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 at 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 business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Ministry of Education CA Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
  - MOE provides its services in accordance with its Certification Practice Statement

- 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; and
  - 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.1.

MOE does not escrow its CA keys, does not provide CA-Provided Subscriber Key Generation Services and CA-Provided Subscriber Key Storage and Recovery Services, and Integrated Circuit Card (ICC) lifecycle management, and does not provide Subordinate CA certificate lifecycle management services. Accordingly, our procedures did not extend to controls that would address those criteria.

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 v2.1.

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

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

comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with 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 key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations, and over the development, maintenance, and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

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

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at 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.

Opinion

In our opinion, 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 v2.1.

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 v2.1, nor the suitability of any of MOE's services for any customer's intended purpose.

Use of the WebTrust seal

MOE'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.

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

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 the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate validation
- Subscriber key management

The management of MOE is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key management controls, 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 MOE's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

MOE management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in MOE management's opinion, in providing its Certification Authority (CA) services in Republic of Korea, throughout the period 1 January 2019 through 31 December 2019, MOE has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Ministry of Education CA Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
  - MOE provides its services in accordance with its Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles; and
  - 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.1, including the following:

CA Business Practices Disclosure
- Certification Practice Statement (CPS)

CA Business Practices Management
- Certification Practice Statement Management

교육부

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

Subscriber Key Lifecycle Management Controls
- 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

MOE does not escrow its CA keys, does not provide CA-Provided Subscriber Key Generation Services and CA-Provided Subscriber Key Storage and Recovery Services, and Integrated Circuit Card (ICC) lifecycle management, and does not provide Subordinate CA certificate lifecycle management services. Accordingly, our assertion does not extend to controls that would address those criteria.

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