WEBTRUST® FOR CERTIFICATION AUTHORITIES

Illustrative Reports Under CSAE 3000 and CSAE 3001

Version 1.0

Published 1 September 2017

Document History

Version	Publication Date	Revision Summary
1.0	1 September 2017	Initial publication

Acknowledgements

This document has been prepared by the CPA Canada WebTrust/PKI Assurance Task Force (the "Task Force") for use by those auditors licensed to perform WebTrust for Certification Authorities audits by CPA Canada.

Members of the Task Force are:

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

Significant support has been provided by:

- Daniel J. Adam, *Deloitte & Touche LLP*
- Donoghue Clarke, *Ernst & Young LLP*
- Timothy Crawford, *BDO USA, LLP*
- Zain Shabbir, *KPMG LLP*

CPA Canada Support

- Kaylynn Pippo, (Staff Contact)
- Bryan Walker
- Janet Treasure, Vice President, Member Development and Support
- Gord Beal, Vice President, Research, Guidance and Support

Table of Contents

Reporting Guidance

Professional Standards

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

- Canadian Standard for Assurance Engagements (CSAE) 3000, *Attestation Engagements Other Than Audits or Reviews of Historical Financial Information*
- Canadian Standard for Assurance Engagements (CSAE) 3001, *Direct Engagements*

Traditionally, under recently replaced reporting standards in Canada, the attestation engagement 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 CSAE 3000 should normally be used 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 as to which standard to use depends on the nature of the engagement. The auditor will need to agree with the client in advance as to the nature of the engagement and the related standard, 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 organization that are only intended to be used within that organization (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 organization's intranet that is accessible to all organization users.

CA Processing Locations

All reports issued should list the city, state/province (if applicable), and country of all physical locations used in CA operations. This includes 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 are performed.

List of Root and Subordinate CAs in Scope

All reports issued must list all root and subordinate CAs that were subject to audit. 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 audit 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 audit 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 2016 to 31 January 2017 and were maintained online to provide revocation status information only. The CA certificate for the XY CA expired on 5 January 2017 and was not renewed. The CA certificate for the YA CA was revoked on 2 February 2017 and was not re-issued.

Reference to Applicable Audit Criteria

All reports issued should make reference to the applicable audit criteria used, including the version number. These 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 2017, or May 7, 2017). Numerical date formats (i.e. 07/05/2017 or 05/07/2017) should be avoided.

Reporting on Subscriber Registration Activities

The auditor 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 the assertion-based engagement, 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 examination 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 examined and reported upon separately 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 audit 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 examination 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 auditor note in the audit report that the criteria were not audited 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 examination did not extend to controls that would address those criteria.

Qualified Audit Reports

In Canada, there are various ways in which to report a scenario where the CA does not meet the necessary criteria.

Under CSAE 3000, depending on whether management has modified their assertion or not, the auditor 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 Auditor will assess the materiality and pervasiveness of the matter(s) of non-compliance and determine if the effects of a matter are:

- not so material or pervasive, then the auditor would issue a qualified opinion (Example 1.4: Qualified opinion)
- material and pervasive, then the auditor would issue an adverse opinion or disclaimer of conclusion.

This option is not recommended by the Task Force as management appears as either not being aware of the issues that cause the audit 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 certain criteria. It reflects management's acknowledgement of the issues causing the audit qualification.

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

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

Rather, when CSAE 3000 is used for reporting, the second option should be used in the opinion of the Task Force as it will not confuse the users of the report. This option is shown as example CA1.5.

Under CSAE 3001, the auditor reports directly on the subject matter and applicable criteria since there is no management assertion provided for these engagements. When the auditor issues a qualified report, it is referenced to the subject matter and applicable criteria. When a report is issues under CSAE 3001, no management assertion is included in the report. This option is shown as example CA1.6.

WebTrust for Certification Authorities

Canadian Standards – CSAE 3000/3001

Example CA1.1 – Unqualified Opinion, Attestation Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[1] that for its Certification Authority (CA) operations at <LOCATION>[2], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][3], 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)][4]

- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][5]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[6]

- 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;

---

[1] Hyperlink to assertion
[2] CA processing locations as defined in the "Reporting Guidance" section
[3] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[4] 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
[5] Remove bracketed text/bullet if CA has a combined CP and CPS document
[6] If CA has a combined CP/CPS then remove references to Certificate Policy

- 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[7].

[(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.][8]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our audit did not extend to controls that would address those criteria.][9]

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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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;

---

[7] Include applicable version number and hyperlink to the criteria document
[8] Remove bracketed text if external RAs are not used
[9] 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.

(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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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.][10]

Firm Name
City, State/Province, Country
Report Date

[10] Remove bracketed text if a seal is not issued

Example CA1.2 – Unqualified Opinion, Attestation Engagement, Point in Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[11] that for its Certification Authority (CA) operations at <LOCATION>[12], as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][13], 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][14]

- 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)][15]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[16]

- 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

---

[11] Hyperlink to assertion
[12] CA processing locations as defined in the "Reporting Guidance" section
[13] Reference to an appendix or replace with list of Root and Subordinate CAs in scope . Refer to "Reporting Guidance" section
[14] 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
[15] Remove bracketed text/bullet if CA has a combined CP and CPS document
[16] 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[17].

[(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.][18]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our audit did not extend to controls that would address those criteria.][19]

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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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.

---

[17] Include applicable version number and hyperlink to the criteria document
[18] Remove bracketed text if external RAs are not used
[19] 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.

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.

Suitability of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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 CA1.3 – Unqualified Opinion, Direct Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[20], ABC-CA's

- disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices,
- [the consistency of its Certification Practice Statement with its Certificate Policy (if applicable)][21], the provision of services in accordance with its [Certificate Policy (if applicable)][22] and Certification Practice Statement, and
- the effectiveness of its controls over:
    - key and certificate integrity;
    - the authenticity and confidentiality of subscriber and relying party information;
    - the continuity of key and certificate lifecycle management operations; and
    - the development, maintenance, and operation of CA systems integrity,

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope.[23]

[(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.][24]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our audit did not extend to controls that would address those criteria.][25]

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.[26]

---

[20] CA processing locations as defined in the "Reporting Guidance" section
[21] Remove bracketed text if the CA publishes a combined CP/CPS
[22] Remove bracketed text if the CA publishes a combined CP/CPS
[23] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[24] Remove bracketed text if external RAs are not used
[25] 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.
[26] Include applicable version number and hyperlink to the criteria document

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor'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 (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements,* set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all significant 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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA has, in all significant 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][27]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][28]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[29]

- 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.

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.][30]

Firm Name
City, State/Province, Country
Report Date

---

[27] 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
[28] Remove bracketed text/bullet if CA has a combined CP and CPS document
[29] If CA has a combined CP/CPS then remove references to Certificate Policy
[30] Remove bracketed text if a seal is not issued

Example CA1.4 – 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

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[31] that for its Certification Authority (CA) operations at <LOCATION>[32], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][33], 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][34]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][35]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[36]

- 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

---

[31] Hyperlink to assertion
[32] CA processing locations as defined in the "Reporting Guidance" section
[33] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[34] 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
[35] Remove bracketed text/bullet if CA has a combined CP and CPS document
[36] If CA has a combined CP/CPS then remove references to Certificate Policy

- 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[37].

[(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.][38]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our audit did not extend to controls that would address those criteria.][39]

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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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;

[37] Include applicable version number and hyperlink to the criteria document
[38] Remove bracketed text if external RAs are not used
[39] Modify this paragraph as appropriate to exclude certain criteria from scope

(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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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 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.*

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 minimised 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 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 CA1.5 – Qualified Opinion on Physical Security and Business Continuity, Attestation Engagement, Period of Time - Assertion Modified by Management

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[40] that, except for matters described in the assertion, for its Certification Authority (CA) operations at <LOCATION>[41], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][42], 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][43]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][44]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[45]

- 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

---

[40] Hyperlink to assertion
[41] CA processing locations as defined in the "Reporting Guidance" section
[42] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[43] 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
[44] Remove bracketed text/bullet if CA has a combined CP and CPS document
[45] If CA has a combined CP/CPS then remove references to Certificate Policy

- 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[46].

[(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.][47]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our audit did not extend to controls that would address those criteria.][48]

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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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:

(5) 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;
(6) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;

---

[46] Include applicable version number and hyperlink to the criteria document
[47] Remove bracketed text if external RAs are not used
[48] Modify this paragraph as appropriate to exclude certain criteria from scope

(7) testing and evaluating the operating effectiveness of the controls; and
(8) 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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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 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.*

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 minimised 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][49]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][50]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[51]

- 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

[49] 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
[50] Remove bracketed text/bullet if CA has a combined CP and CPS document
[51] If CA has a combined CP/CPS then remove references to Certificate Policy

- 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

Example CA1.6 – 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

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[52], ABC-CA's

- disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices,
- [the consistency of its Certification Practice Statement with its Certificate Policy (if applicable)][53], the provision of services in accordance with its [Certificate Policy (if applicable)][54] and Certification Practice Statement, and
- the effectiveness of its controls over:
    - key and certificate integrity;
    - the authenticity and confidentiality of subscriber and relying party information;
    - the continuity of key and certificate lifecycle management operations; and
    - the development, maintenance, and operation of CA systems integrity,

throughout the period <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope].[55]

[(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.][56]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our audit did not extend to controls that would address those criteria.][57]

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.[58]

---

[52] CA processing locations as defined in the "Reporting Guidance" section
[53] Remove bracketed text if the CA publishes a combined CP/CPS
[54] Remove bracketed text if the CA publishes a combined CP/CPS
[55] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[56] Remove bracketed text if external RAs are not used
[57] Modify this paragraph as appropriate to exclude certain criteria from scope
[58] Include applicable version number and hyperlink to the criteria document

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor'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 (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements,* set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all significant 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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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 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.*

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 minimised 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 significant 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][59]

- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][60]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[61]

- 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.

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

[59] 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
[60] Remove bracketed text/bullet if CA has a combined CP and CPS document
[61] If CA has a combined CP/CPS then remove references to Certificate Policy

Example CA 1.7– Qualified Opinion on Physical Security and Business Continuity, Attestation Engagement, Period of Time – Assertion not Modified by Management - Table presentation

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[62] that for its Certification Authority (CA) operations at <LOCATION>[63], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][64], 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][65]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][66]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[67]

- 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

---

[62] Hyperlink to assertion
[63] CA processing locations as defined in the "Reporting Guidance" section
[64] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[65] 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
[66] Remove bracketed text/bullet if CA has a combined CP and CPS document
[67] If CA has a combined CP/CPS then remove references to Certificate Policy

- 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[68].

[(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.][69]

[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.][70]

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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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;

---

[68] Include applicable version number and hyperlink to the criteria document
[69] Remove bracketed text if external RAs are not used
[70] Modify this paragraph as appropriate to exclude certain criteria from scope

(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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Basis for qualified opinion

During our procedures, we noted the following which 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.	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:

Observation	Relevant WebTrust Criteria
This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.8 to not be met.	• 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 table presented in the basis for qualified opinion 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

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	6D5A334C1BAF569E	rsaEncryption	(4096 bit)	sha256WithRSAEncryption	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	7DAAAF3CF15F8F45	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	Mar 14 01:25:41 2017 GMT	Mar 14 01:25:41 2027 GMT	92:A4:60:D4:ED:AC:57:3D:C2:1B:24:07:0D:AF:AC:DD:F1:0D:8A: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	8FABAF6CF45F884F	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	Apr 22 07:41:53 2017 GMT	Apr 22 07:41:53 2027 GMT	92:A4:60:D4:ED:AC:57:3D:C2:1B:24:07:0D:AF:AC:DD:F1:0D:8A: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][71], and provides the following CA services[72]:

- 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][73], 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.

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>[74], 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][75]

---

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

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

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

[74] CA processing locations as defined in the "Reporting Guidance" section

[75] 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)][76]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[77]

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

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorised individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with [based on][78] the WebTrust Principles and Criteria for Certification Authorities v2.x[79], including the following[80]:

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

---

[76] Remove bracketed text/bullet if CA has a combined CP and CPS document
[77] If CA has a combined CP/CPS then remove references to Certificate Policy
[78] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[79] Include applicable version number and hyperlink to the criteria document
[80] Remove bullets that are not applicable

- 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 audit 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:

- 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:

---

[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

[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

    - [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 [based on][89] the WebTrust Principles and Criteria for Certification Authorities v2.x[90], including the following[91]:

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

---

[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] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[90] Include applicable version number and hyperlink to the criteria document
[91] Remove bullets that are not applicable

- 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 audit opinion date>

Example MA1.3 – Management's Assertion, Period of Time – Modified Assertion Accompanying Qualified Report Example CA1.5

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][92], and provides the following CA services[93]:

- 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][94], 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.

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.	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

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

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

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

	Observation	Relevant WebTrust Criteria
	This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.4 to not be met.	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>[95], throughout the period <DATE> to <DATE>, ABC-CA has:

[95] 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][96]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][97]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[98]

- 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 [based on][99] the WebTrust Principles and Criteria for Certification Authorities v2.x[100], including the following[101]:

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

---

[96] 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
[97] Remove bracketed text/bullet if CA has a combined CP and CPS document
[98] If CA has a combined CP/CPS then remove references to Certificate Policy
[99] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[100] Include applicable version number and hyperlink to the criteria document
[101] Remove bullets that are not applicable

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.][102]

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

[102] 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

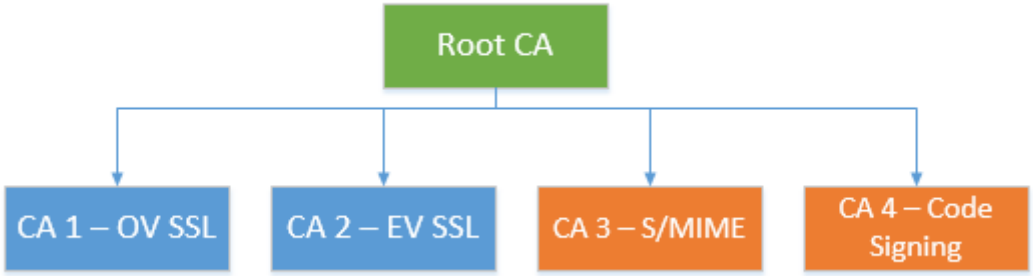
As of the time of publication, the SSL Baseline with Network Security audit criteria incorporates two different CA/Browser Forum requirements documents:

- 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 audit 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.

Canadian Standards – CSAE 3000/3001

Example CA2.1 – Unqualified Opinion, Attestation Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[103] that for its Certification Authority (CA) operations at <LOCATION>[104], 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]][105], 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][106],

  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 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][107]

[And, for its [list of Root and Subordinate CAs in scope for Network Security Requirements]][108]:

---

[103] Hyperlink to assertion
[104] CA processing locations as defined in the "Reporting Guidance" section
[105] 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.
[106] 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
[107] The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the Network Security Requirements
[108] Replace with list of Root and Subordinate CAs in scope for the Network Security Requirements or reference to an appendix, if this is different to the CAs in scope for the SSL Baseline Requirements. If the in-scope CAs are the same for both the SSL Baseline Requirements and the Network Security Requirements, then delete this line and include the full list of CAs in the first paragraph. Refer to "Reporting Guidance" section

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with [Principle 4 of][109] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x [110].

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][111] 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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and][112] 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][113];
(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.

---

[109] Include this bracket if only opining on the Network Security Requirements
[110] Include applicable version number and hyperlink to the criteria document
[111] Include this bracket if only opining on the Network Security Requirements
[112] Delete bracketed text if not covering the SSL Baseline Requirements
[113] Delete bracketed text if not covering the SSL Baseline Requirements

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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][114] 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][115] 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.

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.][116]

Firm Name
City, State/Province, Country
Report Date

[114] Include this bracket if only opining on the Network Security Requirements
[115] Include this bracket if only opining on the Network Security Requirements
[116] 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 CA2.2 – Unqualified Opinion, Attestation Engagement, Point in Time

INDEPENDENT ASSURANCE REPORT

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

Scope

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 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][121]

[And, for its [list of Root and Subordinate CAs in scope for Network Security Requirements]][122]:

---

[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
[122] 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

- 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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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 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.

---

[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
[126] Delete bracketed text if not covering the SSL Baseline Requirements

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

Suitability of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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

[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 CA2.3 – Unqualified Opinion, Direct Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[129], ABC-CA's

- disclosure of its SSL certificate lifecycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website,
- the provision of such services in accordance its disclosed practices, and
- the effectiveness of its controls over:
    - key and SSL certificate integrity;
    - the authenticity and confidentiality of SSL subscriber and relying party information;
    - the continuity of key and SSL certificate lifecycle management operations; and
    - the development, maintenance, and operation of CA systems integrity,
    - [and over meeting the network and certificate system security requirements set forth by the CA/Browser Forum][130]

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]][131].

[We have also been engaged to report on the effectiveness of ABC-CA's controls over meeting the network and certificate system security requirements set forth by the CA/Browser Forum 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][132].][133]

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]

---

[129] CA processing locations as defined in the "Reporting Guidance" section
[130] Include bracketed text if SSL Baseline and Network Security Requirements apply to the same hierarchy. Otherwise, remove and include the next paragraph
[131] 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
[132] Replace with list of CAs in scope for Network Security Requirements or reference to an appendix. This list must repeat all CAs that are in scope for SSL Baseline Requirements as well as all other Non-SSL CAs. Refer to "Reporting Guidance" section
[133] Include this paragraph if the reporting on difference hierarchies for SSL Baseline Requirements vs Network Security Requirements. Otherwise, remove.
[134] Include this bracket if only opining on the Network Security Requirements
[135] Include applicable version number and hyperlink to the criteria document

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor'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 (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements,* set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all significant respects, management's disclosures and controls conform to the WebTrust Criteria, and, accordingly, included:

(1) [obtaining an understanding of ABC-CA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and][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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and

[136] Include this bracket if only opining on the Network Security Requirements
[137] Delete bracketed text if not covering the SSL Baseline Requirements
[138] Delete bracketed text if not covering the SSL Baseline Requirements

correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

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

- 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 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][140]

- 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][141] 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][142] 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.

Use of the WebTrust seal

[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

[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] Include this bracket if only opining on the Network Security Requirements

[(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.][143]

Firm Name
City, State/Province, Country
Report Date

[143] 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][144] and provides SSL CA services.][145]

[ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope for Network Security Requirements][146] and provides non-SSL CA services.][147]

The management of ABC-CA is responsible for establishing and maintaining effective controls over its SSL [and non-SSL] CA operations, including its network and certificate security system controls, [its SSL CA business practices disclosure on its website [or other repository location][148], SSL key lifecycle management controls, and SSL certificate lifecycle management controls.][149] 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][150] controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its SSL [and non-SSL] Certification Authority (CA) services at <LOCATION>[151], 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

---

[144] 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

[145] 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

[146] Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the Network Security Requirements or reference to an appendix. Refer to "Reporting Guidance" section

[147] Include this introductory paragraph if there are additional non-SSL CAs that are in scope for the Network Security Requirements or if only auditing the Network Security Requirements. Remove this paragraph if all in-scope CAs are SSL.

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

[149] Include if SSL Baseline Requirements are in scope. Remove if only Network Security Requirements are in scope.

[150] Include if SSL Baseline Requirements are in scope. Remove if only Network Security Requirements are in scope.

[151] CA processing locations as defined in the "Reporting Guidance" section

- [name and version of certificate policy(ies) (if applicable][152],

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 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][153]

- 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 [based on][154] [Principle 4 of][155] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x [156].

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

[152] 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
[153] The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the Network Security Requirements
[154] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[155] Include this bracket if only opining on the Network Security Requirements
[156] 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][157] and provides SSL CA services.][158]

[ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope for Network Security Requirements][159] and provides non-SSL CA services.][160]

The management of ABC-CA is responsible for establishing controls over its SSL [and non-SSL] CA operations, including its network and certificate security system controls, [its SSL CA business practices disclosure on its website [or other repository location][161], SSL key lifecycle management controls, and SSL certificate lifecycle management controls.][162] 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][163] controls over its SSL CA services. Based on that assessment, in ABC-CA management's opinion, in providing its SSL [and non-SSL] Certification Authority (CA) services at <LOCATION>[164], 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][165],

  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

---

[157] Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the Network Security Requirements or reference to an appendix. Refer to "Reporting Guidance" section

[158] 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

[159] Replace with list of Root and Subordinate CAs in scope for the Network Security Requirements or reference to an appendix. Refer to "Reporting Guidance" section

[160] Include this introductory paragraph if there are additional non-SSL CAs that are in scope for the Network Security Requirements or if only auditing the Network Security Requirements. Remove this paragraph if all in-scope CAs are SSL.

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

[162] Include if SSL Baseline Requirements are in scope. Remove if only Network Security Requirements are in scope.

[163] Include if SSL Baseline Requirements are in scope. Remove if only Network Security Requirements are in scope.

[164] CA processing locations as defined in the "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

- 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 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][166]

- 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 [based on][167] [Principle 4 of][168] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x [169].

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

[166] The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the Network Security Requirements
[167] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[168] Include this bracket if only opining on the Network Security Requirements
[169] Include applicable version number and hyperlink to the criteria document

WebTrust for Certification Authorities – Extended Validation – SSL ("EV SSL")

Canadian Standards – CSAE 3000/3001

Example CA3.1 – Unqualified Opinion, Attestation Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[170] that for its Certification Authority (CA) operations at <LOCATION>[171], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][172], 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][173]

  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[174].

Certification authority's responsibilities

[170] Hyperlink to assertion
[171] CA processing locations as defined in the "Reporting Guidance" section
[172] 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
[173] 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
[174] Include applicable version number and hyperlink to the criteria document

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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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.][175]

Firm Name
City, State/Province, Country
Report Date

[175] Remove bracketed text if a seal is not issued.

Example CA3.2 – Unqualified Opinion, Attestation Engagement, Point in Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[176] that for its Certification Authority (CA) operations at <LOCATION>[177], as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][178], 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][179]

  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[180].

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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

---

[176] Hyperlink to assertion
[177] CA processing locations as defined in the "Reporting Guidance" section
[178] 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
[179] 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
[180] Include applicable version number and hyperlink to the criteria document

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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.

Suitability of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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 CA3.3 – Unqualified Opinion, Direct Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[181], ABC-CA's

- disclosure of its extended validation SSL ("EV SSL") certificate lifecycle management business practices, including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the ABC-CA website,
- the provision of such services in accordance its disclosed practices, and
- the effectiveness of its controls over:
    - key and EV SSL certificate integrity;
    - the authenticity and confidentiality of EV SSL subscriber and relying party information; and
    - the continuity of key and EV SSL certificate lifecycle management operations,

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][182].

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[183].

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor'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

---

[181] CA processing locations as defined in the "Reporting Guidance" section
[182] 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
[183] Include applicable version number and hyperlink to the criteria document

SSL v1.x (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements,* set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all significant 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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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)][184]

  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:

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

- the integrity of keys and 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.

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.][185]

Firm Name
City, State/Province, Country
Report Date

[185] 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][186], 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][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, 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>[188], 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][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

- 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)

---

[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 audit 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

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][192], 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][193], 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>[194], 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][195]

  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 [based on][196] the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x[197].

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

---

[192] Replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to "Reporting Guidance" section
[193] Link to business practices repository location and describe location if not website (i.e. intranet)
[194] CA processing locations as defined in the "Reporting Guidance" section
[195] 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
[196] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[197] Include applicable version number and hyperlink to the criteria document

WebTrust for Certification Authorities – Extended Validation – Code Signing ("EV CS")

Canadian Standards – CSAE 3000/3001

Example CA4.1 – Unqualified Opinion, Attestation Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[198] that for its Certification Authority (CA) operations at <LOCATION>[199], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][200], ABC-CA has:

- disclosed its extended validation code signing ("EV 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][201]

  including its commitment to provide EV CS 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 CS certificates it manages is established and protected throughout their lifecycles; and
    - EV CS subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

- maintained effective controls to provide reasonable assurance that:
    - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
    - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum

---

[198] Hyperlink to assertion
[199] CA processing locations as defined in the "Reporting Guidance" section
[200] 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
[201] 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 [EV CS Signing Authority] [and EV CS Timestamp Authority] is/are operated in conformity with CA/Browser Forum Guidelines][202]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.x[203].

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 Code Signing v1.x.

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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 CS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV CS certificates, EV CS Signing Authority certificates, and EV CS Timestamp Authority certificates;
(2) selectively testing transactions executed in accordance with disclosed EV CS 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.

Relative effectiveness of controls

---

[202] Modify the bracketed text depending on which services the CA provides. If it does not provide a Signing Authority or Timestamp Authority, then remove this bullet point
[203] 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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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 Code Signing 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 Code Signing 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 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.][204]

Firm Name
City, State/Province, Country
Report Date

[204] 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

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

- disclosed its extended validation code signing ("EV 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][208]

  including its commitment to provide EV CS 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 CS certificates it manages is established and protected throughout their lifecycles; and
    - EV CS 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:
    - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
    - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum

- [suitably designed, and placed into operation, controls to provide reasonable assurance that its [EV CS Signing Authority] [and EV CS Timestamp Authority] is/are operated in conformity with CA/Browser Forum Guidelines][209]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.x[210].

---

[205] Hyperlink to assertion
[206] CA processing locations as defined in the "Reporting Guidance" section
[207] 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
[208] 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
[209] Modify the bracketed text depending on which services the CA provides. If it does not provide a Signing Authority or Timestamp Authority, then remove this bullet point
[210] 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 Code Signing v1.x.

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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 CS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV CS certificates, EV CS Signing Authority certificates, and EV CS Timestamp Authority 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.

Suitability of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with

internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

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 Code Signing 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 Code Signing 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 CA4.3 – Unqualified Opinion, Direct Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>[211], ABC-CA's

- disclosure of its extended validation code signing ("EV CS") certificate lifecycle management business practices, including its commitment to provide EV CS certificates in conformity with the CA/Browser Forum Guidelines on the ABC-CA website,
- the provision of such services in accordance its disclosed practices, and
- the effectiveness of its controls over:
    - key and EV CS certificate integrity;
    - the authenticity and confidentiality of EV CS subscriber and relying party information;
    - the continuity of key and EV CS certificate lifecycle management operations;
    - [and over the continuity and provision of EV CS Signing Authority and EV CS Timestamp Authority services][212],

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][213].

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 Code Signing v1.x[214].

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

---

[211] CA processing locations as defined in the "Reporting Guidance" section
[212] Modify or remove as applicable depending on which services the CA provides
[213] 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
[214] Include applicable version number and hyperlink to the criteria document

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 Code Signing v1.x (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements,* set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all significant respects, management's disclosures and controls conform to the WebTrust Criteria, and, accordingly, included:

(1) obtaining an understanding of ABC-CA's EV CS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV CS certificates, EV CS Signing Authority certificates, and EV CS Timestamp Authority certificates;
(2) selectively testing transactions executed in accordance with disclosed EV CS 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.

Relative effectiveness of controls

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

Because of the nature and inherent limitations of controls, ABC-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

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

- disclosed its extended validation code signing ("EV 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 EV CS certificates in conformity with the CA/Browser Forum Guidelines on the ABC-CA website, and provided such services in accordance with its disclosed practices

[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

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

- maintained effective controls to provide reasonable assurance that:
    - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
    - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum

- [maintained effective controls to provide reasonable assurance that its [EV CS Signing Authority] [and EV CS Timestamp Authority] is/are operated in conformity with CA/Browser Forum Guidelines][216]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing 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 Code Signing 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 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.][217]

Firm Name
City, State/Province, Country
Report Date

[216] Modify the bracketed text depending on which services the CA provides. If it does not provide a Signing Authority or Timestamp Authority, then remove this bullet point
[217] 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 known as [list of Root and Subordinate CAs in scope][218], and provides Extended Validation Code Signing ("EV CS") CA services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its EV CS CA operations, including its EV CS CA business practices disclosure on its website [or other repository location][219], EV CS key lifecycle management controls, EV CS certificate lifecycle management controls, EV CS Signing Authority and EV CS Timestamp Authority 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 CS CA services. Based on that assessment, in ABC-CA management's opinion, in providing its EV CS Certification Authority (CA) services at <LOCATION>[220], throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its extended validation code signing ("EV 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][221]

  including its commitment to provide EV CS 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 CS certificates it manages is established and protected throughout their lifecycles; and
    - EV CS subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

- maintained effective controls to provide reasonable assurance that:

---

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

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

[220] CA processing locations as defined in the "Reporting Guidance" section

[221] 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

    - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
    - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum

- [maintained effective controls to provide reasonable assurance that its [EV CS Signing Authority] [and EV CS Timestamp Authority] is/are operated in conformity with CA/Browser Forum Guidelines][222]

in accordance with [based on][223] the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.x[224].

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

[222] Modify the bracketed text depending on which services the CA provides. If it does not provide a Signing Authority or Timestamp Authority, then remove this bullet point
[223] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[224] Include applicable version number and hyperlink to the criteria document

Example MA4.2 – 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][225], and provides Extended Validation Code Signing ("EV CS") CA services.

The management of ABC-CA is responsible for establishing controls over its EV CS CA operations, including its EV CS CA business practices disclosure on its website [or other repository location][226], EV CS key lifecycle management controls, EV CS certificate lifecycle management controls, EV CS Signing Authority and EV CS Timestamp Authority 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 CS CA services. Based on that assessment, in ABC-CA management's opinion, in providing its EV CS Certification Authority (CA) services at <LOCATION>[227], as of <DATE>, ABC-CA has:

- disclosed its extended validation code signing ("EV 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)][228]

  including its commitment to provide EV CS 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 CS certificates it manages is established and protected throughout their lifecycles; and
    - EV CS 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:
    - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
    - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum

---

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

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

[227] CA processing locations as defined in the "Reporting Guidance" section

[228] 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 its [EV CS Signing Authority] [and EV CS Timestamp Authority] is/are operated in conformity with CA/Browser Forum Guidelines][229]

in accordance with [based on][230] the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.x[231].

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

[229] Modify the bracketed text depending on which services the CA provides. If it does not provide a Signing Authority or Timestamp Authority, then remove this bullet point
[230] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[231] Include applicable version number and hyperlink to the criteria document

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

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

Canadian Standards – CSAE 3000/3001

Example CA5.1 – Root Key Generation Ceremony, Attestation Engagement

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[232] that in generating and protecting its [list of Root CAs witnessed] (collectively, "ABC-CA Root CAs") on <DATE>[233] at <LOCATION>[234], 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][235]

- 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

[232] Hyperlink to assertion
[233] Date of witnessing. This can be a range of dates if the ceremony spanned multiple days.
[234] Location of the key generation ceremony
[235] 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

- 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[236].

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 relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. 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;
(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.

---

[236] Include applicable version number and hyperlink to the criteria document

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 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][237] CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x[238].

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 environmental 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>[239] at <LOCATION>[240], 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

[237] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[238] Include applicable version number and hyperlink to the criteria document
[239] Date of witnessing. This can be a range of dates if the ceremony spanned multiple days.
[240] Location of the key generation ceremony

- [name and version of certificate policy (if applicable][241]

- 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 [based on][242] CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x[243].

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

[241] 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
[242] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[243] Include applicable version number and hyperlink to the criteria document