CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

WebTrust® for Certification Authorities

ILLUSTRATIVE REPORTS UNDER CSAE 3000 AND CSAE 3001

Release Date 1 May 2023

Version 3.0

Document History

Version	Publication Date	Revision Summary
1.0	1 September 2017	Initial publication
2.0	1 February 2022	Updated to reflect wording changes in reporting 2018-2021, new code-signing reporting, new verified mark certificate reporting and additional reports not included in 2017 package.
3.0	1 May 2023	Updated to reflect • New Network Security reports • New S/MIME certificate reporting • Changes to reporting for Code Signing reports to incorporate Principle 4 • Baseline reporting, Code Signing reporting and Verified Mark Certificate reporting once new Network Security reports are issued separately • Potential use of “statement” in place of “assertion” • Changes in quality control reporting in reports effective for engagements beginning on or after December 14, 2022 • Other minor corrections where applicable

Acknowledgements

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

Members of the Task Force are:

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

CPA Canada Support

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

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

Table of Contents

Reporting Guidance

Professional Standards

As of the time of publication, illustrative assurance reports in this document have been prepared following the guidance from, and are intended to be issued under the following professional reporting 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, an engagement performed under CSAE 3000 was preferred for WebTrust for CA reporting. Management's assertion was felt to be an important component of the engagement and reporting as it was a clear public demonstration of management's responsibility for the PKI operation being reported on. If there was a qualification, direct reporting was typically used.

The Task Force is of the opinion that 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 practitioner 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.

Reporting on Code-Signing Engagements

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

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

Reporting On Network Security Requirements

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

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

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

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

Public Disclosure of CA Business Practices

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

At least one type of document (CP or CPS) is required to be "publicly available" to relying 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 Facilities

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

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

List of Root and Subordinate CAs in Scope

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

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

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

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

Disclosure of Changes in Scope or Roots with no Activity

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

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

Reference to Applicable WebTrust Principles and Criteria

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

Date Formats

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

Reporting on Subscriber Registration Activities

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

Where external RAs are used

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

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

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

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

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

Qualified Assurance Reports

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

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

1. If Management has not modified its assertion (the assertion states they meet the criteria even though matters of non-compliance were identified)

   The practitioner will assess the materiality and pervasiveness of the matter(s) of non-compliance and determine if the effects or possible effects of a matter are:

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

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

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

   The practitioner can issue:

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

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

Rather, when CSAE 3000 is used for reporting, the second option should be used. This option is shown as example CA1.5.

Under CSAE 3001, the practitioner reports directly on the subject matter and applicable criteria since there is no management assertion provided for these engagements. When the practitioner issues a qualified report, it is referenced to the subject matter and applicable criteria. When a report is issued 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[1]

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

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

1 Subheadings are optional and can be removed if desired.

2 Hyperlink to assertion.

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

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

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

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

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

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

  - subscriber information is properly authenticated (for the registration activities performed by ABC-CA); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to 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.[9]

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

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

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[12] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control[13]

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.

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

10 Remove bracketed text if external RAs are not used.

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

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

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

[The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][14]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][15]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[16] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion[17] is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
2. selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

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

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

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

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

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

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

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

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][19]

Firm Name
City, State/Province, Country
Report Date

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

19 Remove bracketed text if a seal is not issued.

Example CA1.2 – Unqualified opinion, attestation engagement, point in time

INDEPENDENT ASSURANCE REPORT

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

Scope[20]

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

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

20 Subheadings are optional and can be removed if desired.

21 Hyperlink to assertion.

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

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

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

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

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

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

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to 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.[28]

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

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

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[31] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control[32]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][33]

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

29 Remove bracketed text if external RAs are not used.

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

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

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

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

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][34]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[35] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

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

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

The suitability of the design of the controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access

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

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

to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,[36] 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

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

Example CA1.3 – Unqualified opinion, direct engagement, period of time

INDEPENDENT ASSURANCE REPORT

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

Scope[37]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,[38] whether ABC-CA

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][39]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][40]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[41]
- 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

37 Subheadings are optional and can be removed if desired.

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

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

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

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

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][42] in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.[43]

[(If external RAs are used) ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.][44]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.][45]

Certification authority's responsibilities

ABC-CA's management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles Criteria for Certification Authorities v2.x.[46]

Our independence and quality control[47]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][48]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate

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

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

44 Remove bracketed text if external RAs are not used.

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

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

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

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

a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][49]

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities v2.x (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements*. 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.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

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

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)][50]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][51]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[52]
- 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.

50 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.

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

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

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.][53]

Firm Name

City, State/Province, Country

Report Date

53 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[54]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[55, 56] that for its Certification Authority (CA) operations at <LOCATION>,[57] throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[58] 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)][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

54 Subheadings are optional and can be removed if desired.

55 Hyperlink to assertion.

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

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

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

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.

- 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.[62]

[(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.][63]

[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.][64]

Certification authority's responsibilities
ABC-CA's management is responsible for its assertion,[65] 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[66]
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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][67]

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

63 Remove bracketed text if external RAs are not used.

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

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

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

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

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][68]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[69] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- obtaining an understanding of ABC-CA's 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;
- selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
- testing and evaluating the operating effectiveness of the controls; and
- performing such other procedures as we considered necessary in the circumstances.

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems

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

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

and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

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

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

This caused WebTrust Criterion 3.4 which reads:

The CA maintains controls to provide reasonable assurance that:

- *physical access to CA facilities and equipment is limited to 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,[70] 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

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

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[71]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[72] that, except for matters described in the assertion,[73] for its Certification Authority (CA) operations at <LOCATION>,[74] throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[75] ABC-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][76]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][77]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[78]
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by ABC-CA); and

71 Subheadings are optional and can be removed if desired.

72 Hyperlink to assertion.

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

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

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

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

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

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

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.[79]

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

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.][81]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[82] 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[83]

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.

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

80 Remove bracketed text if external RAs are not used.

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

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

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

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

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][85]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[86] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- obtaining an understanding of ABC-CA's 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;
- selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
- testing and evaluating the operating effectiveness of the controls; and
- performing such other procedures as we considered necessary in the circumstances.

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

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

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

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

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)][87]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][88]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[89]
- 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

87 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.

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

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

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

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

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[90]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,[91] whether ABC-CA

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][92]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][93]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[94]
- 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

90 Subheadings are optional and can be removed if desired.

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

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

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

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

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][95] in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.[96]

[(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.][97]

[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.][98]

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.[99]

Our independence and quality control[100]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][101]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate

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

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

97 Remove bracketed text if external RAs are not used.

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

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

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

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

a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][102]

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities v2.x (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements*. 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.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

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

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)][103]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][104]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[105]
- 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

103 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.

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

105 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[106]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[107, 108] that for its Certification Authority (CA) operations at <LOCATION>,[109] throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[110] 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)][111]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][112]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[113]
- 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

106 Subheadings are optional and can be removed if desired.

107 Hyperlink to assertion.

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

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

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

111 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.

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

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

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to 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.[114]

[(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.][115]

[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.][116]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[117] 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[118]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][119]

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

115 Remove bracketed text if external RAs are not used.

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

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

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

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

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][120]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[121] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
2. selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

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

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

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. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.8 to not be met.	3.8: The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum: • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • the storage of backups of systems, data and configuration information at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery. The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation or degradation of the CA's services.

Qualified opinion

In our opinion, except for the matters described in the table presented in the basis for qualified opinion section above, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,[122] 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

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

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	6D5A 334C 1BAF 569E	rsaEncryption	(4096 bit)	sha256 WithRSA Encryption	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	7DAA AF3C F15F 8F45	rsaEncryption	(2048 bit)	sha256 WithRSA Encryption	Mar 14 01:25:41 2017 GMT	Mar 14 01:25:41 2027 GMT	92:A4:60:D 4:ED:AC:57 :3D:C2:1B:2 4:07:0D: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	8FAB AF6C F45F 884F	rsaEncryption	(2048 bit)	sha256 WithRSA Encryption	Apr 22 07:41:53 2017 GMT	Apr 22 07:41:53 2027 GMT	92:A4:60: D4:ED:AC :57:3D:C2: 1B:24:07:0 D: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,[123] Period of Time

ABC-CA MANAGEMENT'S ASSERTION[124]

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

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

The management of ABC-CA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website [or other repository location],[127] CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, 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.

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

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

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

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

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

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its Certification Authority (CA) services at <LOCATION>,[128] 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)][129]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][130]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[131]
- 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

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

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

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

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

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

CA Business Practices Disclosure

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

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

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

133 Remove bullets that are not applicable.

- CA Key Escrow

Subscriber Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

[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[134] does not extend to controls that would address those criteria.][135]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

Example MA1.2 – Management's Assertion,[136] Point in Time

ABC-CA MANAGEMENT'S ASSERTION[137]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],[138] and provides the following CA services:[139]

- 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],[140] 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.

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

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

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

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

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

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its Certification Authority (CA) services at <LOCATION>,[141] 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)][142]
- 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)][143]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[144]
- 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

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

142 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.

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

144 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,[145] including the following:[146]

CA Business Practices Disclosure

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

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

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

146 Remove bullets that are not applicable.

- CA Key Escrow

Subscriber Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

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

Example MA1.3 – Management's Assertion,[147] Period of Time – Modified Assertion Accompanying Qualified Report Example CA1.5

ABC-CA MANAGEMENT'S ASSERTION[148]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],[149] and provides the following CA services:[150]

- 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],[151] 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.

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

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

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

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

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

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

	Observation	Relevant WebTrust Criteria
1	We noted that electronic and auditable dual-custody multi-factor entrance and exit controls to secure PKI area were not implemented. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.4 to not be met.	3.4: The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorised individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented
2	We noted that a sufficient disaster recovery plan was not developed and tested. Additionally, physically secure disaster recovery facilities were not available. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.8 to not be met.	3.8: The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum: • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • the storage of backups of systems, data and configuration information at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery. The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation or degradation of the CA's services.

Based on that assessment, in ABC-CA management's opinion, except for the matters described in the preceding table, in providing its Certification Authority (CA) services at <LOCATION>,[152] 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)][153]
- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][154]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[155]
- 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

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

153 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.

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

155 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,[156] including the following:[157]

CA Business Practices Disclosure

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

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Escrow

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

157 Remove bullets that are not applicable.

Subscriber Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our assertion[158] does not extend to controls that would address those criteria.][159]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

159 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[160]

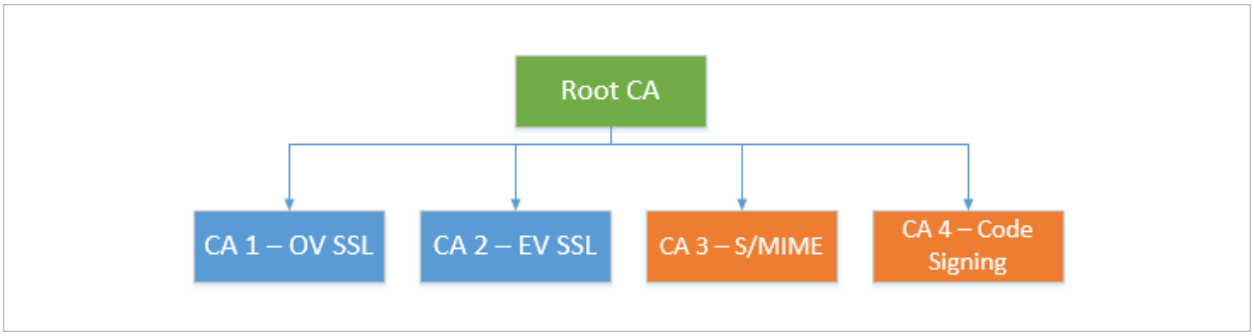
Currently, the SSL Baseline with Network Security principles and criteria incorporates two different CA/Browser Forum requirements documents:

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

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

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

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



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

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

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

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[161]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[162, 163] that for its Certification Authority (CA) operations at <LOCATION>,[164] 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]],[165, 166] 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)],[167]

  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

161 Subheadings are optional and can be removed if desired.

162 Hyperlink to assertion.

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

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

165 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.

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

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

— CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

[[And, for its [list of Root and Subordinate CAs in scope for Network Security Requirements]]:[168]

- 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]][169]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][170] v2.x.[171]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[172] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][173] v2.x.

Our independence and quality control[174]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][175]

168 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.

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

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

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

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

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

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

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

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][176]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[177] 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*. 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 obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[178]
2. selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems

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

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

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

and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,[179] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][180] v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][181] 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][182] 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.][183]

Firm Name
City, State/Province, Country
Report Date

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

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

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

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

183 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[184]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[185, 186] that for its Certification Authority (CA) operations at <LOCATION>,[187] 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]],[188, 189] 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)],[190]

  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
- 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

184 Subheadings are optional and can be removed if desired.

185 Hyperlink to assertion.

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

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

188 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.

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

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

[[And, for its [list of Root and Subordinate CAs in scope for Network Security Requirements]]:[191]

- 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][192]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][193] v2.x.[194]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[195] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][196] v2.x.

Our independence and quality control[197]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][198]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate

191 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.

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

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

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

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

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

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

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

a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][199]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion,[200] 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*. 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 obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[201]
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

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

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

The suitability of the design of the controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

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

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

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

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

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,[202] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][203] v2.x.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][204] 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

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

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

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

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

INDEPENDENT ASSURANCE REPORT

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

Scope[205]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,[206] whether ABC-CA has

- disclosed its SSL certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)],[207]

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

throughout the period <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for SSL Baseline Requirements and [Network Security Requirements],[208]

205 Subheadings are optional and can be removed if desired.

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

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

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

[[And, for CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Network Security Requirements]]:[209]

- 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][210]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL [Baseline with Network Security][211] v2.x.[212]

Certification authority's responsibilities

ABC-CA's management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][213] v2.x.[214]

Our independence and quality control[215]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][216]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate

209 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.

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

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

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

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

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

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

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

a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][217]

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][218] v2.x (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements*. 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 obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[219]
2. selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems

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

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

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

and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA 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)],[220]

  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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][221] v2.x.

[[And, for CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Network Security Requirements]]:[222]

- 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][223]

220 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.

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

222 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.

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

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with [Network Security][224] 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][225] 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.][226]

Firm Name

City, State/Province, Country

Report Date

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

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

226 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,[227] Period of Time

ABC-CA MANAGEMENT'S ASSERTION[228]

[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][229]][230] and provides SSL CA services.][231]

[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][232] and provides non-SSL CA services.][233, 234]

The management of ABC-CA is responsible for establishing and maintaining effective controls over its SSL [and non-SSL][235] CA operations, including [its network and certificate security system controls],[236] its SSL CA business practices disclosure on its website [or other repository location],[237] SSL key lifecycle management controls, and SSL certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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

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

229 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.

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

231 Include this introductory paragraph if all CAs are SSL CAs and therefore in scope for SSL Baseline Requirements and Network Security Requirements.

232 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.

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

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

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

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

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

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its SSL [and non-SSL][238] Certification Authority (CA) services at <LOCATION>,[239] throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)],[240]

  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
- [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][241]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][242] v2.x.[243]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

240 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.

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

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

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

Example MA2.2 – Management's Assertion,[244] Point in Time

ABC-CA MANAGEMENT'S ASSERTION[245]

[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]][246, 247] and provides SSL CA services.][248]

[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][249] and provides non-SSL CA services.][250]

The management of ABC-CA is responsible for establishing controls over its SSL [and non-SSL][251] CA operations, including [its network and certificate security system controls,][252] its SSL CA business practices disclosure on its website [or other repository location],[253] SSL key lifecycle management controls, and SSL certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, controls placed into operation can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations.

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

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

246 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.

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

248 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 the scope of the engagement is only the Network Security Requirements.

249 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.

250 Include this introductory paragraph if there are additional non-SSL CAs that are in scope for the Network Security Requirements or if the scope of the engagement is only the Network Security Requirements. Remove this paragraph if all in-scope CAs are SSL.

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

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

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

ABC-CA management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in ABC-CA management's opinion, in providing its SSL [and non-SSL][254] Certification Authority (CA) services at <LOCATION>,[255] 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)],[256]

  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
- [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][257]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline [with Network Security][258] v2.x.[259]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

256 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.

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

258 Delete if separate WebTrust for Network Security Report is issued

259 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[260]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[261, 262] that for its Certification Authority (CA) operations at <LOCATION>,[263] throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[264] 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)][265]

  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)

260 Subheadings are optional and can be removed if desired.

261 Hyperlink to assertion.

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

263 CA processing locations as defined in the "Reporting Guidance" section

264 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.

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x.[266]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[267] 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[268]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][269]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][270]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[271] 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*. 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:

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

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

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

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

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

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

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

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,[272] 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.

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

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – Extended Validation SSL Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][273]

Firm Name

City, State/Province, Country

Report Date

273 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[274]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[275, 276] that for its Certification Authority (CA) operations at <LOCATION>,[277] as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[278] 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)][279]

  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.[280]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[281] 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.

274 Subheadings are optional and can be removed if desired.

275 Hyperlink to assertion.

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

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

278 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.

279 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.

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

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

Our independence and quality control[282]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][283]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][284]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[285] 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*. 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.

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

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

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

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

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

The suitability of the design of the controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,[286] 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

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

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

INDEPENDENT ASSURANCE REPORT

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

Scope[287]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,[288] whether ABC-CA has

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][289]

  including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

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

Certification authority's responsibilities

ABC-CA's management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x.[290]

287 Subheadings are optional and can be removed if desired.

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

289 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.

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

Our independence and quality control[291]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][292]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][293]

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, Direct Engagements. 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.

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

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

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

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

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

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][294]

  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.

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

This report does not include any representation as to the quality of ABC-CA’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x, nor the suitability of any of ABC-CA’s services for any 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.][295]

Firm Name

City, State/Province, Country

Report Date

295 Remove bracketed text if a seal is not issued.

Management's Assertion

Example MA3.1 – Management's Assertion,[296] Period of Time

ABC-CA MANAGEMENT'S ASSERTION[297]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],[298] 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],[299] 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>,[300] 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)][301]

  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:

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

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

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

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

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

301 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.[302]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

Example MA3.2 – Management's Assertion,[303] Point in Time

ABC-CA MANAGEMENT'S ASSERTION[304]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],[305] 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],[306] 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>,[307] 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)][308]

  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

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

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

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

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

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

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

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x.[309]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

WebTrust for Certification Authorities – Code Signing ("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[310]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[311, 312] that for its Certification Authority (CA) operations at <LOCATION>,[313] throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[314] ABC-CA has:

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][315]

  including its commitment to provide CS certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.

310 Subheadings are optional and can be removed if desired.

311 Hyperlink to assertion.

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

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

314 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.

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

- maintained effective controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x
- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]][316] maintained effective controls to provide reasonable assurance that:
  - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[317]]

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

Certification Authority's responsibilities

ABC-CA's management is responsible for its assertion,[318] including the fairness of its presentation, and the provision of its described services, based on [the WebTrust Principles and Criteria for Certification Authorities – Code Sign Baseline Requirements v3.x.[319]

Our independence and quality control[320]

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.

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

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

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

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

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

[The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][321]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][322]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[323] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's CS [and EVCS][324] certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of CS [and EVCS] certificates, CS [and EVCS] Signing Authority certificates, and CS [and EVCS] Timestamp Authority certificates [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[325]
2. selectively testing transactions executed in accordance with disclosed CS [and EVCS] certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

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

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

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

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

324 If applicable.

325 Delete if separate WebTrust for Network Security Report is issued

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent Limitations

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

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,[326] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Code Sign Baseline Requirements v3.x.

This report does not include any representation as to the quality of ABC-CA's services other than its CA operations at *<LOCATION>,*[327] nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – Code Signing Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][328]

Firm Name
City, State/Province, Country
Report Date

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

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

328 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[329]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[330, 331] that for its Certification Authority (CA) operations at <LOCATION>,[332] throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[333] ABC-CA has:

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][334]

  including its commitment to provide CS certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - CS subscriber information is properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.
- suitably designed, and placed into operation, controls to provide reasonable that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x.[335]

329 Subheadings are optional and can be removed if desired.

330 Hyperlink to assertion.

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

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

333 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.

334 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.

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

- For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]][336]

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

  — EV CS subscriber information is properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;

  — The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.

- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[337]]

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

Certification Authority's responsibilities

ABC-CA's management is responsible for its assertion,[338] including the fairness of its presentation, and the provision of its described services, based on [the WebTrust Principles and Criteria for Certification Authorities – Code Sign Baseline Requirements v3.x.[339]

Our independence and quality control[340]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][341]

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

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

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

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

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

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

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][342]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[343] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's CS [and EVCS][344] certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of CS [and EVCS] certificates, CS [and EVCS] Signing Authority certificates, and CS [and EVCS] Timestamp Authority certificates [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[345]
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

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

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

The suitability of the design of the controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

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

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

344 If applicable.

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

Inherent limitations

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

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,[346] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – for Certification Authorities – Code Sign Baseline Requirements v3.x.

This report does not include any representation as to the quality of ABC-CA's services other than its CA operations at *<LOCATION>,*[347] nor the suitability of any of ABC-CA's services for any customers intended purpose.

Firm Name

City, State/Province, Country

Report Date

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

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

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

INDEPENDENT ASSURANCE REPORT

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

Scope[348]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,[349] whether ABC-CA has

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][350]

  including its commitment to provide CS certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.
- maintained effective controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x
- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]][351] maintained effective controls to provide reasonable assurance that:
  - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;

348 Subheadings are optional and can be removed if desired.

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

350 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.

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

  - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[352]

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

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

Our independence and quality control[353]
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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][354]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][355]

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

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

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

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

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – Authorities – Code Signing Baseline Requirements v3x., 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's CS [and EVCS][356] certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of CS [and EVCS] certificates, CS [and EVCS] Signing Authority certificates, and CS [and EVCS] Timestamp Authority certificates [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[357]
2. selectively testing transactions executed in accordance with disclosed CS [and EVCS] certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and performing such other procedures as we considered necessary in the circumstances.

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

356 If applicable.

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

Opinion

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

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][358]

  including its commitment to provide CS certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.
- maintained effective controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x
- For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]][359] maintained effective controls to provide reasonable assurance that:
  - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[360]]

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

358 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.

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

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

This report does not include any representation as to the quality of ABC-CA's services other than its *Certification Authority (CA) operations at <LOCATION>,*[361] nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – Code Signing Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][362]

Firm Name
City, State/Province, Country
Report Date

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

362 Remove bracketed text if a seal is not issued.

Management's Assertion

Example MA4.1 – Management's Assertion,[363] period of time

ABC-CA MANAGEMENT'S ASSERTION[364]

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

The management of ABC-CA is responsible for establishing and maintaining effective controls over its code signing services, including [its network and certificate security system controls],[365] its code signing business practices disclosure on its website, code signing key lifecycle management controls, and certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][366]

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

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

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

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

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

  - CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.
- maintained effective controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x
- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]][367]

  maintained effective controls to provide reasonable assurance that:
  - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[368]]

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

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

Example MA4.2 – Management's Assertion,[369] Point in Time

ABC-CA MANAGEMENT'S ASSERTION[370]

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

The management of ABC-CA is responsible for establishing and maintaining effective controls over its code signing services, including [its network and certificate security system controls],[371] its code signing business practices disclosure on its website, code signing key lifecycle management controls, and certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, 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 CS CA services. Based on that assessment, in ABC-CA management's opinion, in providing its CS CA services at <LOCATION>,[372] as of <DATE>, ABC-CA has:

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][373]

  including its commitment to provide CS certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.

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

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

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

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

373 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 CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v1.x
- [For CAs as enumerated in Attachment B are only in scope for [or [list of Root and Subordinate CAs in scope for Principle 3: Extended Validation Code Signing Service Requirements]][374] suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.
- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[375]]

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

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

WebTrust for Certification Authorities – Network Security ("NS")

Canadian Standards – CSAE 3000/3001

Example CA5.1 – Unqualified Opinion, Attestation Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope[376]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[377, 378] that for its Certification Authority (CA) operations at <LOCATION>,[379] throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope], ABC-CA has:

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.[380]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[381] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.

376 Subheadings are optional and can be removed if desired

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

378 Hyperlink to assertion.

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

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

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

Our independence and quality control[382]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][383]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][384]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[385] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion[386] is fairly stated, and, accordingly, included:

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

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

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

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

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

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

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,[387] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.

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

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][388]

Firm Name

City, State/Province, Country

Report Date

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

388 Remove bracketed text if a seal is not issued.

Example CA5.2 – Unqualified Opinion, Attestation Engagement, Point in Time

INDEPENDENT ASSURANCE REPORT

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

Scope[389]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[390, 391] that for its Certification Authority (CA) operations at <LOCATION>,[392] as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope], ABC-CA has:

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.[393]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[394] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.

Our independence and quality control[395]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][396]

389 Subheadings are optional and can be removed if desired.

390 Hyperlink to assertion.

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

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

393 Include applicable version number and hyperlink to the criteria document

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

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

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

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][397]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion,[398] 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.* This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion[399] is fairly stated, and, accordingly, included:

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

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

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

The suitability of the design of the controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems

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

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

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

and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,[400] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.

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

Firm Name
City, State/Province, Country
Report Date

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

Example CA5.3 – Unqualified Opinion, Direct Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope[401]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,[402] whether ABC-CA has

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

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

Certification authority's responsibilities

ABC-CA's management is responsible for its controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1. x.[403]

Our independence and quality control[404]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][405]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate

401 Subheadings are optional and can be removed if desired.

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

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

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

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

a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][406]

Practitioner's responsibilities

Our responsibility is to express an opinion on the conformity of ABC-CA management's controls with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all significant respects, management's controls conform to the WebTrust Criteria, and, accordingly, included:

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

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

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

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

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

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

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

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities –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.][407]

Firm Name

City, State/Province, Country

Report Date

407 Remove bracketed text if a seal is not issued.

Management's Assertion

Example MA5.1 – Management's Assertion,[408] Period of Time

ABC-CA MANAGEMENT'S ASSERTION[409]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope] and provides SSL [and non-SSL][410] CA services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its SSL [and non-SSL][411] CA operations, including its network and certificate security system controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its SSL [and non-SSL][412] Certification Authority (CA) services at <LOCATION>,[413] throughout the period <DATE> to <DATE>, ABC-CA has:

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.[414]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

410 If applicable, otherwise delete.

411 If applicable, otherwise delete.

412 If applicable, otherwise delete.

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

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

Example MA5.2 – Management's Assertion,[415] Point in Time

ABC-CA MANAGEMENT'S ASSERTION[416]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope] and provides SSL [and non-SSL][417] CA services.

The management of ABC-CA is responsible for establishing controls over its SSL [and non-SSL][418] CA operations, including its network and certificate security system controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, controls placed into operation can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations.

ABC-CA management has assessed its controls over its SSL CA services. Based on that assessment, in ABC-CA management's opinion, in providing its SSL [and non-SSL][419] Certification Authority (CA) services at <LOCATION>,[420] as of <DATE>, ABC-CA has:

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.x.[421]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

417 If applicable, otherwise delete.

418 If applicable, otherwise delete.

419 If applicable, otherwise delete.

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

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

WebTrust for Certification Authorities – S/MIME Certificates ("S/MIME")

Canadian Standards – CSAE 3000/3001

Example CA6.1 – Unqualified Opinion, Attestation Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope[422]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[423, 424] that for its Certification Authority (CA) operations at <LOCATION>,[425] throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[426] ABC-CA has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)],[427]

  including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;

422 Subheadings are optional and can be removed if desired.

423 Hyperlink to assertion.

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

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

426 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.

427 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 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
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference][428]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.[429]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[430] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.

Our independence and quality control[431]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][432]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][433]

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

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

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

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

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

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

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[434] 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.* This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion[435] is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates, [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[436]
2. selectively testing transactions executed in accordance with disclosed S/MIME certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

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

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

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

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,[437] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.

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

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – S/MIME Certificates Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][438]

Firm Name

City, State/Province, Country

Report Date

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

438 Remove bracketed text if a seal is not issued.

Example CA6.2 – Unqualified Opinion, Attestation Engagement, Point in Time

INDEPENDENT ASSURANCE REPORT

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

Scope[439]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[440, 441] that for its Certification Authority (CA) operations at <LOCATION>,[442] as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[443] ABC-CA has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)],[444]

  including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirement on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to 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

439 Subheadings are optional and can be removed if desired.

440 Hyperlink to assertion.

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

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

443 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.

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

- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[445]]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.[446]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[447] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.

Our independence and quality control[448]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][449]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][450]

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

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

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

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

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

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

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[451] 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.* This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion[452] is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates, [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[453]
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

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

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

The suitability of the design of the controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

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

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

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

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

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,[454] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.

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

Firm Name

City, State/Province, Country

Report Date

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

Example CA6.3 – Unqualified Opinion, Direct Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope[455]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,[456] whether ABC-CA has

- disclosed its S/MIME certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)],[457]

  including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[458]]

throughout the period <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.[459]

455 Subheadings are optional and can be removed if desired.

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

457 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.

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

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

Certification authority's responsibilities
ABC-CA's management is responsible for its disclosures and controls, including the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1. x.

Our independence and quality control[460]
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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][461]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][462]

Practitioner's responsibilities
Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements.* 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 S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates, [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[463]

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

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

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

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

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

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

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

- disclosed its S/MIME certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)],[464]

  including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- maintained effective controls to provide reasonable assurance that:

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

  - logical and physical access to CA systems and data is restricted to 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
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[465]]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.

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

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – S/MIME Certificates Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][466]

Firm Name

City, State/Province, Country

Report Date

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

466 Remove bracketed text if a seal is not issued.

Management's Assertion

Example MA6.1 – Management's Assertion,[467] Period of Time

ABC-CA MANAGEMENT'S ASSERTION[468]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][469] and provides S/MIME CA services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including [its network and certificate security system controls],[470] its S/MIME CA business practices disclosure on its website [or other repository location, S/MIME key lifecycle management controls, and S/MIME certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its S/MIME CA services at <LOCATION>,[471] throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)],[472]

  including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:

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

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

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

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

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

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

  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to 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
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference][473]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.[474]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

Example MA6.2 – Management's Assertion,[475] Point in Time

ABC-CA MANAGEMENT'S ASSERTION[476]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope[477] and provides S/MIME CA services.

The management of ABC-CA is responsible for establishing controls over its S/MIME CA operations, including [its network and certificate security system controls],[478] its S/MIME CA business practices disclosure on its website [or other repository location],[479] S/MIME key lifecycle management controls, and S/MIME certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, controls placed into operation can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its S/MIME CA services. Based on that assessment, in ABC-CA management's opinion, in providing its S/MIME Certification Authority (CA) services at <LOCATION>,[480] as of <DATE>, ABC-CA has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)],[481]

  including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirement on the ABC-CA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:

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

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

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

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

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

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

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

  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by ABC-CA)
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to 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
- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference][482]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.x.[483]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

Lifecycle Reports

In addition to the reports discussed in the prior section, the Browser community, as part of their trusted root programs, are requesting reports covering key components of a root key's lifecycle. Included in this section are reports covering:

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

Canadian Standards – CSAE 3000/3001

Example CA7.1 – Root Key Generation Ceremony, attestation engagement

INDEPENDENT ASSURANCE REPORT

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

Scope[484]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[485, 486] that in generating and protecting its [list of Root CAs witnessed] (collectively, "ABC-CA Root CAs") on <DATE>[487] at <LOCATION>,[488] 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)][489]
- 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)

484 Subheadings are optional and can be removed if desired.

485 Hyperlink to assertion.

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

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

488 Location of the key generation ceremony.

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

- performed, during the root key generation process, all procedures required by the Root Key Generation Script(s)
- generated the CA keys in a physically secured environment as described in its CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x.[490]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[491] 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[492]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][493]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][494]

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

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

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

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

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

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[495] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion[496] is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's documented plan of procedures to be performed for the generation of the certification authority key pairs for the ABC-CA Root CAs;
2. reviewing the detailed CA key generation script(s) for conformance with industry standard practices;
3. testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;
4. physical observation of all procedures performed during the root key generation process to ensure that the procedures actually performed on <DATE> were in accordance with the Root Key Generation Script(s) for the ABC-CA Root CAs; and
5. performing such other procedures as we considered necessary in the circumstances.

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

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,[497] 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

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

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

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

Management's Assertion

Example MA7.1 – Management's Assertion[498]

ABC-CA MANAGEMENT'S ASSERTION[499]

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][500] CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x.[501]

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>[502] at <LOCATION>,[503] with the following identifying information:

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

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

500 Use "in accordance with" for Canadian and International standards. Use "based on" for US standards.

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

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

503 Location of the key generation ceremony.

Root name	Subject key identifier	Certificate serial number
ABC-CA Root CA 1	0a:4b:33:d1:f9:a8:9f:33:12:00:ab	14:2b:c7:d1
ABC-CA Root CA 2	8f:7d:c4:33:19:0a:0b:de:f1:42:11	1b:23:d4:f2

ABC-CA has:

- followed the CA key generation and protection requirements in its:
  - [name and version of certification practice statement]; and
  - [name and version of certificate policy (if applicable)][504]
- included appropriate, detailed procedures and controls in its Root Key Generation Script(s):
  - [name, version number, and date of root key generation script(s). This may also include additional scripts such as server build scripts]
- maintained effective controls to provide reasonable assurance that the ABC-CA Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Script(s)
- performed, during the root key generation process, all procedures required by the Root Key Generation Script(s)
- generated the CA keys in a physically secured environment as described in its CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x.[505]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

504 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.

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

Reporting on Life Cycle

Canadian Standards – CSAE 3000/3001

Example CA7.2 – Unqualified opinion, attestation engagement (for various lifecycle events), period of time

INDEPENDENT ASSURANCE REPORT

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

Scope[506]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[507] that in managing the key lifecycle events for its Certification Authority ("CA") private keys and/or key pairs (include if applicable keys not yet associated with a specific CA) contained on assets at <LOCATION(S)>,[508] throughout the period <DATE> to <DATE> for its CA keys enumerated in Attachment A,[509] ABC CA has:

- disclosed its key lifecycle management requirements in its
  - — [name and version of certification practice statement(s)]; and
  - — [name and version of its certificate policy(ies) (if applicable)]

  and followed such key lifecycle management requirements.

[if WTCA criteria 4.2 is applicable][510]

- maintained effective controls to provide reasonable assurance that keys are backed up, stored, and recovered by authorized personnel in trusted roles using multiple person control in a physically secured environment

[if WTCA criteria 4.4 is applicable]

- maintained effective controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations

[if WTCA criteria 4.6 is applicable]

- maintained controls to provide reasonable assurance that:

506 Subheadings are optional and can be removed if desired.

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

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

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

510 Include only those criteria applicable to the current reporting.

  - copies of keys that no longer serve a valid business purpose are destroyed in accordance with ABC CA's disclosed business practices; and
  - copies of keys are completely destroyed at the end of the key pair life cycle in accordance with ABC CA's disclosed business practices

[if WTCA criteria 4.8 is applicable]

- maintained effective controls to provide reasonable assurance that:
  - devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity;
  - access to CA cryptographic hardware is limited to authorized personnel in trusted roles using multiple person control; and
  - CA cryptographic hardware is functioning correctly

[if WTCA 4.10 criteria is applicable]

- maintained effective controls to provide reasonable assurance that:
  - private keys that are physically transported from one facility to another remain confidential and maintain their integrity;
  - hardware containing keys and associated activation materials are prepared for transport in a physically secure environment by authorized personnel in trusted roles using multiple person controls, and are transported within sealed tamper evident packaging;
  - keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and
  - key transportation events are logged

[if WTCA 4.11 criteria is applicable]

- maintained effective controls to provide reasonable assurance that:
  - keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration, are completed in a physically secure environment by authorized personnel in trusted roles using multiple person control;
  - hardware and software tools used during the key migration process are tested by authorized personnel in trusted roles using multiple person controls prior to the migration event; and
  - key migration events follow a documented script and are logged

in accordance with the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11[511] of the WebTrust Principles and Criteria for Certification Authorities v2.x.[512]

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

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

Certification Authority's responsibilities
ABC-CA's management is responsible for its assertion,[513] including the fairness of its presentation, and the provision of its described services in accordance with the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11[514] of the WebTrust Principles and Criteria for Certification Authorities v2.x.

Our independence and quality control[515]
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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][516]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][517]

Practitioner's responsibilities
Our responsibility is to express an opinion on management's assertion[518] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion[519] is fairly stated, and, accordingly, included:

- obtaining an understanding of ABC CA's documented plan of procedures to be performed for the key lifecycle management.

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

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

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

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

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

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

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

- reviewing the detailed key logs for conformance with industry standard practices and disclosed practices in the Certificate Policy and Certification Practice Statement.
- testing and evaluating the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the service.
- performing such other procedures as we considered necessary in the circumstances.

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,[520] as referred to above, is fairly stated, in all material respects, in accordance with the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11[521] of the WebTrust Principles and Criteria for Certification Authorities v2.x.[522]

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>,*[523] nor the suitability of any of ABC-CA's services for any customer's intended purpose.

Firm Name
City, State/Province, Country
Report Date

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

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

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

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

Attachment A – CAs In-Scope for Key Lifecycle Management Activities[524]

CA KEYS STORED, BACKUP, AND RECOVERED IN <LOCATION(S)>[525]

CA subject name	Subject key identifier	Certificate serial number	SHA256 thumbprint

KEY DESTRUCTION

CA subject name	Subject key identifier	Certificate serial number	SHA256 thumbprint

KEYS TRANSPORTED / MIGRATED FROM <LOCATION(S)>[526] TO <LOCATION(S)>[527]

CA subject name	Subject key identifier	Certificate serial number	SHA256 thumbprint

524 The tables below are provided as examples, but each CA should specify the level of detail they wish to disclose based on the needs of the users.

525 Include applicable location(s).

526 Include applicable location(s).

527 Include applicable location(s).

Management's Assertion[528]

Example MA7.2 – Management's Assertion[529] on Life Cycle

ABC-CA MANAGEMENT'S ASSERTION[530]

ABC CA, Inc. ("ABC CA") has deployed a public key infrastructure. As part of this deployment, it was necessary to implement and maintain effective key lifecycle management controls in managing the key lifecycle events of its Certification Authority ("CA") private keys and key pairs (include if applicable keys not yet associated with a specific CA) to ensure the integrity, confidentiality, and availability of private keys contained in assets at <LOCATION(S)>,[531] throughout the period January 1, 2XXX to December 31, 2XXX for its CA keys enumerated in Attachment A.[532]

The keys were managed in accordance with key lifecycle management requirements described in the Certificate Policy and Certification Practice Statement.

ABC CA management has maintained effective CA Key Lifecycle Management Controls based on the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11[533] of the WebTrust Principles and Criteria for Certification Authorities v2.x.[534] These controls were designed to provide reasonable assurance of adherence to these practices throughout the key lifecycle management process.

ABC CA management is responsible for establishing and maintaining procedures over its CA Key Lifecycle Management Controls, and over the integrity and confidentiality of all private keys and activation materials (including physical keys, tokens, and passwords) used in the establishment of the ABC CA keys, and for the CA environmental controls relevant to the protection of its keys.

ABC CA management has assessed the procedures and controls for the CA Key Lifecycle Management Controls. Based on that assessment, in management's opinion, in protecting its keys, ABC CA has:

- disclosed its key lifecycle management requirements in its
  - [name and version of certification practice statement(s)]; and
  - [name and version of its certificate policy(ies) (if applicable)]

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

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

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

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

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

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

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

and followed such key lifecycle management requirements.

[if WTCA 4.2 is applicable]

- maintained effective controls to provide reasonable assurance that keys are backed up, stored, and recovered by authorized personnel in trusted roles using multiple person control in a physically secured environment

[if WTCA 4.4 is applicable]

- maintained effective controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations

[if WTCA 4.6 is applicable]

- maintained controls to provide reasonable assurance that:
  - copies of keys that no longer serve a valid business purpose are destroyed in accordance with ABC CA's disclosed business practices; and
  - copies of keys are completely destroyed at the end of the key pair life cycle in accordance with ABC CA's disclosed business practices

[if WTCA 4.8 is applicable]

- maintained effective controls to provide reasonable assurance that:
  - devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity;
  - access to CA cryptographic hardware is limited to authorized personnel in trusted roles using multiple person control; and
  - CA cryptographic hardware is functioning correctly

[if WTCA 4.10 is applicable]

- maintained effective controls to provide reasonable assurance that:
  - private keys that are physically transported from one facility to another remain confidential and maintain their integrity;
  - hardware containing keys, and associated activation materials, are prepared for transport in a physically secure environment by authorized personnel in trusted roles using multiple person controls, and are transported within sealed tamper evident packaging;
  - keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and
  - keys transportation events are logged

[if WTCA 4.11 is applicable]

- maintained effective controls to provide reasonable assurance that:
  - keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration, are completed in a physically secure environment by authorized personnel in trusted roles using multiple person control;
  - hardware and software tools used during the keys migration process are tested by authorized personnel in trusted roles using multiple person controls prior to the migration event; and
  - keys migration events follow a documented script and are logged

in accordance with the applicable criteria in 4.2, 4.4, 4.6, 4.8, 4.10, and 4.11[535] of the WebTrust Principles and Criteria for Certification Authorities v2.x.[536]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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

WebTrust for Certification Authorities – Verified Mark Certificates

Canadian Standards – CSAE 3000/3001

Example CA8.1 – Unqualified opinion, attestation engagement, period of time

INDEPENDENT ASSURANCE REPORT

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

Scope[537]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[538, 539] that for its Certification Authority (CA) operations at <LOCATION>,[540] throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[541] ABC-CA has:

- disclosed its Verified Mark (VM) certificate practices and procedures in its
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][542]

  including its commitment to provide VM certificates in conformity with the applicable Minimum Security Requirements for Issuance of Verified Mark Certificates (VMC Guidelines), and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
  - The integrity of CA keys it manages is established and protected throughout their life cycles.

537 Subheadings are optional and can be removed if desired.

538 Hyperlink to assertion.

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

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

541 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.

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

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[543]]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.[544]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[545] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.

Our independence and quality control[546]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][547]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate

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

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

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

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

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

a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][548]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[549] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion[550] is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's VM certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of VM certificates [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[551]
2. selectively testing transactions executed in accordance with disclosed VM certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

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

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

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

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

Opinion

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion,[552] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.

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

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – Verified Mark Certificates Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][553]

Firm Name
City, State/Province, Country
Report Date

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

553 Remove bracketed text if a seal is not issued.

Example CA8.2 – Unqualified opinion, attestation engagement, point in time

INDEPENDENT ASSURANCE REPORT

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

Scope[554]

We have been engaged, in a reasonable assurance engagement, to report on ABC-CA management's assertion[555, 556] that for its Certification Authority (CA) operations at <LOCATION>,[557] as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope],[558] ABC-CA has:

- disclosed its Verified Mark (VM) certificate practices and procedures in its
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][559]

  including its commitment to provide VM certificates in conformity with the applicable Minimum Security Requirements for Issuance of Verified Mark Certificates (VMC Guidelines), and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
  - The integrity of CA keys it manages is established and protected throughout their life cycles.
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

554 Subheadings are optional and can be removed if desired.

555 Hyperlink to assertion.

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

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

558 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.

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

- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[560]]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.[561]

Certification authority's responsibilities

ABC-CA's management is responsible for its assertion,[562] including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.

Our independence and quality control[563]

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][564]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][565]

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

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

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

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

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

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

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion[566] 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*. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion[567] is fairly stated, and, accordingly, included:

1. obtaining an understanding of ABC-CA's VM certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of VM certificates [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[568]
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

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

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

The suitability of the design of the controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

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

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

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

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

Opinion

In our opinion, as of <DATE>, ABC-CA management's assertion,[569] as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.

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

Firm Name
City, State/Province, Country
Report Date

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

Example CA8.3 – Unqualified Opinion, Direct Engagement, Period of Time

INDEPENDENT ASSURANCE REPORT

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

Scope[570]

We have been engaged, in a reasonable assurance engagement, to report on, for its Certification Authority (CA) operations at <LOCATION>,[571] whether ABC-CA has

- disclosed its Verified Mark (VM) certificate practices and procedures in its
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][572]

  including its commitment to provide VM certificates in conformity with the applicable Minimum Security Requirements for Issuance of Verified Mark Certificates (VMC Guidelines), and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
  - The integrity of CA keys it manages is established and protected throughout their life cycles.
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[573]]

570 Subheadings are optional and can be removed if desired.

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

572 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.

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

throughout the period <DATE> to <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope] in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1. x.[574]

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

Our independence and quality control[575]
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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements* and, accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][576]

[The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.][577]

Practitioner's responsibilities
Our responsibility is to express an opinion on the conformity of ABC-CA management's disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x (the "WebTrust Criteria"), based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3001, *Direct Engagements*. This standard requires that we plan

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

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

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

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

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 VM certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of VM certificates [and obtaining an understanding of ABC-CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum];[578]
2. selectively testing transactions executed in accordance with disclosed VM certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

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

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

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

- disclosed its Verified Mark (VM) certificate practices and procedures in its
  - — [name and version of certification practice statement(s)]; and
  - — [name and version of certificate policy(ies) (if applicable)][579]

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

579 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.

including its commitment to provide VM certificates in conformity with the applicable Minimum Security Requirements for Issuance of Verified Mark Certificates (VMC Guidelines), and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
  - The integrity of CA keys it manages is established and protected throughout their life cycles.
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[580]]

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

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

Use of the WebTrust seal

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – Verified Mark Certificates Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][581]

Firm Name

City, State/Province, Country

Report Date

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

581 Remove bracketed text if a seal is not issued.

Management's Assertion

Example MA8.1 – Management's Assertion,[582] Period of Time

ABC-CA MANAGEMENT'S ASSERTION[583]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],[584] and provides Verified Mark (VM) Certificate services.

The management of ABC-CA is responsible for establishing and maintaining effective controls over its VM CA operations, including its VM CA business practices disclosure on its website [or other repository location],[585] VM key lifecycle management controls, and VM certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its VM CA services. Based on that assessment, in ABC-CA management's opinion, in providing its Certification Authority (CA) services at <LOCATION>,[586] throughout the period <DATE> to <DATE>, ABC-CA has:

- disclosed its Verified Mark (VM) certificate practices and procedures in its
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][587]

  including its commitment to provide VM certificates in conformity with the applicable Minimum Security Requirements for Issuance of Verified Mark Certificates (VMC Guidelines), and provided such services in accordance with its disclosed practices

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

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

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

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

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

587 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:
  - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
  - The integrity of CA keys it manages is established and protected throughout their life cycles.
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- [maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[588]]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.[589]

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

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

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

Example MA8.2 – Management's Assertion,[590] point in time

ABC-CA MANAGEMENT'S ASSERTION[591]

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope],[592] and provides Verified Mark (VM) Certificate services.

The management of ABC-CA is responsible for establishing controls over its VM CA operations, including its VM CA business practices disclosure on its website [or other repository location],[593] VM key lifecycle management controls, and VM certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, controls placed into operation can only provide reasonable assurance with respect to ABC-CA's Certification Authority operations.

ABC-CA management has assessed its disclosures of its certificate practices and controls over its VM CA services. Based on that assessment, in ABC-CA management's opinion, in providing its Certification Authority (CA) services at <LOCATION>,[594] as of <DATE>, ABC-CA has:

- disclosed its Verified Mark (VM) certificate practices and procedures in its
  - [name and version of certification practice statement(s)]; and
  - [name and version of certificate policy(ies) (if applicable)][595]

  including its commitment to provide VM certificates in conformity with the applicable Minimum Security Requirements for Issuance of Verified Mark Certificates (VMC Guidelines), and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - VMC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;

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

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

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

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

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

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

  - The integrity of CA keys it manages is established and protected throughout their life cycles.
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- [suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that are incorporated by reference.[596]]

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.x.[597]

<Signoff Name and Title>

<Date that matches the assurance opinion date>

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

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