Deloitte Anjin LLC
9F., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
07326, Korea

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

INDEPENDENT ASSURANCE REPORT

To the management of Ministry of the Interior and Safety ("MOIS"):

Scope
We have been engaged, in a reasonable assurance engagement, to report on MOIS management's assertion that for its Certification Authority (CA) operations at the primary data center in Gwangju, Republic of Korea, and the secondary data center in Daejeon, Republic of Korea, throughout the period 22 April 2025 to 21 April 2026 for its CAs as enumerated in Attachment A in scope for TLS Baseline Requirements, MOIS has:

- disclosed its TLS certificate lifecycle management business practices in its:
  - GSSL Certificate Policy(CP) / Certification Practices Statement(CPS) v2.1;
  - GSSL Certification Practices Statement(CPS) v2.0;
  - GSSL Certification Practices Statement(CPS) v1.9;
  - GSSL Certification Practices Statement(CPS) v1.8; and
  - GSSL Certification Practices Statement(CPS) v1.7;

  including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the MOIS website, and provided such services in accordance with its disclosed practices

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

- 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 – TLS Baseline v2.9.

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust Principles and Criteria for Certification Authorities – Network Security address this requirement and are reported on in a separate report.

Certification Authority's responsibilities
MOIS'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 –TLS Baseline v2.9.

Our independence and quality management
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 Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner'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:

Deloitte.

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

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

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

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

Opinion
In our opinion, throughout the period 22 April 2025 to 21 April 2026, MOIS 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 – TLS Baseline v2.9.

This report does not include any representation as to the quality of MOIS's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.9, nor the suitability of any of MOIS's services for any customer's intended purpose.

Use of the WebTrust seal
MOIS's use of the WebTrust for Certification Authorities – TLS Baseline 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 Anjin LLC.

Deloitte Anjin LLC
Seoul, Republic of Korea
20 July 2026

Deloitte.

Attachment A

List of CAs in Scope

Root CA
#1. MOIS SSL Root CA
OV TLS Issuing CA
#2. MOIS SSL Server CA

Deloitte.

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial Number	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA256 Fingerprint
1	1	CN=MOIS SSL Root CA O=Ministry of the Interior and Safety C=KR	CN=MOIS SSL Root CA O=Ministry of the Interior and Safety C=KR	0449EFC3EB1A24235A08C1DD3B7062C1167488F2	rsaEncryption	4096 Bits	Sha256	22 February 2023 06:38:27 GMT	22 February 2043 01:00:00 GMT	375A09FBCE24E1E767C7BE0768CCDC281F84310D	1CF341AE35341AC3AE1DC68D5B10DC0C9DC1307656F75FD92CA2C68489D52E9A
2	1	CN=MOIS SSL Server CA O=Ministry of the Interior and Safety C=KR	CN=MOIS SSL Root CA O=Ministry of the Interior and Safety C=KR	07A6BCD13F5A00A94013438694C289585616DB3B	rsaEncryption	3072 Bits	Sha256	23 February 2023 09:32:48 GMT	23 February 2033 01:00:00 GMT	5B2F93083BC8B13D111F5F4119F4A754C0C687C5	C435BF6129E9773DECAECA19CA8AC9C372E72BB0D280983C9D45D5602710A556

Ministry of the Interior and Safety

Ministry of the Interior and Safety MANAGEMENT'S ASSERTION

Ministry of the Interior and Safety ("MOIS") operates the Certification Authority (CA) services known as Attachment A in scope for TLS Baseline Requirements and provides TLS CA services.

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

MOIS management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in providing its TLS Certification Authority (CA) services at the primary data center in Gwangju, Republic of Korea, and the secondary data center in Daejeon, Republic of Korea, throughout the period 22 April 2025 to 21 April 2026, MOIS has:

- disclosed its TLS certificate lifecycle management business practices in its:
  - GSSL Certificate Policy(CP) / Certification Practices Statement(CPS) v2.1;
  - GSSL Certification Practices Statement(CPS) v2.0;
  - GSSL Certification Practices Statement(CPS) v1.9;
  - GSSL Certification Practices Statement(CPS) v1.8; and
  - GSSL Certification Practices Statement(CPS) v1.7

  including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the MOIS website, and provided such services in accordance with its disclosed practices

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

- 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 – TLS Baseline v2.9.



Sang Chul Park
Deputy Director, Digital Security Policy Division
Ministry of the Interior and Safety
Republic of Korea
20 July 2026

Ministry of the Interior and Safety

Attachment A

List of CAs in Scope

Root CA
#1. MOIS SSL Root CA
OV TLS Issuing CA
#2. MOIS SSL Server CA

Ministry of the Interior and Safety

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial Number	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA256 Fingerprint
1	1	CN=MOIS SSL Root CA O=Ministry of the Interior and Safety C=KR	CN=MOIS SSL Root CA O=Ministry of the Interior and Safety C=KR	0449EFC3EB1A24235A08C1DD3B7062C1167488F2	rsaEncryption	4096 Bits	Sha256	22 February 2023 06:38:27 GMT	22 February 2043 01:00:00 GMT	375A09FBCE24E1E767C7BE0768CCDC281F84310D	1CF341AE35341AC3AE1DC68D5B10DC0C9DC1307656F75FD92CA2C68489D52E9A
2	1	CN=MOIS SSL Server CA O=Ministry of the Interior and Safety C=KR	CN=MOIS SSL Root CA O=Ministry of the Interior and Safety C=KR	07A6BCD13F5A00A94013438694C289585616DB3B	rsaEncryption	3072 Bits	Sha256	23 February 2023 09:32:48 GMT	23 February 2033 01:00:00 GMT	5B2F93083BC8B13D111F5F4119F4A754C0C687C5	C435BF6129E9773DECAECA19CA8AC9C372E72BB0D280983C9D45D5602710A556