WEBTRUST® FOR CERTIFICATION AUTHORITIES

Illustrative Reports Under SSAE 18

Version 1.0

Published 1 September 2017

Document History

Version	Publication Date	Revision Summary
1.0	1 May 2017	Initial publication- Conforming changes for SSAE 18.

Acknowledgements

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

Members of the Task Force are:

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

Significant support has been provided by:

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

CPA Canada Support

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

Table of Contents

Reporting Guidance

Professional Standards

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

- US –AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*) ("AT-C205")

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

CA Processing Locations

All reports issued should list the city, state/province (if applicable), and country of all physical locations used in CA operations. This includes data center locations (primary and alternate sites), registration authority locations (for registration authority operations performed by the CA), and all other locations where general IT and business process controls that are relevant to CA operations are performed.

List of Root and Subordinate CAs in Scope

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

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

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

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

Disclosure of Changes in Scope or Roots with no Activity

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

The XY (*Attachment A, CA #13*), YA (*Attachment A, CA #9*), L1 (*Attachment A, CA #10*), and Y2 (*Attachment A, CA #14*) CAs did not issue certificates during the period 1 month 2016 to 31 month 2017 and were maintained online to provide revocation status information only. The CA certificate for the XY CA expired on 5 January 2017 and was not renewed. The CA certificate for the YA CA was revoked on 2 February 2017 and was not re-issued.

Reference to Applicable Audit Criteria

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

Date Formats

Dates listed in the report and management's assertion should follow a consistent format with the full name of the month spelt out (i.e. 7 May 2016, or May 7, 2016). Numerical date formats (i.e. 07/05/2016 or 05/07/2016) should be avoided.

Reporting when 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 Certification Practice Statement and applicable Certificate Policy(s). The functions performed by these specific groups would typically be outside the scope of the WebTrust for Certification Authorities examination performed for the CA. In this case management's assertion should specify those aspects of the registration process that are not handled by the CA. External RAs could be examined and reported upon separately from the CA, using the relevant criteria contained in the relevant WebTrust Principles and Criteria for Certification Authorities Version being reported on. It is recommended that a separate paragraph be included audit report when external RAs are used:

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

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

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

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

Modified Opinions

SSAE 18, paragraph .79 states, "If the practitioner has concluded that conditions exist that, individually or in combination, result in one or more material misstatements based on the criteria, the practitioner should modify the opinion and should express a qualified or adverse opinion directly on the subject matter, not on the assertion, even when the assertion acknowledges the misstatement."

In such situations, the Task Force recommends that management's assertion be amended, and still attached to the audit report. It reflects management's acknowledgement of the issues causing the audit qualification.

WebTrust for Certification Authorities

US (AICPA) Standards – AT-C205

Example US1.1 – Unmodified Opinion, Reporting on Management's Assertion, Period of Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined ABC-CA management's assertion[1] that for its Certification Authority (CA) operations at <LOCATION>[2], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root Subordinate CAs in scope][3], ABC-CA has

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - [name and version of certification practice statement(s)]; and
    - [name and version of certificate policy(ies) (if applicable][4]

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

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

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

[1] Hyperlink to assertion
[2] CA processing locations as defined in the "Reporting Guidance" section
[3] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[4] At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet
[5] Remove bracketed text/bullet if CA has a combined CP and CPS document
[6] If CA has a combined CP/CPS then remove references to Certificate Policy

based on the WebTrust Principles and Criteria for Certification Authorities v2.x[7]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion, based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

[(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 examination did not extend to the controls exercised by these external registration authorities.][8]

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*[10], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][11]

[*Practitioner's signature*]
[*Practitioner's city and state*]

---

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

[8] Remove bracketed text if external RAs are not used

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

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

[12] Hyperlink to assertion

[*Date of practitioner's report*]

Example US1.2 – Unmodified Opinion, Reporting on Management's Assertion, Point in Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined ABC-CA management's assertion[12] that for its Certification Authority (CA) operations at <LOCATION>[13], as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][14], 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][15]

- 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)][16]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[17]

- 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 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

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

based on the WebTrust Principles and Criteria for Certification Authorities v2.x[18]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

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.

[(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 examination did not extend to the controls exercised by these external registration authorities.][19]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.][20]

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

In our opinion, management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*[21], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Practitioner's signature*]
[*Practitioner's city, and state*]

[18] Include applicable version number and hyperlink to the criteria document[19] Remove bracketed text if external RAs are not used[20] 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.
[19] Remove bracketed text if external RAs are not used[20] 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.
[20] 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.
[21] CA processing locations as defined in the "Reporting Guidance" section

[*Date of practitioner's report*]

Example US1.3 – Unmodified Opinion, Reporting on Subject Matter, Period of Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined for its Certification Authority (CA) operations at <LOCATION>[22],

a. ABC-CA's disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices.

b. the effectiveness of ABC-CA's controls over the

- consistency of its Certification Practice Statement with its Certificate Policy(ies) (if applicable)][23],
- provision of services in accordance with its [Certificate Policy (if applicable)][24] and Certification Practice Statement,
- establishment and protection of the integrity of keys and certificates it manages throughout their lifecycle,
- authenticity and confidentiality of subscriber and relying party information,
- continuity of key and certificate lifecycle management operations, and
- development, maintenance, and operation of CA systems integrity

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][25].

ABC-CA's management is responsible for these disclosures and for maintaining effective controls based on the WebTrust Principles and Criteria for Certification Authorities v2.x[26]. Our responsibility is to express an opinion based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

[22] CA processing locations as defined in the "Reporting Guidance" section
[23] Remove bracketed text if the CA publishes a combined CP/CPS
[24] Remove bracketed text if the CA publishes a combined CP/CPS
[25] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section

[(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 examination did not extend to the controls exercised by these external registration authorities.][27]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.][28]

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, throughout the period <DATE> to <DATE>, for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][29], in all material respects, ABC-CA

a. disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices.

b. maintained effective controls over the

   - consistency of its Certification Practice Statement with its Certificate Policy(ies) (if applicable)][30],
   - provision of services in accordance with its [Certificate Policy (if applicable)][31] and Certification Practice Statement,
   - establishment and protection of the integrity of keys and certificates it manages throughout their lifecycle,
   - authenticity and confidentiality of subscriber and relying party information,
   - continuity of key and certificate lifecycle management operations, and
   - development, maintenance, and operation of CA systems integrity

based on the WebTrust Principles and Criteria for Certification Authorities v2x.

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

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

[27] Remove bracketed text if external RAs are not used
[28] 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.
[29] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[30] Remove bracketed text if the CA publishes a combined CP/CPS
[31] Remove bracketed text if the CA publishes a combined CP/CPS

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - [name and version of certification practice statement(s)]; and
    - [name and version of certificate policy(ies) (if applicable][32]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][33]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[34]

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

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

based on 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 other than its *CA operations at <LOCATION>*[35], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[(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.][36]

[*Practitioner's signature*]
[*Practitioner's city, and state*]
[*Date of practitioner's report*]

[32] At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet
[33] Remove bracketed text/bullet if CA has a combined CP and CPS document
[34] If CA has a combined CP/CPS then remove references to Certificate Policy
[35] CA processing locations as defined in the "Reporting Guidance" section
[37] Hyperlink to assertion

Example US1.4 – Unmodified Opinion, Reporting on Management's Assertion, US Federal PKI and other Bridge CA Scenarios, Period of Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - ABC-CA Certificate Policy[40] (ies) Version X dated <DATE> ("ABC-CA CP") (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9)
    - ABC-CA Certification Practice Statement [41]Version X dated <DATE> ("ABC-CA CPS") that is consistent with the ABC-CA CP (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9); and
    - [if applicable] Memorandum of Agreement [42]dated <DATE> between the [Federal PKI Policy Authority][43] and ABC-CA ("ABC-MOA") (including all [or specified] sections [except XXX])

- provided its CA services in accordance with its disclosed practices, including:
    - ABC-CA CP (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9);
    - ABC-CA CPS that is consistent with the ABC-CA CP (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9); and
    - [if applicable] ABC-MOA (including all [or specified] sections [except XXX])

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

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - The continuity of key and certificate management operations is maintained; and

[37] Hyperlink to assertion
[38] CA processing locations as defined in the "Reporting Guidance" section
[39] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[40] Hyperlink to this document if available
[41] Hyperlink to this document if available
[42] Hyperlink to this document if available
[43] Replace bracketed text with the name of the appropriate policy authority in a different bridge scenario

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

based on the WebTrust Principles and Criteria for Certification Authorities v2.x[44].

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations. and we have not evaluated the effectiveness of such controls. [(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 examination did not extend to the controls exercised by these external registration authorities.][45]

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*[46], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

(*Practitioner signature)*
[*Practitioner's city, and state*]
[*Date of practitioner's report*]

[45] Remove bracketed text if external RAs are not used
[45] Remove bracketed text if external RAs are not used
[46] CA processing locations as defined in the "Reporting Guidance" section

Example US1.5A – Modified Opinion on Physical Security and Business Continuity, Report on Subject Matter, Period of Time – list issues

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined for ABC-CA's Certification Authority (CA) operations at <LOCATION>[47],

- ABC-CA's disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices, [the consistency of its Certification Practice Statement with its Certificate Policy (if applicable)][48], the provision of services in accordance with its [Certificate Policy (if applicable)][49] and Certification Practice Statement, and

- the effectiveness of ABC-CA's controls over key and certificate integrity, the authenticity and confidentiality of subscriber and relying party information, the continuity of key and certificate lifecycle management operations, and development, maintenance, and operation of CA systems integrity throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][50].

ABC-CA's management is responsible these disclosures and for maintaining effective controls, based on the WebTrust Principles Criteria for Certification Authorities v2.x[51]. Our responsibility is to express an opinion, based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

[(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 examination did not extend to the controls exercised by these external registration authorities.][52]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.][53]

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the

[47] CA processing locations as defined in the "Reporting Guidance" section
[48] Remove bracketed text if the CA publishes a combined CP/CPS
[49] Remove bracketed text if the CA publishes a combined CP/CPS
[50] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section

[52] Remove bracketed text if external RAs are not used
[53] 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.

examination to obtain reasonable assurance about whether, throughout the period <DATE> to <DATE>, for its [list of Root and Subordinate CAs in scope][54], in all material respects, ABC-CA,:

a. 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][55]

b. maintained effective controls to provide reasonable assurance that:

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

based on the WebTrust Principles and Criteria for Certification Authorities v2.x.

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

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

This caused WebTrust Criterion 3.4 which reads:

The CA maintains controls to provide reasonable assurance that:

- *physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control;*
- *CA facilities and equipment are protected from environmental hazards;*

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

[55] 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

[56] Remove bracketed text/bullet if CA has a combined CP and CPS document

[57] If CA has a combined CP/CPS then remove references to Certificate Policy

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

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

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

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

to not be met.

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

In our opinion, except for the matters described in the preceding paragraphs, 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][58]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][59]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[60]

- maintained effective controls to provide reasonable assurance that:

[58] 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

[59] Remove bracketed text/bullet if CA has a combined CP and CPS document

[60] If CA has a combined CP/CPS then remove references to Certificate Policy

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

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

based on 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 other than its *CA operations at <LOCATION>*[61], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Practitioner's signature*]
[*Practitioner's city, and state*]
[*Date of practitioner's report*]

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

Example US1.5B – Modified Opinion on Physical Security and Business Continuity, Report on Subject Matter, Period of Time – issues in table format

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

We have examined for ABC-CA's Certification Authority (CA) operations at <LOCATION>[62],

- ABC-CA's disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices, [the consistency of its Certification Practice Statement with its Certificate Policy (if applicable)][63], the provision of services in accordance with its [Certificate Policy (if applicable)][64] and Certification Practice Statement, and

- the effectiveness of ABC-CA's controls over key and certificate integrity, the authenticity and confidentiality of subscriber and relying party information, the continuity of key and certificate lifecycle management operations, and development, maintenance, and operation of CA systems integrity throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][65].

ABC-CA's management is responsible these disclosures and for maintaining effective controls, based on the WebTrust Principles Criteria for Certification Authorities v2.x[66]. Our responsibility is to express an opinion, based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

[(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 examination did not extend to the controls exercised by these external registration authorities.][67]

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.][68]

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the

[62] CA processing locations as defined in the "Reporting Guidance" section
[63] Remove bracketed text if the CA publishes a combined CP/CPS
[64] Remove bracketed text if the CA publishes a combined CP/CPS
[65] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section

[67] Remove bracketed text if external RAs are not used
[68] Modify this paragraph as appropriate to exclude certain criteria from scope. Please note that criteria can be excluded only if the CA does not provide the related service.

examination to obtain reasonable assurance about whether, throughout the period <DATE> to <DATE>, for its [list of Root and Subordinate CAs in scope][69], in all material respects, ABC-CA,:

a. 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][70]

b. maintained effective controls to provide reasonable assurance that:

   - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][71]
   - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[72]
   - 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
   - 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

based on the WebTrust Principles and Criteria for Certification Authorities v2.x.

During our examination, 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;

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

[70] 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

[71] Remove bracketed text/bullet if CA has a combined CP and CPS document

[72] If CA has a combined CP/CPS then remove references to Certificate Policy

#	Observation	Relevant WebTrust Criteria
		• 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.

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

In our opinion, except for the matters described in the preceding table, 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][73]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][74]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[75]

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

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

based on 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 other than its *CA operations at <LOCATION>*[76], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Practitioner's signature*]
[*Practitioner's city, and state*]
[*Date of practitioner's report*]

[73] 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
[74] Remove bracketed text/bullet if CA has a combined CP and CPS document
[75] If CA has a combined CP/CPS then remove references to Certificate Policy
[76] CA processing locations as defined in the "Reporting Guidance" section

SAMPLE APPENDIX A

List of CAs in Scope

- **Root CAs**
  - Number and List
- **OV SSL Issuing CAs**
  - Number and List
- **EV SSL Issuing CAs**
  - Number and List
- **Private Trust Issuing CAs**
  - Number and List
- **Non-EV Code Signing Issuing CAs**
  - Number and List
- **EV Code Signing Issuing CAs**
  - Number and List
- **Secure Email (S/MIME) CAs**
  - Number and List
- **Document Signing CAs**
  - Number and List
- **Adobe CAs**
  - Number and List
- **Timestamp CAs**
  - Number and List
- **Other CAs**
  - Number and List

Sample CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	6D5A334C1BAF569E	rsaEncryption	(4096 bit)	sha256 WithRSAEncryption	Mar 13 17:13:04 2017 GMT	Dec 31 17:13:04 2030 GMT	02:AE:95:D6:52:E5:01:87:40:AD:11:AF:DC:CD:01:EE:69:A7:D4:77	DB:AF:00:71:06:47:95:A5:78:FC:FD:9F:9E:19:63:BF:E6:D1:3D:D8:FE:8C:47:A0:7E:33:BB:77:F9:1A:15:19
2	1	C=CA O=ABC-CA Inc. CN=ABC-CA Issuing CA – EV	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	7DAAAF3CF15F8F45	rsaEncryption	(2048 bit)	sha256 WithRSAEncryption	Mar 14 01:25:41 2017 GMT	Mar 14 01:25:41 2027 GMT	92:A4:60:D4:ED:AC:57:3D:C2:1B:24:07:0D:AF:AC:DD:F1:0D:8A:9A	DF:30:CF:75:83:21:F7:F6:D0:08:21:05:AB:CD:BA:A4:59:38:B3:42:CF:5D:10:38:27:92:52:E8:A7:D3:3A:9F
2	2	C=CA O=ABC-CA Inc. CN=ABC-CA Issuing CA – EV	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	8FABAF6CF45F884F	rsaEncryption	(2048 bit)	sha256 WithRSAEncryption	Apr 22 07:41:53 2017 GMT	Apr 22 07:41:53 2027 GMT	92:A4:60:D4:ED:AC:57:3D:C2:1B:24:07:0D:AF:AC:DD:F1:0D:8A:9A	DC:25:7D:4E:09:57:8E:1F:86:E8:17:95:CA:FF:57:6C:D8:DD:AE:BD:A9:0D:30:23:3E:24:CA:AC:B4:C6:60:B1

Management's Assertion

Example MA1.1 – Management's Assertion, Period of Time

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][77], and provides the following CA services[78]:

- 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][79], CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

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

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its CA services at <LOCATION>[80], 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

[77] Replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to "Reporting Guidance" section
[78] This is a list of common services provided by CAs. Add and remove from this list to include the relevant services being provided
[79] Link to business practices repository location and describe location if not website (i.e. intranet)
[80] CA processing locations as defined in the "Reporting Guidance" section

- [name and version of certificate policy(ies) (if applicable][81]

- maintained effective controls to provide reasonable assurance that:
  - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][82]
  - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[83]

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

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

based on[84] the WebTrust Principles and Criteria for Certification Authorities v2.x[85], including the following[86]:

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

---

[81] At least of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet
[82] Remove bracketed text/bullet if CA has a combined CP and CPS document
[83] If CA has a combined CP/CPS then remove references to Certificate Policy
[84] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[85] Include applicable version number and hyperlink to the criteria document
[86] Remove bullets that are not applicable

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

CA Key Lifecycle Management Controls

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

Subscriber Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

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

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

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][87], and provides the following CA services[88]:

- 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][89], CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

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

ABC-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ABC-CA management's opinion, in providing its Certification Authority (CA) services at <LOCATION>[90], 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][91]

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

[87] Replace with list of Root and Subordinate CAs in scope or reference to an appendix. Refer to "Reporting Guidance" section
[88] This is a list of common services provided by CAs. Add and remove from this list to include the relevant services being provided
[89] Link to business practices repository location and describe location if not website (i.e. intranet)
[90] CA processing locations as defined in the "Reporting Guidance" section
[91] At least of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet

    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][92]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[93]

- 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 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

based on the WebTrust Principles and Criteria for Certification Authorities v2.x[94], including the following[95]:

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

[92] Remove bracketed text/bullet if CA has a combined CP and CPS document
[93] If CA has a combined CP/CPS then remove references to Certificate Policy
[94] Include applicable version number and hyperlink to the criteria document
[95] Remove bullets that are not applicable

- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

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

Subscriber Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

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

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

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope][96], and provides the following CA services[97]:

- 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][98], 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 CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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

#	Observation	Relevant WebTrust Criteria
1	We noted that electronic and auditable dual-custody multi-factor entrance and exit controls to secure PKI area were not implemented.	3.4: The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorised

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

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

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

#	Observation	Relevant WebTrust Criteria
	This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.4 to not be met.	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>[99], throughout the period <DATE> to <DATE>, ABC-CA has:

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - [name and version of certification practice statement(s)]; and
    - [name and version of certificate policy(ies) (if applicable][100]

- maintained effective controls to provide reasonable assurance that:
    - [ABC-CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)][101]
    - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)[102]

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

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

in accordance with [based on][103] the WebTrust Principles and Criteria for Certification Authorities v2.x[104], including the following[105]:

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

---

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

CA Environmental Controls

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

CA Key Lifecycle Management Controls

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

Subscriber Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.][106]

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

[106] Modify this paragraph as appropriate to exclude certain criteria from scope

WebTrust for Certification Authorities – SSL Baseline with Network Security

Specific Reporting Guidance for SSL Baseline with Network Security

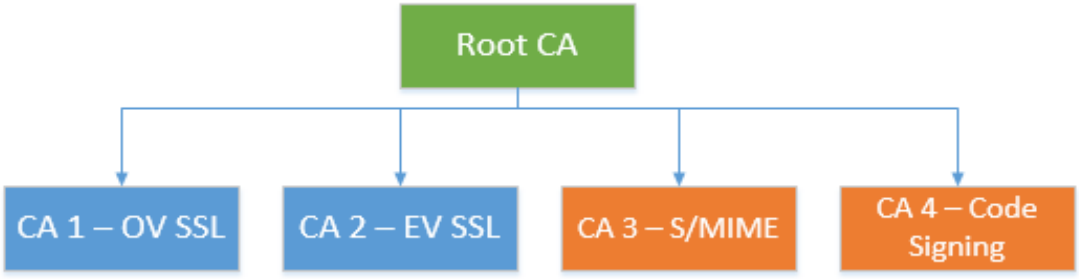
As of the time of publication, the SSL Baseline with Network Security audit criteria incorporates two different CA/Browser Forum requirements documents:

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

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

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

For example, in the following PKI hierarchy:



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

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

US (AICPA) Standards – AT-C 205

Example US2.1 – Unmodified Opinion, Reporting on Management's Assertion, Period of Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined ABC-CA management's assertion[107] that for its Certification Authority (CA) operations at <LOCATION>[108], 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, 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][109],

  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][110]

[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]][111]:

---

[107] Hyperlink to assertion

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

[109] 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

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

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

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

based on [Principle 4 of][112] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x[113]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*[114], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][115]

[*Practitioner's signature*]
[*Practitioner's city and state*]
[*Date of practitioner's report*]

[112] Include this bracket if only opining on the Network Security Requirements
[113] Include applicable version number and hyperlink to the criteria document
[114] CA processing locations as defined in the "Reporting Guidance" section
[115] Remove bracketed text if a seal is not issued. Seals will only be issued when the SSL Baseline Requirements are covered. Reports covering only the Network Security Requirements are not eligible for a seal.

Example US2.2 – Unmodified Opinion, Reporting on Management's Assertion, Point in Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined ABC-CA management's assertion[116] that for its Certification Authority (CA) operations at <LOCATION>[117], as of <DATE> for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope for SSL Baseline Requirements [and Network Security Requirements]][118], 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][119],

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

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

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity][120]

[And, for CAs as enumerated in Attachment A [or list of Root and Subordinate CAs in scope for Network Security Requirements]][121]:

---

[116] Hyperlink to assertion

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

[118] Reference to an appendix or replace with list of Root and Subordinate CAs in scope for the SSL Baseline Requirements (and Network Security Requirements if these are the same]. Refer to "Reporting Guidance" section

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

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

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

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

based on [Principle 4 of][122] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x[123]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

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.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

In our opinion, management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA's services other than its *Certification Authority (CA) operations at <LOCATION>*[124], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Practitioner's signature*]
[*Practitioner's city and state*]
[*Date of practitioner's report*]

[122] Include this bracket if only opining on the Network Security Requirements
[123] Include applicable version number and hyperlink to the criteria document
[124] CA processing locations as defined in the "Reporting Guidance" section

Example US2.3 – Unmodified Opinion, Reporting on Subject Matter, Period of Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined for its Certification Authority (CA) operations at <LOCATION>[125],

a. ABC-CA's disclosure of its SSL certificate lifecycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website
b. the provision of such services in accordance its disclosed practices
c. the effectiveness of its controls over
    - key and SSL certificate integrity,
    - the authenticity and confidentiality of SSL subscriber and relying party information,
    - continuity of key and SSL certificate lifecycle management operations, and
    - development, maintenance, and operation of CA systems integrity,
    - [and meeting the network and certificate system security requirements set forth by the CA/Browser Forum][126]

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]][127].

[We have also examined the effectiveness of ABC-CA's controls over meeting the network and certificate system security requirements set forth by the CA/Browser Forum throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list of Root and Subordinate CAs in scope for Network Security Requirements][128].][129]

ABC-CA's management is responsible for these disclosures and for maintaining effective controls based on the WebTrust Principles and Criteria for Certification Authorities v2.x[130]. Our responsibility is to express an opinion based on our examination.

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. Our examination did not

[125] CA processing locations as defined in the "Reporting Guidance" section
[126] Include bracketed text if SSL Baseline and Network Security Requirements apply to the same hierarchy. Otherwise, remove and include the next paragraph
[127] Replace with list of Root and Subordinate CAs in scope for the SSL Baseline Requirements (and Network Security Requirements if these are the same) or reference to an appendix. Refer to "Reporting Guidance" section
[128] Replace with list of CAs in scope for Network Security Requirements or reference to an appendix. This list must include all CAs in scope for SSL Baseline Requirements and non-SSL CAs. Refer to "Reporting Guidance" section
[129] Include this paragraph if the reporting on difference hierarchies for SSL Baseline Requirements vs Network Security Requirements. Otherwise, remove.

extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, throughout the period <DATE> to <DATE>, for its [list of Root and Subordinate CAs in scope][131], in all material respects, ABC-CA

a. disclosed its SSL certificate lifecycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website,
b. provided such services in accordance its disclosed practices,
c. maintained effective controls over
    - key and SSL certificate integrity,
    - the authenticity and confidentiality of SSL subscriber and relying party information,
    - continuity of key and SSL certificate lifecycle management operations, and
    - development, maintenance, and operation of CA systems integrity,
    - [and meeting the network and certificate system security requirements set forth by the CA/Browser Forum][132]

based on [Principle 4 of][133] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x.

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

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

a. disclosed its SSL certificate lifecycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website,
b. provided such services in accordance its disclosed practices,
c. maintained effective controls over
    - key and SSL certificate integrity,
    - the authenticity and confidentiality of SSL subscriber and relying party information,
    - continuity of key and SSL certificate lifecycle management operations, and
    - development, maintenance, and operation of CA systems integrity,

[131] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[132] Include bracketed text if SSL Baseline and Network Security Requirements apply to the same hierarchy. Otherwise, remove and include the next paragraph
[133] Include this bracket if only opining on the Network Security Requirements

- [and meeting the network and certificate system security requirements set forth by the CA/Browser Forum][134]

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

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by [Principle 4 of][136] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][137]

[*Practitioner's signature*]
[*Practitioner's city and state*]
[*Date of practitioner's report*]

[134] Include bracketed text if SSL Baseline and Network Security Requirements apply to the same hierarchy. Otherwise, remove and include the next paragraph
[135] Include this bracket if only opining on the Network Security Requirements
[136] Include this bracket if only opining on the Network Security Requirements
[137] Remove bracketed text if a seal is not issued. Seals will only be issued when the SSL Baseline Requirements are covered. Reports covering only the Network Security Requirements are not eligible for a seal.

Management's Assertion

Example MA2.1 – Management's Assertion, Period of Time

ABC-CA MANAGEMENT'S ASSERTION

[ABC Certification Authority, Inc. ("ABC-CA") operates the Certification Authority (CA) services known as [list of Root and Subordinate CAs in scope for SSL Baseline Requirements and Network Security Requirements][138] and provides SSL CA services.][139]

ABC-CA management has assessed its [disclosures of its certificate practices and][140] controls over its SSL CA services. Based on that assessment, in providing its SSL [and non-SSL] Certification Authority (CA) services at <LOCATION>[141], 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][142],

  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][143]

- 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

---

[138] 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

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

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

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

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

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

based on [Principle 4 of][144] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x [145].

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

[144] Include this bracket if only opining on the Network Security Requirements
[145] Include applicable version number and hyperlink to the criteria document

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

ABC-CA MANAGEMENT'S ASSERTION

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

ABC-CA management has assessed its [disclosures of its certificate practices and][148] controls over its EV SSL CA services. Based on that assessment, in providing its SSL [and non-SSL] Certification Authority (CA) services at <LOCATION>[149], 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)][150],

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

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

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity][151]

- 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

[146] 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
[147] Include this introductory paragraph if all CAs are SSL CAs and therefore in scope for SSL Baseline Requirements and Network Security Requirements. Remove this paragraph if only auditing the Network Security Requirements
[148] Include if SSL Baseline Requirements are in scope. Remove if only Network Security Requirements are in scope.
[149] CA processing locations as defined in the "Reporting Guidance" section
[150] At least of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet
[151] The first 3 paragraphs pertain to the SSL Baseline Requirements and can be removed if only opining on the Network Security Requirements

based on [Principle 4 of][152] the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.x [153].

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

[152] Include this bracket if only opining on the Network Security Requirements
[153] Include applicable version number and hyperlink to the criteria document

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

US (AICPA) Standards – AT-C205

Example US3.1 – Unmodified Opinion, Reporting on Management's Assertion, Period of Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined ABC-CA management's assertion[154] that for its Certification Authority (CA) operations at <LOCATION>[155], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][156], 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][157]

  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)

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x[158]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

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. Our examination did not extend

[154] Hyperlink to assertion
[155] CA processing locations as defined in the "Reporting Guidance" section
[156] Reference to an appendix or replace with list of Root and Subordinate CAs in scope . Refer to "Reporting Guidance" section
[157] At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet
[158] Include applicable version number and hyperlink to the criteria document

to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*[159], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[(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.][160]

[*Practitioner's signature*]
[*Practitioner's city and state*]
[*Date of practitioner's report*]

[159] CA processing locations as defined in the "Reporting Guidance" section
[160] Remove bracketed text if a seal is not issued

Example US3.2 – Unmodified Opinion, Reporting on Management's Assertion, Point in Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined ABC-CA management's assertion[161] that for its Certification Authority (CA) operations at <LOCATION>[162], as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][163], 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][164]

  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)

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x[165]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

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.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion,

---

[161] Hyperlink to assertion
[162] CA processing locations as defined in the "Reporting Guidance" section
[163] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[164] 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
[165] Include applicable version number and hyperlink to the criteria document

whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

In our opinion, management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*[166], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Practitioner's signature*]
[*Practitioner's city, and state*]
[*Date of practitioner's report*]

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

Example US3.3 – Unmodified Opinion, Reporting on Subject Matter, Period of Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined for its Certification Authority (CA) operations at <LOCATION>[167],

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

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][168].

ABC-CA's management is responsible for these disclosures and for maintaining effective controls based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.x [169]. Our responsibility is to express an opinion based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, throughout the period <DATE> to <DATE>, for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][170], in all material respects, ABC-CA

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

[167] CA processing locations as defined in the "Reporting Guidance" section
[168] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section

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

- [name and version of certificate policy(ies) (if applicable][171]

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)

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

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

In our opinion, throughout the period <DATE> to <DATE>, ABC-CA has, in all material 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][172]

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

- 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)

based on 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 other than its *CA operations at <LOCATION>*[173], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[171] 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

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

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

[(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.][174]

[*Practitioner's signature*]
[*Practitioner's city, and state*]
[*Date of practitioner's report*]

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

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

US (AICPA) Standards – AT-C205

Example US4.1 – Unmodified Opinion, Reporting on Management's Assertion, Period of Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined ABC-CA management's assertion[175] that for its Certification Authority (CA) operations at <LOCATION>[176], throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][177], ABC-CA has:

- disclosed its extended validation code signing ("EV CS") certificate lifecycle management business practices in its:
    - [name and version of certification practice statement(s)]; and
    - [name and version of certificate policy(ies) (if applicable][178]

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

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

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

[175] Hyperlink to assertion
[176] CA processing locations as defined in the "Reporting Guidance" section
[177] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. This should include EV CS Signing Authorities and EV CS Timestamp Authorities as applicable. Refer to "Reporting Guidance" section
[178] At least one of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet

- [maintained effective controls to provide reasonable assurance that its [EV CS Signing Authority] [and EV CS Timestamp Authority] is/are operated in conformity with CA/Browser Forum Guidelines][179]

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.x[180]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*[181], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – Extended Validation Code Signing Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][182]

[*Practitioner's signature*]
[*Practitioner's city and state*]
[*Date of practitioner's report*]

[179] Modify the bracketed text depending on which services the CA provides. If it does not provide a Signing Authority or Timestamp Authority, then remove this bullet point
[180] Include applicable version number and hyperlink to the criteria document
[181] CA processing locations as defined in the "Reporting Guidance" section
[182] Remove bracketed text if a seal is not issued

Example US4.2 – Unmodified Opinion, Reporting on Management's Assertion, Point in Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined ABC-CA management's assertion[183] that for its Certification Authority (CA) operations at <LOCATION>[184], as of <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][185], ABC-CA has:

- disclosed its extended validation code signing ("EV CS") certificate lifecycle management business practices in its:
    - [name and version of certification practice statement(s)]; and
    - [name and version of certificate policy(ies) (if applicable][186]

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

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

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

- [suitably designed, and placed into operation, controls to provide reasonable assurance that its [EV CS Signing Authority] [and EV CS Timestamp Authority] is/are operated in conformity with CA/Browser Forum Guidelines][187]

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.x[188]. ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

---

[183] Hyperlink to assertion

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

[185] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. This should include EV CS Signing Authorities and EV CS Timestamp Authorities as applicable. Refer to "Reporting Guidance" section

[186] 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

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

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

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.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

In our opinion, management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA's services other than its *CA operations at <LOCATION>*[189], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Practitioner's signature*]
[*Practitioner's city, and state*]
[*Date of practitioner's report*]

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

Example US4.3 – Unmodified Opinion, Reporting on Subject Matter, Period of Time

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined for its Certification Authority (CA) operations at <LOCATION>[190],

a. ABC-CA's disclosure of its extended validation code signing ("EV CS") certificate lifecycle management business practices, including its commitment to provide EV CS certificates in conformity with the CA/Browser Forum Guidelines on the ABC-CA website,
b. the provision of such services in accordance its disclosed practices,
c. the effectiveness of its controls over
    - key and EV CS certificate integrity,
    - the authenticity and confidentiality of EV CS subscriber and relying party information,
    - continuity of key and EV CS certificate lifecycle management operations,
    - [and over the continuity and provision of EV CS Signing Authority and EV CS Timestamp Authority services][191]

throughout the period <DATE> to <DATE> for its CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][192].

ABC-CA's management is responsible for these disclosures and for maintaining effective controls based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.x [193]. Our responsibility is to express an opinion based on our examination.

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, throughout the period <DATE> to <DATE>, for CAs as enumerated in Attachment A [or list Root and Subordinate CAs in scope][194], in all material respects, ABC-CA

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

[190] CA processing locations as defined in the "Reporting Guidance" section
[191] Modify or remove as applicable depending on which services the CA provides
[192] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section
[193] Include applicable version number and hyperlink to the criteria document
[194] Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to "Reporting Guidance" section

    - [name and version of certificate policy(ies) (if applicable][195]

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

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

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

- [maintained effective controls to provide reasonable assurance that its [EV CS Signing Authority] [and EV CS Timestamp Authority] is/are operated in conformity with CA/Browser Forum Guidelines][196]

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.x.

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

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

- disclosed its extended validation code signing ("EV CS") certificate lifecycle management business practices in its:
    - [name and version of certification practice statement(s)]; and
    - [name and version of certificate policy(ies) (if applicable][197]

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

- maintained effective controls to provide reasonable assurance that:

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

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

[197] 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 CS certificates it manages is established and protected throughout their lifecycles; and
    - EV CS subscriber information is properly authenticated (for the registration activities performed by ABC-CA)

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

- [maintained effective controls to provide reasonable assurance that its [EV CS Signing Authority] [and EV CS Timestamp Authority] is/are operated in conformity with CA/Browser Forum Guidelines][198]

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.x.

This report does not include any representation as to the quality of ABC-CA's services other than its *Certification Authority (CA) operations at <LOCATION>*[199], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[(If a seal is issued) ABC-CA's use of the WebTrust for Certification Authorities – Extended Validation Code Signing Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.][200]

[*Practitioner's signature*]
[*Practitioner's city, and state*]
[*Date of practitioner's report*]

[198] Modify the bracketed text depending on which services the CA provides. If it does not provide a Signing Authority or Timestamp Authority, then remove this bullet point
[199] CA processing locations as defined in the "Reporting Guidance" section
[200] Remove bracketed text if a seal is not issued.

Reporting on Root Key Generation

US (AICPA) Standards – AT-C205

Example US5.1 – Root Key Generation Ceremony

REPORT OF THE INDEPENDENT ACCOUNTANT

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

We have examined ABC-CA management's assertion[201] that in generating and protecting its [list of Root CAs witnessed] (collectively, "ABC-CA Root CAs") on <DATE>[202] at <LOCATION>[203], with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number	SHA1 Thumbprint
ABC-CA Root CA 1	0a:4b:33:d1:f9:a8:9f:33:12:00:ab	14:2b:c7:d1	f7 06 15 3a b6 d5 8b be 1a bb 85 0c 93 12 0f df 9b ea ad 63
ABC-CA Root CA 2	8f:7d:c4:33:19:0a:0b:de:f1:42:11	1b:23:d4:f2	f7 06 16 3a b6 d5 8b be 1a bb 75 0c 92 12 0f df 9b ea ad 63

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][204]

- 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)

---

[201] Hyperlink to assertion
[202] Date of witnessing. This can be a range of dates if the ceremony spanned multiple days.
[203] Location of the key generation ceremony
[204] At least of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet

- generated the CA keys in a physically secured environmental 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

based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x[205].

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants 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 our examination provides a reasonable basis for our opinion.

In our opinion, as of <DATE>, ABC-CA management's assertion, as referred to above, is fairly stated, in all material respects, based on 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 other than its *Certification Authority (CA) operations at <LOCATION>*[206], nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Practitioner's signature*]
[*Practitioner's city, and state*]
[*Date of practitioner's report]*

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

Management's Assertion

Example MA5.1 – Management's Assertion

ABC-CA MANAGEMENT'S ASSERTION

ABC Certification Authority, Inc. ("ABC-CA") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs known as [list of Root CAs witnessed] (collectively, "ABC-CA Root CAs"). These CA's will serve as Root CAs for client certificate services. In order to allow the CA's to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's private signing key. This helps assure the non-refutability of the integrity of the ABC-CA Root CAs' key pairs, and in particular, the private signing keys.

ABC-CA management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in ABC-CA's Certificate Policy (CP) [and/or] Certification Practice Statement (CPS), and its Root Key Generation Script(s), which are in accordance with [based on][207] CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x[208].

ABC-CA management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

ABC-CA management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the ABC-CA Root CAs, and for the CA environment controls relevant to the generation and protection of its CA keys.

ABC-CA management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys for the ABC-CA Root CA's on <DATE>[209] at <LOCATION>[210], with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number	SHA1 Thumbprint
ABC-CA Root CA 1	0a:4b:33:d1:f9:a8:9f:33:12:00:ab	14:2b:c7:d1	f7 06 15 3a b6 d5 8b be 1a bb 85 0c 93 12 0f df 9b ea ad 63
ABC-CA Root CA 2	8f:7d:c4:33:19:0a:0b:de:f1:42:11	1b:23:d4:f2	f7 06 16 3a b6 d5 8b be 1a bb 75 0c 92 12 0f df 9b ea ad 63

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

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][211]

- included appropriate, detailed procedures and controls in its Root Key Generation Script(s):
    - [name, version number, and date of root key generation script(s). This may also include additional scripts such as server build scripts]

- maintained effective controls to provide reasonable assurance that the ABC-CA Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Script(s)

- performed, during the root key generation process, all procedures required by the Root Key Generation Script(s)

- generated the CA keys in a physically secured environment as described in its CP/CPS

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge

- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with [based on][212] CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.x[213].

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

[211] At least of these documents should be hyperlinked. Refer to "Reporting Guidance" section. If the CA does not have a separate CP then remove the second bullet
[212] Use 'in accordance with' for Canadian and International standards. Use 'based on' for US standards
[213] Include applicable version number and hyperlink to the criteria document