):

Scope[192]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[193] that for its Certification Authority (CA) operations at <LOCATION>[194], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][195], 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][196]

  including its commitment to provide CS certificates in conformity with the applicable Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, 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.

192 Subheadings are optional and can be removed if desired.

193 Hyperlink to assertion.

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

195 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.

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.

- 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[197].

[And, 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]][198]:

- 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.

In accordance with the WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing Certificates v2.x.

Certification Authority's responsibilities

ABC-CA's management is responsible for its assertion, 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 v2.x[199].

Our independence and quality control

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.

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

198 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.

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

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion 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 assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's CS [and EVCS][200] 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;
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.

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, 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 v2.x.

200 If applicable.

This report does not include any representation as to the quality of ABC-CA's services other than its CA operations at <LOCATION>[201], 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.][202]

Firm Name
City, State/Province, Country
Report Date

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

202 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"):

Scope[203]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[204] that for its Certification Authority (CA) operations at <LOCATION>[205], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][206], 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][207]

  including its commitment to provide CS certificates in conformity with the applicable Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
- 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[208].

203 Subheadings are optional and can be removed if desired.

204 Hyperlink to assertion.

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

206 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.

207 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.

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

[And, 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]][209]:

- 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.

In accordance with the WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing Certificates v2.x.

Certification Authority's responsibilities

ABC-CA's management is responsible for its assertion, 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 v2.x[210].

Our independence and quality control

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.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion 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

209 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.

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

Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's CS [and EVCS][211] 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;
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 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.

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, 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 v2.x.

211 If applicable.

This report does not include any representation as to the quality of ABC-CA's services other than its CA operations at <LOCATION>[212], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

212 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"):

Scope[213]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[214], 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]][215]

  including its commitment to provide CS certificates in conformity with the applicable Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, 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[216].

213 Subheadings are optional and can be removed if desired.

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

215 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.

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

[And, 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]][217]:

- 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.

throughout the period <DATE> to <DATE> in accordance with the WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing Certificates v2.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 – Publicly Trusted Code Signing Certificates v2.x.

Our independence and quality control
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.

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 – Publicly Trusted Code Signing Certificates 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

217 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.

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][218] 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;
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
  - — [name and version of certificate policy(ies) (if applicable][219]

  including its commitment to provide CS certificates in conformity with the applicable Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, and provided such services in accordance with its disclosed practices

218 If applicable.

219 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:
  - 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[220].

[And, 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]][221]:

- 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.

throughout the period <DATE> to <DATE> in accordance with the WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing Certificates v2.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>[222], 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.][223]

Firm Name
City, State/Province, Country
Report Date

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

221 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.

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

223 Remove bracketed text if a seal is not issued.

Management's Assertion

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

ABC-CA MANAGEMENT'S ASSERTION

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.

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][224]

  including its commitment to provide CS certificates in conformity with the applicable Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, 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[225].

224 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.

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

[And, 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]][226]:

- 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.

throughout the period <DATE> to <DATE> based on the WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing Certificates v2.x.

<Signoff Name and Title>
<Date that matches the assurance opinion date>

226 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.

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:

- a Root Key Generation Ceremony
- key lifecycle events
  - key back up, storage and recovery
  - key usage for intended functions
  - key destruction
  - key transport

Root Key Generation Ceremonies

Specific Reporting Guidance for Root Key Generation Ceremonies

The included report is intended to be issued as part of a WebTrust practitioner's witnessing of a CA's Root Key Generation Ceremony. The report template is designed for the witness of the creation of a Root CA key pair (i.e., the top-level CA in a PKI hierarchy), however it can be adapted to report on a subordinate CA as well.

In cases where the practitioner witnesses the creation of multiple root keys in a single ceremony, it is acceptable to issue one report provided that each root is covered by the same CP/CPS, and all relevant root key scripts are referenced.

At a minimum, the assurance report must include the subject key identifier of each key witnessed.

International Standards – ISAE 3000

Example IN5.1 – Root key generation ceremony, attestation engagement

INDEPENDENT ASSURANCE REPORT

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

Scope[227]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[228] that in generating and protecting its [list of Root CAs witnessed] (collectively, "ABC-CA Root CAs") on <DATE>[229] at <LOCATION>[230], 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]][231]
- 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)

227 Subheadings are optional and can be removed if desired.

228 Hyperlink to assertion.

229 Date of witnessing. This can be a range of dates if the ceremony spanned multiple days.

230 Location of the key generation ceremony.

231 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[232].

Certification authority's responsibilities
ABC-CA's management is responsible for its assertion, 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 control
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.

Practitioner's responsibilities
Our responsibility is to express an opinion on management's assertion 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 assertion 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;

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

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, 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

Management's Assertion

Example MA5.1 – Management's assertion

ABC-CA MANAGEMENT'S ASSERTION

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][233] CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x[234].

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>[235] at <LOCATION>[236], with the following identifying information:

233 Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards.

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

235 Date of witnessing. This can be a range of dates if the ceremony spanned multiple days.

236 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][237]
- 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[238].

<Signoff Name and Title>
<Date that matches the assurance opinion date>

237 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.

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

Reporting on Life Cycle

International Standards – ISAE 3000

Example CA5.2 – Unqualified opinion, attestation engagement (for various lifecycle events), period of time

INDEPENDENT ASSURANCE REPORT

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

Scope[239]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion 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)>[240], throughout the period <DATE> to <DATE> for its CA keys enumerated in Attachment A[241], 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][242]

- 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

239 Subheadings are optional and can be removed if desired.

240 Include applicable locations based on the criteria in-scope.

241 List in-scope CA keys or other key pair identifiers.

242 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 4.11[243] of the WebTrust Principles and Criteria for Certification Authorities v2.x[244].

Certification Authority's responsibilities
ABC-CA's management is responsible for its assertion, 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 4.11[245] of the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control
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.

Practitioner's responsibilities
Our responsibility is to express an opinion on management's assertion 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 assertion 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.

243 Include only those criteria that are applicable to the current reporting.

244 Hyperlink to the current version of the WebTrust Principles and Criteria for Certification Authorities.

245 Include only those criteria that are applicable to the current reporting.

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, 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 4.11[246] of the WebTrust Principles and Criteria for Certification Authorities v2.x[247].

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*[248], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

246 Include only those criteria that are applicable to the current reporting.

247 Hyperlink to the current version of the WebTrust Principles and Criteria for Certification Authorities.

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

Attachment A – CAs in-scope for key lifecycle management activities[249]

CA KEYS STORED, BACKUP, AND RECOVERED IN <LOCATION(S)>[250]

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)>[251] TO <LOCATION(S)>[252]

CA subject name	Subject key identifier	Certificate serial number	SHA256 thumbprint

249 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.

250 Include applicable location(s).

251 Include applicable location(s).

252 Include applicable location(s).

Management Assertion

Example MA5.2 – Management's assertion on life cycle

ABC-CA MANAGEMENT'S ASSERTION

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)>[253], throughout the period January 1, 2XXX to December 31, 2XXX for its CA keys enumerated in Attachment A[254].

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 4.11[255] of the WebTrust Principles and Criteria for Certification Authorities v2.x[256]. 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.

253 Include applicable locations based on the criteria in-scope.

254 List in-scope CA keys or other key pair identifiers.

255 Include only those criteria that are applicable to the current reporting.

256 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 4.11[257] of the WebTrust Principles and Criteria for Certification Authorities v2.x[258].

<Signoff Name and Title>
<Date that matches the assurance opinion date>

257 Include only those criteria that are applicable to the current reporting.

258 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 IN6.1 – Unqualified opinion, attestation engagement, period of time

INDEPENDENT ASSURANCE REPORT

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

Scope[259]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[260] that for its Certification Authority (CA) operations at <LOCATION>[261], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][262], 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][263]

  including its commitment to provide VM certificates in conformity with the applicable Verified Mark Certificate Requirements as set out at https://bimigroup.org/resources/VMC_Guidelines_latest.pdf, 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.

259 Subheadings are optional and can be removed if desired.

260 Hyperlink to assertion.

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

262 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.

263 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x[264].

Certification authority's responsibilities
ABC-CA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.

Our independence and quality control
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.

Practitioner's responsibilities
Our responsibility is to express an opinion on management's assertion 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 assertion is fairly stated, and, accordingly, included:

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

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;
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 management's assertion, 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.][265]

Firm Name
City, State/Province, Country
Report Date

265 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"):

Scope[266]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[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 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)][270]

  including its commitment to provide VM certificates in conformity with the applicable Verified Mark Certificate Requirements as set out at https://bimigroup.org/resources/VMC_Guidelines_latest.pdf, 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]

266 Subheadings are optional and can be removed if desired.

267 Hyperlink to assertion.

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.

- 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 – Verified Mark Certificates v1.x[271].

Certification authority's responsibilities
ABC-CA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.

Our independence and quality control
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.

Practitioner's responsibilities
Our responsibility is to express an opinion on management's assertion 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 assertion 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;
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

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

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, 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.

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"):

Scope[272]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[273], 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)][274]

  including its commitment to provide VM certificates in conformity with the applicable Verified Mark Certificate Requirements as set out at https://bimigroup.org/resources/VMC_Guidelines_latest.pdf, 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

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.

272 Subheadings are optional and can be removed if desired.

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

274 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.

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[275].

Our independence and quality control
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.

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:

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;
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.

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

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][276]

  including its commitment to provide VM certificates in conformity with the applicable Verified Mark Certificate Requirements as set out at https://bimigroup.org/resources/VMC_Guidelines_latest.pdf, 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]

276 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 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 – 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.][277]

Firm Name
City, State/Province, Country
Report Date

277 Remove bracketed text if a seal is not issued.

Management's Assertion

Example MA6.1 – Management's assertion, period of time

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][278], 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][279], 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>[280], 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][281]

  including its commitment to provide VM certificates in conformity with the applicable Verified Mark Certificate Requirements as set out at https://bimigroup.org/resources/VMC_Guidelines_latest.pdf, 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;

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

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

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.

  - 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x[282].

<Signoff Name and Title>
<Date that matches the assurance opinion date>

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

Example MA6.2 – Management's assertion, point in time

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][283], 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][284], 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>[285], 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][286]

  including its commitment to provide VM certificates in conformity with the applicable Verified Mark Certificate Requirements as set out at https://bimigroup.org/resources/VMC_Guidelines_latest.pdf, 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.

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

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

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

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.

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x[287].

<Signoff Name and Title>
<Date that matches the assurance opinion date>

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