Deloitte Anjin LLC
9Fl., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
150-945, Korea

Tel: +82 (2) 6676 1000
Fax: +82 (2) 6674 2114
www.deloitteanjin.co.kr

INDEPENDENT ASSURANCE REPORT

To the Management of Ministry of Education ("MOE"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on MOE management's assertion that for its Certification Authority (CA) operations in Republic of Korea, throughout the period 1 January 2018 to 31 December 2018 for its CAs as enumerated in APPENDIX A, MOE has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Ministry of Education CA Certification Practice Statement

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the MOE 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 MOE)

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

And, for its CAs as enumerated in Appendix A for Network Security Requirements:

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

The information included in Attachment C, 'Other information provided by the CA' is presented by the management of MOE to provide additional information to users of this report. This information has not been subjected to our procedures, and, accordingly, we express no opinion on it.

Certification authority's responsibilities

MOE's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

Our independence and quality control

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

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory

Deloitte.

Deloitte Anjin LLC
9Fl., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
150-945, Korea

Tel: +82 (2) 6676 1000
Fax: +82 (2) 6674 2114
www.deloitteanjin.co.kr

requirements.

Auditor's responsibilities

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

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

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

Relative effectiveness of controls

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

Inherent limitations

Because of the nature and inherent limitations of controls, MOE'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.

Basis for qualified opinion

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

	Observation	Relevant WebTrust Criteria
1	We noted that the CA certificate, CA134100031, does not contain HTTP URLs in CRL Distribution Point extension and does NOT have authorityInformationAcesss extension. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline	**P2, 2.4:** The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subordinate CA certificates conform to the Baseline Requirements. • Baseline Requirements 7.1.2.2.b. cRLDistributionPoints:

Deloitte.

Deloitte Anjin LLC
9Fl., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
150-945, Korea

Tel: +82 (2) 6676 1000
Fax: +82 (2) 6674 2114
www.deloitteanjin.co.kr

	Observation	Relevant WebTrust Criteria
	with Network Security v2.3, Principle 2, Criterion 2.4 to not be met.	This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service. • Baseline Requirements 7.1.2.2.c. authorityInformationAccess: With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366].
2	We noted that the validity period of some subscriber certificates issued from 1 March 2018 exceeded the maximum 825 days. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.7 to not be met.	**P2, 2.7:** The CA maintains controls to provide reasonable assurance that the validity period of Subscriber certificates issued does not exceed the maximum as specified in the Baseline Requirements. • Baseline Requirements 6.3.2. Certificate Operational Periods and Key Pair Usage Periods Subscriber Certificates issued after 1 March 2018 MUST have a Validity Period no greater than 825 days. Subscriber Certificates issued after 1 July 2016 but prior to 1 March 2018 MUST have a Validity Period no greater than 39 months
3	During the period, there were instances regarding DN structure with fixed values: • organizationName was fixed as Government of Korea; • organizationalUnitName was fixed as Group of Server; and • locallyName and stateOrProvinceName did not exist. Certificates which have multiple commonNames in Subject were issued.	**P2, 2.14:** The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including: • subject:commonName • subject:organizationName • subject:givenName • subject:surname • subject:streetAddress • subject:localityName • subject:stateOrProvinceName • subject:postalCode

Deloitte.

Deloitte Anjin LLC
9Fl., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
150-945, Korea

Tel: +82 (2) 6676 1000
Fax: +82 (2) 6674 2114
www.deloitteanjin.co.kr

	Observation	Relevant WebTrust Criteria
	This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.14 to not be met.	• subject:countryName • subject:organizationalUnitName • Other Subject Attributes • Subject field requirements if Reserved Certificate Policy Identifiers are asserted • Subject Information for Root and Subordinate CA certificates
4	We noted that a certificate which had RSA 2024 bits module was issued. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.16 to not be met.	**P2, 2.16:** The CA maintains controls to provide reasonable assurance that it rejects a certificate request if the Public Key does not meet the requirements set forth in Sections 6.1.5, 6.1.6, or if it has a weak Private Key (such as a Debian weak key). • Baseline Requirements 6.1.5. Key Sizes: Certificates MUST meet the following requirements for algorithm type and key size. ○ Subscriber Certificates Minimum RSA modulus size (bits): 2048
5	During the period, validation of domain authorization was conducted by official documents classified as a Domain Authorization Document. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 4.1 to not be met.	**P2, 4.1:** The CA maintains controls to provide reasonable assurance that prior to issuing a Certificate: the CA obtains confirmation in accordance with the SSL Baseline Requirements Sections 3.2.2.4, 3.2.2.5, 3.2.2.6 and 4.2.2 related to the Fully-Qualified Domain Name(s) (including wildcard domains and new gTLDs (generic top-level domains)) and IP address(es) listed in the Certificate; and the CA maintains records of which validation method, including the relevant SSL Baseline Requirements version number, used to validate every domain. • Baseline Requirements 3.2.2.4.5 Domain Authorization Document: Confirming the Applicant's control over the FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the date of

Deloitte.

Deloitte Anjin LLC
9Fl., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
150-945, Korea

Tel: +82 (2) 6676 1000
Fax: +82 (2) 6674 2114
www.deloitteanjin.co.kr

	Observation	Relevant WebTrust Criteria
		the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space. For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.
6	Procedures on prevention by a CAA record were not documented. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 4.11 to not be met.	**P2, 4.11:** The CA maintains controls to provide reasonable assurance that it documents potential certificate issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances.
7	We noted that certain subscriber certificates were not revoked within 24 hours after the CA recognized mis-issued certificates. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 5.3 to not be met.	**P2, 5.3:** The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 4. The CA obtains evidence that the Certificate was misused; 5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or

Deloitte.

Deloitte Anjin LLC
9Fl., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
150-945, Korea

Tel: +82 (2) 6676 1000
Fax: +82 (2) 6674 2114
www.deloitteanjin.co.kr

Observation	Relevant WebTrust Criteria
	IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); 7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 8. The CA is made aware of a material change in the information contained in the Certificate; 9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; 10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 12. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; 13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;

Deloitte Anjin LLC
9Fl., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
150-945, Korea

Tel: +82 (2) 6676 1000
Fax: +82 (2) 6674 2114
www.deloitteanjin.co.kr

Observation	Relevant WebTrust Criteria
	14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time)

Qualified Opinion

In our opinion, except for the matters described in the preceding section entitled 'Basis for qualified opinion', throughout the period 1 January 2018 to 31 December 2018, MOE management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

This report does not include any representation as to the quality of MOE's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3 nor the suitability of any of MOE's services for any customer's intended purpose.

Deloitte Anjin LLC
Seoul, Republic of Korea
30 September 2019

Appendix A [List of CAs in Scope]

OV SSL Issuing CAs
#1. CA134100031

Appendix B [CA Identifying Information for in Scope CAs]

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA1 Fingerprint
1	1	CN = CA134100031 OU = GPKI O = Government of Korea C = KR	CN = GPKIRootCA1 OU = GPKI O = Government of Korea C = KR	2719	sha256RSA	2048 Bits	sha256	December 15 15:00:13 2011	December 15 15:00:13 2021	8e46f80d9e7876a2cc1ae40f517f52d74d9c5b1b	64e67825842bca22e68ebf67a343dd65b6375869

교육부

Ministry of Education MANAGEMENT'S ASSERTION

Ministry of Education ("MOE") operates the Certification Authority (CA) services known as Appendix A and provides SSL CA services.

MOE management has assessed its disclosures of its certificate practices and controls over its SSL CA services. During our assessment, we noted the observations in Appendix C, which caused the relevant criteria to not be met.

Based on that assessment, in MOE management's opinion, except for the matters described in the preceding table, in providing its SSL Certification Authority (CA) services at the Republic of Korea, throughout the period 1 January 2018 to 31 December 2018, MOE has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Ministry of Education CA Certification Practice Statement

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the MOE 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 MOE)

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

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

Do-young, Kim
Information Security team Leader
Ministry of Education
Republic of Korea
30 September 2019

Appendix A. List of CAs in Scope

OV SSL Issuing CAs
#1. CA134100031

Appendix B. CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA1 Fingerprint
1	1	CN = CA134100031 OU = GPKI O = Government of Korea C = KR	CN = GPKIRootCA1 OU = GPKI O = Government of Korea C = KR	2719	sha256RSA	2048 Bits	sha256	December 15 15:00:13 2011	December 15 15:00:13 2021	8e46f80d9e7876a2cc1ae40f517f52d74d9c5b1b	64e67825842bca22e68ebf67a343dd65b6375869

Appendix C. Observations which caused the relevant criteria to not be met

	Observation	Relevant WebTrust Criteria
1	The CA certificate, CA134100031, does NOT contain HTTP URLs in CRL Distribution Point extension. The CA certificate, CA134100031, does NOT have authorityInformationAcesss extension. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.4 to not be met.	**P2, 2.4:** The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subordinate CA certificates conform to the Baseline Requirements. • Baseline Requirements 7.1.2.2.b. cRLDistributionPoints: This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service. • Baseline Requirements 7.1.2.2.c. authorityInformationAccess: With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366].
2	Validity period of some of subscriber certificates issued from 1 March 2018 exceeded the maximum that is 825 days. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.7 to not be met.	**P2, 2.7:** The CA maintains controls to provide reasonable assurance that the validity period of Subscriber certificates issued does not exceed the maximum as specified in the Baseline Requirements. • Baseline Requirements 6.3.2. Certificate Operational Periods and Key Pair Usage Periods Subscriber Certificates issued after 1 March 2018 MUST have a Validity Period no greater than 825 days. Subscriber Certificates issued after 1 July 2016 but prior to 1 March 2018 MUST have a Validity Period no greater than 39 months
3	During the period, there were instances regarding DN structure with fixed values: • organizationName was fixed as Government of Korea;	**P2, 2.14:** The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including:

	Observation	Relevant WebTrust Criteria
	• organizationalUnitName was fixed as Group of Server; and • locallyName and stateOrProvinceName were not exist. Certificates which have multiple commonNames in Subject were issued. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.14 to not be met.	• subject:commonName • subject:organizationName • subject:givenName • subject:surname • subject:streetAddress • subject:localityName • subject:stateOrProvinceName • subject:postalCode • subject:countryName • subject:organizationalUnitName • Other Subject Attributes • Subject field requirements if Reserved Certificate Policy Identifiers are asserted • Subject Information for Root and Subordinate CA certificates
4	A certificate which had RSA 2024 bits module was issued. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.16 to not be met.	**P2, 2.16:** The CA maintains controls to provide reasonable assurance that it rejects a certificate request if the Public Key does not meet the requirements set forth in Sections 6.1.5, 6.1.6, or if it has a weak Private Key (such as a Debian weak key). • Baseline Requirements 6.1.5. Key Sizes: Certificates MUST meet the following requirements for algorithm type and key size. ○ Subscriber Certificates Minimum RSA modulus size (bits): 2048
5	During the period, validation of domain authorization was conducted by official documents classified as Domain Authorization Document. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 4.1 to not be met.	**P2, 4.1:** The CA maintains controls to provide reasonable assurance that prior to issuing a Certificate: the CA obtains confirmation in accordance with the SSL Baseline Requirements Sections 3.2.2.4, 3.2.2.5, 3.2.2.6 and 4.2.2 related to the Fully-Qualified Domain Name(s) (including wildcard domains and new gTLDs (generic top-level domains)) and IP address(es) listed in the Certificate; and the CA maintains records of which validation method, including the relevant SSL Baseline Requirements version number, used to validate every domain. • Baseline Requirements 3.2.2.4.5 Domain Authorization Document: Confirming the Applicant's control over the FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain

	Observation	Relevant WebTrust Criteria
		Contact. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space. For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.
6	Procedures on prevention by a CAA record were not documented. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 4.11 to not be met.	**P2, 4.11:** The CA maintains controls to provide reasonable assurance that it documents potential certificate issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances.
7	Some of subscriber certificates were not revoked within 24 hours after the CA recognized mis-issued certificates. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 5.3 to not be met.	**P2, 5.3:** The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 4. The CA obtains evidence that the Certificate was misused; 5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a

Observation	Relevant WebTrust Criteria
	court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); 7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 8. The CA is made aware of a material change in the information contained in the Certificate; 9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; 10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 12. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; 13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate; 14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser

Observation	Relevant WebTrust Criteria
	Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time)