

INDEPENDENT ASSURANCE REPORT

To the Management of NAVER Cloud Trust Services Corp. (“NCTS”):

Scope

We have been engaged, in a reasonable assurance engagement, to report on NCTS management’s [assertion](#) that for its Certification Authority (CA) operations at Chuncheon-si, Gangwon-do, Anyang-si, Gyeonggi-do and Seongnam-si, Gyeonggi-do, Republic of Korea, throughout the period 1 October 2024 to 30 September 2025 for its CAs as enumerated in [Appendix A](#), NCTS has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement as enumerated in [Appendix B](#)
- maintained effective controls to provide reasonable assurance that:
 - o NCTS provides its services in accordance with its Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
 - o the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - o the integrity of subscriber certificates it manages is established and protected throughout their lifecycles;
 - o subscriber information is properly authenticated (for the registration activities performed by NCTS); and
 - o cross certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
 - o logical and physical access to CA systems and data is restricted to authorized individuals;
 - o the continuity of key and certificate management operations is maintained; and
 - o 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 v2.2.2](#).

NCTS does not escrow its CA keys, does not provide subscriber key generation services, does not provide subscriber key storage and recovery services, does not support integrated circuit card lifecycle management services, does not provide certificate suspension services, 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

NCTS’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 v2.2.2](#).

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:

1. obtaining an understanding of NCTS'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 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.

The relative effectiveness and significance of specific controls at NCTS 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 unauthorised 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 1 October 2024 to 30 September 2025, NCTS 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 v2.2.2](#).

This report does not include any representation as to the quality of NCTS's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), nor the suitability of any of NCTS's services for any customer's intended purpose.

Use of the WebTrust seal

NCTS'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.



Tel: +82 2 2112 0001
Fax: +82 2 2112 0501
<http://www.kpmg.com/kr>

Gangnam Finance Center, 152,
Teheran-ro, Gangnam-gu,
Seoul, Republic of Korea

KPMG Samjong Accounting Corp.

KPMG Samjong Accounting Corp.
Seoul, Republic of Korea
21 November 2025

Appendix A – List of CAs In-Scope

| CA# | Cert# | Subject | Issuer | Serial Number | Key Algorithm | Key Sizes | Digest Algorithm | Not Before | Not After | Subject Key Identifier | SHA256 Fingerprint |
|-------------------------|-------|---|---|--|---------------|-----------|------------------|-----------------------------|-----------------------------|--|--|
| Root CAs | | | | | | | | | | | |
| 1 | 1 | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | 0194301EA20BDD F5C5332AB14344 71F8D6504D0D | rsaEncryption | 4096 Bits | sha384 | 18 Aug 2017 08:58:42 GMT | 18 Aug 2037 23:59:59 GMT | D29F88DFA1CD2 CBDECF53B01019 33327B2EB604B | 88F438DCF8FFD1FA8F429115FF E5F82AE1E06E0C70C375FAAD71 7B34A49E7265 |
| 2 | 1 | CN = NAVER Cloud Trust Services RSA Root G1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Cloud Trust Services RSA Root G1 O = NAVER Cloud Trust Services Corp. C = KR | 0193205EA337C2 A7BB2756B16E35 C27119203EF1 | rsaEncryption | 4096 Bits | sha384 | 07 Jun 2023 06:30:54 GMT | 06 Jun 2043 23:59:59 GMT | EF080D6D82682E 1ADA5AEDF3FEE 2A206F39BE7F8 | 49A2762987788D4834B32305D76 7760F244D507742E8C2539FD4C A3AD52C16EE |
| 3 | 1 | CN = NAVER Cloud Trust Services ECC Root G1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Cloud Trust Services ECC Root G1 O = NAVER Cloud Trust Services Corp. C = KR | 017F20237EE5821 13466C837E47815 E5BE12BA15 | ecdsa | 384 Bits | sha384 | 07 Jun 2023 13:20:29 GMT | 06 Jun 2043 23:59:59 GMT | 3A0A3FAD7D8E32 BDF26CFB8952E3 D0F62AC18F79 | A7C8681042F3675AA8505D3BA3 13D80F8AC3250FDF874AD29B83 4689C087FB11 |
| Cross-Signed CAs | | | | | | | | | | | |
| 2 | 2 | CN = NAVER Cloud Trust Services RSA Root G1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | 104872734231F16 88ABC4792E5759 5957126C9EA | rsaEncryption | 4096 Bits | sha384 | 09 Dec 2024 00:00:00 GMT | 09 Dec 2038 11:59:59 GMT | EF080D6D82682E 1ADA5AEDF3FEE 2A206F39BE7F8 | 67F9DA159B4AEB3B55E2C37C40 2E91CEFE87D784D81CE949FA53 2184620C3CFD |
| 3 | 2 | CN = NAVER Cloud Trust Services ECC Root G1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | 112D765CBA0A84 0B06E8B2A66A90 5E17C6A835C7 | ecdsa | 384 Bits | sha384 | 09 Dec 2024 00:00:00 GMT | 09 Dec 2038 11:59:59 GMT | 3A0A3FAD7D8E32 BDF26CFB8952E3 D0F62AC18F79 | 355CD125F93CE5BF268F958C1D 1F8AAD289FDBD41BAFAA85669 1DB7260F2ACAB |
| Intermediate CAs | | | | | | | | | | | |
| 4 | 1 | CN = NAVER Secure Certification Authority 1 O = NAVER BUSINESS PLATFORM Corp. C = KR | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | 06046233A582557 6A48272694718A8 000F2F000D | rsaEncryption | 2048 Bits | sha256 | 18 Aug 2017 10:05:55 GMT | 18 Aug 2027 23:59:59 GMT | E9F9EB97BE21F2 54C7E926370239 BAFCB19B0CE9 | C5EB1A7639B9D8D70B4F82ADD 80794175EE4B6A3DB1861B3871 7C96FC1914927 |
| 5 | 1 | CN = NAVER Cloud Trust Services G1 RSA CA1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Cloud Trust Services RSA Root G1 O = NAVER Cloud Trust Services Corp. C = KR | 04A10F19A216DC BBF6088447D8F3 71ADCEE7D249 | rsaEncryption | 4096 Bits | sha384 | 07 Jun 2023 09:47:29 GMT | 06 Jun 2033 23:59:59 GMT | 14BBBA4ABDDA9 ED64BD9F0940F9 C120DE204910D | 17832DBB48F609B722A27507F1 D327DE062D7F7B85B71325D8D D99B19FB5BAD4 |
| 6 | 1 | CN = NAVER Cloud Trust Services G1 ECC CA1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Cloud Trust Services ECC Root G1 O = NAVER Cloud Trust Services Corp. C = KR | 05FAD6522186F62 AE88BCB51D545F 41EA4A35736 | ecdsa | 384 Bits | sha384 | 07 Jun 2023 14:24:08 GMT | 06 Jun 2033 23:59:59 GMT | DE51B87731B450 000DE025D58F2E 138E30802E76 | 882D9924FC69A00574D54C2BB4 014825A1C1C71FA1D0238CAC86 5FE0AA4AD60B |



Tel: +82 2 2112 0001
Fax: +82 2 2112 0501
<http://www.kpmg.com/kr>

Gangnam Finance Center, 152,
Teheran-ro, Gangnam-gu,
Seoul, Republic of Korea

Appendix B – Certification Practice Statement and Certificate Policy Versions In-Scope

| Policy Name | Version | Date |
|---|---------|------------------|
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.6 | 19 June 2025 |
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.5 | 5 March 2025 |
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.4 | 26 November 2024 |
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.3 | 17 October 2024 |
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.2 | 27 December 2023 |

NAVER Cloud Trust Services Corp. MANAGEMENT'S ASSERTION

NAVER Cloud Trust Services Corp. ("NCTS") operates the Certification Authority (CA) services known as [Appendix A](#), and provides the following CA services:

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Cross certification

The management of NCTS 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, certificate lifecycle management controls, and cross 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 NCTS's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

NCTS management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in NCTS management's opinion, in providing its Certification Authority (CA) services at Chuncheon-si, Gangwon-do, Anyang-si, Gyeonggi-do and Seongnam-si, Gyeonggi-do, Republic of Korea, throughout the period 1 October 2024 to 30 September 2025, NCTS has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement as enumerated in [Appendix B](#)
- maintained effective controls to provide reasonable assurance that:
 - o NCTS provides its services in accordance with its Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
 - o the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - o the integrity of subscriber certificates it manages is established and protected throughout their lifecycles;
 - o subscriber information is properly authenticated (for the registration activities performed by NCTS); and
 - o cross certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
 - o logical and physical access to CA systems and data is restricted to authorized individuals;
 - o the continuity of key and certificate management operations is maintained; and
 - o 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 v2.2.2](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and 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
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate and Cross Certificate Lifecycle Management Controls

- Cross Certificate Lifecycle Management

NCTS does not escrow its CA keys, does not provide subscriber key generation services, does not provide subscriber key storage and recovery services, does not support integrated circuit card lifecycle management services, does not provide certificate suspension services, and does not provide subordinate CA certificate lifecycle management services. Accordingly, our procedures did not extend to controls that would address those criteria.

NAVER Cloud

Trust Services

NAVER Green Factory, 6, Buljeong-ro,
Jeongja-dong, Bundang-gu, Seongnam-si,
Gyeonggi-do, Republic of Korea

박한용

Park, Han Yong
Chief Privacy Officer / Data Protection Officer
NAVER Cloud Trust Services Corp.
Republic of Korea
21 November 2025

Appendix A – List of CAs In-Scope

| CA# | Cert# | Subject | Issuer | Serial Number | Key Algorithm | Key Sizes | Digest Algorithm | Not Before | Not After | Subject Key Identifier | SHA256 Fingerprint |
|-------------------------|-------|---|---|--|---------------|-----------|------------------|-----------------------------|-----------------------------|--|--|
| Root CAs | | | | | | | | | | | |
| 1 | 1 | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | 0194301EA20BDD F5C5332AB14344 71F8D6504D0D | rsaEncryption | 4096 Bits | sha384 | 18 Aug 2017 08:58:42 GMT | 18 Aug 2037 23:59:59 GMT | D29F88DFA1CD2 CBDECF53B01019 33327B2EB604B | 88F438DCF8FFD1FA8F429115FF E5F82AE1E06E0C70C375FAAD71 7B34A49E7265 |
| 2 | 1 | CN = NAVER Cloud Trust Services RSA Root G1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Cloud Trust Services RSA Root G1 O = NAVER Cloud Trust Services Corp. C = KR | 0193205EA337C2 A7BB2756B16E35 C27119203EF1 | rsaEncryption | 4096 Bits | sha384 | 07 Jun 2023 06:30:54 GMT | 06 Jun 2043 23:59:59 GMT | EF080D6D82682E 1ADA5AEDF3FEE 2A206F39BE7F8 | 49A2762987788D4834B32305D76 7760F244D507742E8C2539FD4C A3AD52C16EE |
| 3 | 1 | CN = NAVER Cloud Trust Services ECC Root G1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Cloud Trust Services ECC Root G1 O = NAVER Cloud Trust Services Corp. C = KR | 017F20237EE5821 13466C837E47815 E5BE12BA15 | ecdsa | 384 Bits | sha384 | 07 Jun 2023 13:20:29 GMT | 06 Jun 2043 23:59:59 GMT | 3A0A3FAD7D8E32 BDF26CFB8952E3 D0F62AC18F79 | A7C8681042F3675AA8505D3BA3 13D80F8AC3250FDF874AD29B83 4689C087FB11 |
| Cross-Signed CAs | | | | | | | | | | | |
| 2 | 2 | CN = NAVER Cloud Trust Services RSA Root G1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | 104872734231F16 88ABC4792E5759 5957126C9EA | rsaEncryption | 4096 Bits | sha384 | 09 Dec 2024 00:00:00 GMT | 09 Dec 2038 11:59:59 GMT | EF080D6D82682E 1ADA5AEDF3FEE 2A206F39BE7F8 | 67F9DA159B4AEB3B55E2C37C40 2E91CEFE87D784D81CE949FA53 2184620C3CFD |
| 3 | 2 | CN = NAVER Cloud Trust Services ECC Root G1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | 112D765CBA0A84 0B06E8B2A66A90 5E17C6A835C7 | ecdsa | 384 Bits | sha384 | 09 Dec 2024 00:00:00 GMT | 09 Dec 2038 11:59:59 GMT | 3A0A3FAD7D8E32 BDF26CFB8952E3 D0F62AC18F79 | 355CD125F93CE5BF268F958C1D 1F8AAD289FDBD41BAFAA85669 1DB7260F2ACAB |
| Intermediate CAs | | | | | | | | | | | |
| 4 | 1 | CN = NAVER Secure Certification Authority 1 O = NAVER BUSINESS PLATFORM Corp. C = KR | CN = NAVER Global Root Certification Authority O = NAVER BUSINESS PLATFORM Corp. C = KR | 06046233A582557 6A48272694718A8 000F2F000D | rsaEncryption | 2048 Bits | sha256 | 18 Aug 2017 10:05:55 GMT | 18 Aug 2027 23:59:59 GMT | E9F9EB97BE21F2 54C7E926370239 BAFCB19B0CE9 | C5EB1A7639B9D8D70B4F82ADD 80794175EE4B6A3DB1861B3871 7C96FC1914927 |
| 5 | 1 | CN = NAVER Cloud Trust Services G1 RSA CA1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Cloud Trust Services RSA Root G1 O = NAVER Cloud Trust Services Corp. C = KR | 04A10F19A216DC BBF6088447D8F3 71ADCEE7D249 | rsaEncryption | 4096 Bits | sha384 | 07 Jun 2023 09:47:29 GMT | 06 Jun 2033 23:59:59 GMT | 14BBBA4ABDDA9 ED64BD9F0940F9 C120DE204910D | 17832DBB48F609B722A27507F1 D327DE062D7F7B85B71325D8D D99B19FB5BAD4 |
| 6 | 1 | CN = NAVER Cloud Trust Services G1 ECC CA1 O = NAVER Cloud Trust Services Corp. C = KR | CN = NAVER Cloud Trust Services ECC Root G1 O = NAVER Cloud Trust Services Corp. C = KR | 05FAD6522186F62 AE88BCB51D545F 41EA4A35736 | ecdsa | 384 Bits | sha384 | 07 Jun 2023 14:24:08 GMT | 06 Jun 2033 23:59:59 GMT | DE51B87731B450 000DE025D58F2E 138E30802E76 | 882D9924FC69A00574D54C2BB4 014825A1C1C71FA1D0238CAC86 5FE0AA4AD60B |

Appendix B – Certification Practice Statement and Certificate Policy Versions In-Scope

| Policy Name | Version | Date |
|---|---------|------------------|
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.6 | 19 June 2025 |
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.5 | 5 March 2025 |
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.4 | 26 November 2024 |
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.3 | 17 October 2024 |
| NAVER Cloud Trust Services Certification Practice Statement | 1.0.2 | 27 December 2023 |