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, except for matters described in the assertion, for its Certification Authority (CA) operations in Republic of Korea, throughout the period 1 January 2019 to 31 December 2019 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

- 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.

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 requirements.

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

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	A policy or practice on processing CAA DNS Records is not disclosed in the Certification Practice Statement and during the audit period, checking for CAA records was not performed. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 1, Criterion 1.6 and Principle 2, Criterion 4.10 and 4.11 to not be met.	**P1, 1.6:** The CA discloses in its Certificate Policy (CP) and/or Certification Practices Statement (CPS) under section 4.2 (if the CA's disclosures follow RFC 3647) or under section 4.1 (if the CA's disclosures follow RFC 2527) its policy or practice on processing CAA (Certification Authority Authorisation) DNS Records for Fully Qualified Domain Names that is consistent with the SSL Baseline Requirements, and specifies the set of Issuer Domain Names that that the CA recognises in CAA "issue"

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
		or "issuewild" records as permitting it to issue. The CA maintains controls to provide reasonable assurance that it logs all actions taken, if any, consistent with its processing practice. **P2, 4.10:** For certificates issued on or after 8 September 2017, the CA maintains controls to provide reasonable assurance that as part of the issuance process, it checks for CAA records, and, if present, processes the certificate request in accordance with the requirements set forth in Section 3.2.2.8 of the Baseline Requirements. **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.
2	The new subordinate certificate issued in 2019 contains a serial number less than 64 bits (2719). Also, this serial number is same as one of the previous certificates and this is not unique for each certificate. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.1 and 2.6 to not be met.	**P2, 2.1:** The CA maintains controls to provide reasonable assurance that Root, Subordinate, and Subscriber certificates generated by the CA contain certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG. **P2, 2.6:** The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the Baseline Requirements Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated after the Effective Date (1 July 2012) are set in accordance with RFC 5280.
3	Subordinate Certificate CA134100031 did not contain HTTP URLs in the CRL distribution points extension. Subordinate Certificate CA134100031 did not have an authority information access extension. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.4, 5.5 and 5.6 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. **P2, 5.5:** The CA maintains controls to provide reasonable assurance that the CA: • makes revocation information available via the cRLDistributionPoints and/or authorityInformationAccess certificate extensions for Subordinate CA and

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
	Subscriber Certificates in accordance with the SSL Baseline Requirements Section 7.1.2. • for high-traffic FQDNs, distributes its OCSP responses in accordance with SSL Baseline Requirements. **P2, 5.6:** 'The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of Subscriber Certificates: ○ If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the next Update field must not be more than ten (10) days beyond the value of the this Update field; and ○ The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four (4) days and OCSP responses must have a maximum expiration time of ten (10) days. • for the status of subordinate CA Certificates ○ The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the next Update field must not be more than twelve months beyond the value of the this Update field; and ○ The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate. • The CA makes revocation information available through an OCSP capability using the GET method for Certificates

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
		issued in accordance with the SSL Baseline Requirements.
4	During the audit period, Subscriber certificates did not contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.5 to not be met.	**P2, 2.5:** The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated after the Effective Date (1 July 2012) conform to the Baseline Requirements.
5	During the audit period, Subscriber certificates containing a negative interger serial number were issued. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.6 to not be met.	**P2, 2.6:** The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the Baseline Requirements Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated after the Effective Date (1 July 2012) are set in accordance with RFC 5280.
6	During the audit period, validation of domain authorization was conducted by official documents that were issued by government organizations who have legal ownership of requesting domains, 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.
7	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

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
	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 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;

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
		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 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)
8	An examination on the information verification requirements for Validation Specialists of CA and Delegated Third Party was not performed This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 6.2 and 6.4 to not be met.	**P2, 6.2:** The CA maintains controls to provide reasonable assurance that: • the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. • the CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. • the CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. • the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements.

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
	• all personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs. **P2, 6.4:** The CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified opinion section above, throughout the period 1 January 2019 to 31 December 2019, 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.

Deloitte Anjin LLC
Seoul, Republic of Korea

5 August 2020

Appendix A. List of CAs in Scope

OV SSL Issuing CAs
#1. CA134100031

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint
1	1	CN = CA134100031 OU = GPKI O = Government of Korea C = KR	CN = GPKIRootCA1 OU = GPKI O = Government of Korea C = KR	2719	rsaEncryption	2048 Bits	sha256	2011-12-15 15:00:13 KST	2021-12-15 15:00:13 KST	8e46f80d9e7876a2cc1ae40f517f52d74d9c5b1b	49CE7CEE30BCE37388E747DFA46DA3439C75C89C1F34443AE6A43203D6F17436
1	2	CN = CA134100031 OU = GPKI O = Government of Korea C = KR	CN = GPKIRootCA1 OU = GPKI O = Government of Korea C = KR	2719	rsaEncryption	2048 Bits	sha256	2011-12-15 15:00:13 KST	2030-12-15 15:00:13 KST	8e46f80d9e7876a2cc1ae40f517f52d74d9c5b1b	7AD6DAEEAEFAB87225AB0BF9FBF874A17311A3718D1F86EF14EE67511B89B7E3

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 B, which caused the relevant criteria to not be met.

Based on that assessment, in MOE management's opinion, except for the matters described in Appendix B, in providing its SSL Certification Authority (CA) services at the Republic of Korea, throughout the period 1 January 2019 to 31 December 2019, 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

Do-young, Kim
Information Security team Leader
Ministry of Education
Republic of Korea
5 August 2020

Appendix A. List of CAs in Scope

OV SSL Issuing CAs
#1. CA134100031

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA2 Fingerprint
1	1	CN = CA134100031 OU = GPKI O = Government of Korea C = KR	CN = GPKIRootCA1 OU = GPKI O = Government of Korea C = KR	2719	rsaEncryption	2048 Bits	sha256	2011-12-15 15:00:13 KST	2021-12-15 15:00:13 KST	8e46f80d9e7876a2cc1ae40f517f52d74d9c5b1b	49CE7CEE30BCE37388E747DFA46DA3439C75C89C1F34443AE6A43203D6F17436
1	2	CN = CA134100031 OU = GPKI O = Government of Korea C = KR	CN = GPKIRootCA1 OU = GPKI O = Government of Korea C = KR	2719	rsaEncryption	2048 Bits	sha256	2011-12-15 15:00:13 KST	2030-12-15 15:00:13 KST	8e46f80d9e7876a2cc1ae40f517f52d74d9c5b1b	7AD6DAEEAEFAB87225AB0BF9FBF874A17311A3718D1F86EF14EE67511B89B7E3

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

	Observation	Relevant WebTrust Criteria
1	A policy or practice on processing CAA DNS Records is not disclosed in CPS and during the audit period, checking for CAA records was not performed. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 1, Criterion 1.6 and Principle 2, Criterion 4.10 and 4.11 to not be met.	**P1, 1.6:** The CA discloses in its Certificate Policy (CP) and/or Certification Practices Statement (CPS) under section 4.2 (if the CA's disclosures follow RFC 3647) or under section 4.1 (if the CA's disclosures follow RFC 2527) its policy or practice on processing CAA (Certification Authority Authorisation) DNS Records for Fully Qualified Domain Names that is consistent with the SSL Baseline Requirements, and specifies the set of Issuer Domain Names that that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue. The CA maintains controls to provide reasonable assurance that it logs all actions taken, if any, consistent with its processing practice. **P2, 4.10:** For certificates issued on or after 8 September 2017, the CA maintains controls to provide reasonable assurance that as part of the issuance process, it checks for CAA records, and, if present, processes the certificate request in accordance with the requirements set forth in Section 3.2.2.8 of the Baseline Requirements. **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.
2	The new subordinate certificate issued in 2019 contains a serial number less than 64 bits (2719). Also, this serial number is same as one of the previous certificates and this is not unique for each certificate. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.1 and 2.6 to not be met.	**P2, 2.1:** The CA maintains controls to provide reasonable assurance that Root, Subordinate, and Subscriber certificates generated by the CA contain certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG. **P2, 2.6:** The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the Baseline Requirements Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated after the Effective Date (1 July 2012) are set in accordance with RFC 5280.
3	Subordinate Certificate CA134100031 did not contain HTTP URLs in CRL Distribution Point extension.	**P2, 2.4:** The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate

Observation	Relevant WebTrust Criteria
Subordinate Certificate CA134100031 did not have Authority Information Access extension. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.4, 5.5 and 5.6 to not be met.	Policy Identifiers) of Subordinate CA certificates conform to the Baseline Requirements. **P2, 5.5:** The CA maintains controls to provide reasonable assurance that the CA: • makes revocation information available via the cRLDistributionPoints and/or authorityInformationAccess certificate extensions for Subordinate CA and Subscriber Certificates in accordance with the SSL Baseline Requirements Section 7.1.2. • for high-traffic FQDNs, distributes its OCSP responses in accordance with SSL Baseline Requirements. **P2, 5.6:** 'The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of Subscriber Certificates: ○ If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the nextUpdate field must not be more than ten (10) days beyond the value of the thisUpdate field; and ○ The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four (4) days and OCSP responses must have a maximum expiration time of ten (10) days. • for the status of subordinate CA Certificates ○ The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CACertificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field; and ○ The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

	Observation	Relevant WebTrust Criteria
		• The CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the SSL Baseline Requirements.
4	During the audit period, Subscriber certificates did not contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.5 to not be met.	**P2, 2.5:** The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated after the Effective Date (1 July 2012) conform to the Baseline Requirements.
5	During the audit period, Subscriber certificates containing a negative interger serial number were issued. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.6 to not be met.	**P2, 2.6:** The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the Baseline Requirements Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated after the Effective Date (1 July 2012) are set in accordance with RFC 5280.
6	During the audit period, validation of domain authorization was conducted by official documents that were issued by government organizations who have legal ownership of requesting domains, 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.
7	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

Observation	Relevant WebTrust Criteria
	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 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;

	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)
8	An examination on the information verification requirements for Validation Specialists of CA and Delegated Third Party was not performed This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 6.2 and 6.4 to not be met.	**P2, 6.2:** The CA maintains controls to provide reasonable assurance that: • the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. • the CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. • the CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. • the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements. • all personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs. **P2, 6.4:** The CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the

Observation	Relevant WebTrust Criteria
	document retention and event logging requirements of Section 5.4.1.