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 2023 to 30 September 2024 for its CAs as enumerated in Appendix A in scope for SSL Baseline Requirements, NCTS has:

- disclosed its SSL certificate lifecycle management business practices in its Certification Practice Statement as enumerated in Appendix B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the NCTS 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 NCTS)

- 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 – SSL Baseline with Network Security v2.7.

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 – SSL Baseline with Network Security v2.7.

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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates;
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.

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 2023 to 30 September 2024, 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 – SSL Baseline with Network Security v2.7.

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 – SSL Baseline with Network Security v2.7, nor the suitability of any of NCTS's services for any customer's intended purpose.

Other matters

Without modifying our opinion, we noted the following other matters during our procedures:

Matter Topic		Matter Description
1	Certificate Issuance	NAVER Cloud Trust Services disclosed in Mozilla Bug #1866448 that it issued a DV certificate that was improperly validated.
2	Certificate Issuance	NAVER Cloud Trust Services disclosed in Mozilla Bug #1908128 that it issued a certificate issued with an incorrect OCSP URI in AIA.
3	Certificate Issuance	NAVER Cloud Trust Services disclosed in Mozilla Bug #1908130 that it issued 3 ECC certificates with incorrect keyUsage.

While the NCTS assertion notes all issues disclosed on Bugzilla from 1 October 2023 through the date of this report, we have only noted those instances relevant to the CAs enumerated in

Appendix A and applicable to the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7.

Use of the WebTrust seal

NCTS's use of the WebTrust for Certification Authorities – SSL 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.

KPMG Samjong Accounting Corp.

KPMG Samjong Accounting Corp.
Seoul, Republic of Korea
22 November 2024

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	0194301EA20BDDF5C5332AB1434471F8D6504D0D	rsaEncryption	4096 Bits	sha384	18 Aug 2017 08:58:42 GMT	18 Aug 2037 23:59:59 GMT	D29F88DFA1CD2CBDECF53B0101933327B2EB604B	88F438DCF8FFD1FA8F429115FFE5F82AE1E06E0C70C375FAAD717B34A49E7265
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	0193205EA337C2A7BB2756B16E35C27119203EF1	rsaEncryption	4096 Bits	sha384	07 Jun 2023 06:30:54 GMT	06 Jun 2043 23:59:59 GMT	EF080D6D82682E1ADA5AEDF3FEE2A206F39BE7F8	49A2762987788D4834B32305D767760F244D507742E8C2539FD4CA3AD52C16EE
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	017F20237EE582113466C837E47815E5BE12BA15	ecdsa	384 Bits	sha384	07 Jun 2023 13:20:29 GMT	06 Jun 2043 23:59:59 GMT	3A0A3FAD7D8E32BDF26CFB8952E3D0F62AC18F79	A7C8681042F3675AA8505D3BA313D80F8AC3250FDF874AD29B834689C087FB11
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	06046233A5825576A48272694718A8000F2F000D	rsaEncryption	2048 Bits	sha256	18 Aug 2017 10:05:55 GMT	18 Aug 2027 23:59:59 GMT	E9F9EB97BE21F254C7E926370239BAFCB19B0CE9	C5EB1A7639B9D8D70B4F82ADD80794175EE4B6A3DB1861B38717C96FC1914927
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	04A10F19A216DCBBF6088447D8F371ADCEE7D249	rsaEncryption	4096 Bits	sha384	07 Jun 2023 09:47:29 GMT	06 Jun 2033 23:59:59 GMT	14BBBA4ABDDA9ED64BD9F0940F9C120DE204910D	17832DBB48F609B722A27507F1D327DE062D7F7B85B71325D8DD99B19FB5BAD4
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	05FAD6522186F62AE88BCB51D545F41EA4A35736	ecdsa	384 Bits	sha384	07 Jun 2023 14:24:08 GMT	06 Jun 2033 23:59:59 GMT	DE51B87731B450000DE025D58F2E138E30802E76	882D9924FC69A00574D54C2BB4014825A1C1C71FA1D0238CAC865FE0AA4AD60B

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

Policy Name	Version	Date
NAVER Cloud Trust Services Certification Practice Statement	1.0.2	27 December 2023
NAVER Cloud Trust Services Certification Practice Statement	1.0.1	24 August 2023

NAVER Cloud
Trust Services

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

NAVER Cloud Trust Services Corp. MANAGEMENT’S ASSERTION

NAVER Cloud Trust Services (“NCTS”) operates the Certification Authority (CA) services known as Appendix A in scope for SSL Baseline Requirements and provides SSL CA services.

The management of NCTS is responsible for establishing and maintaining effective controls over its SSL CA operations, including its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL 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 SSL CA services. Based on that assessment, in providing its SSL 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 2023 to 30 September 2024, NCTS has:

- disclosed its SSL certificate lifecycle management business practices in its Certification Practice Statement as enumerated in Appendix B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the NCTS 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 NCTS)

- 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 – SSL Baseline with Network Security v2.7.

NCTS has disclosed the following matters publicly on Mozilla's Bugzilla platform. These matters were included below due to being open during the period 1 October 2023 through the date of this report.

Bug ID	Summary	Opened	Closed	Resolution
1866448	NAVER Cloud Trust Services: DV Certificate issued with improperly validated	24 November 2023	14 February 2024	FIXED
1908128	NAVER Cloud Trust Services: Certificate issued with incorrect OCSP URI in AIA	16 July 2024	28 August 2024	FIXED
1908130	NAVER Cloud Trust Services: Incorrect keyUsage for ECC certificate	16 July 2024	28 August 2024	FIXED

Park, Han Yong
Chief Privacy Officer / Data Protection Officer
NAVER Cloud Trust Services Corp.
Republic of Korea
22 November 2024

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	0194301EA20BDDF5C5332AB1434471F8D6504D0D	rsaEncryption	4096 Bits	sha384	18 Aug 2017 08:58:42 GMT	18 Aug 2037 23:59:59 GMT	D29F88DFA1CD2CBDECF53B0101933327B2EB604B	88F438DCF8FFD1FA8F429115FFE5F82AE1E06E0C70C375FAAD717B34A49E7265
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	0193205EA337C2A7BB2756B16E35C27119203EF1	rsaEncryption	4096 Bits	sha384	07 Jun 2023 06:30:54 GMT	06 Jun 2043 23:59:59 GMT	EF080D6D82682E1ADA5AEDF3FEE2A206F39BE7F8	49A2762987788D4834B32305D767760F244D507742E8C2539FD4CA3AD52C16EE
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	017F20237EE582113466C837E47815E5BE12BA15	ecdsa	384 Bits	sha384	07 Jun 2023 13:20:29 GMT	06 Jun 2043 23:59:59 GMT	3A0A3FAD7D8E32BDF26CFB8952E3D0F62AC18F79	A7C8681042F3675AA8505D3BA313D80F8AC3250FDF874AD29B834689C087FB11
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	06046233A5825576A48272694718A8000F2F000D	rsaEncryption	2048 Bits	sha256	18 Aug 2017 10:05:55 GMT	18 Aug 2027 23:59:59 GMT	E9F9EB97BE21F254C7E926370239BAFCB19B0CE9	C5EB1A7639B9D8D70B4F82ADD80794175EE4B6A3DB1861B38717C96FC1914927
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	04A10F19A216DCBBF6088447D8F371ADCEE7D249	rsaEncryption	4096 Bits	sha384	07 Jun 2023 09:47:29 GMT	06 Jun 2033 23:59:59 GMT	14BBBA4ABDDA9ED64BD9F0940F9C120DE204910D	17832DBB48F609B722A27507F1D327DE062D7F7B85B71325D8DD99B19FB5BAD4
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	05FAD6522186F62AE88BCB51D545F41EA4A35736	ecdsa	384 Bits	sha384	07 Jun 2023 14:24:08 GMT	06 Jun 2033 23:59:59 GMT	DE51B87731B450000DE025D58F2E138E30802E76	882D9924FC69A00574D54C2BB4014825A1C1C71FA1D0238CAC865FE0AA4AD60B

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

Policy Name	Version	Date
NAVER Cloud Trust Services Certification Practice Statement	1.0.2	27 December 2023
NAVER Cloud Trust Services Certification Practice Statement	1.0.1	24 August 2023