Independent Assurance Report

To the management of the National Development Council：

Scope

We have been engaged, in a reasonable assurance engagement, to report on National Development Council (NDC) management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan, throughout the period April 1, 2018 through March 31, 2019 for its CAs as enumerated in Appendix for SSL Baseline Requirements and Network Security Requirements, NDC has:

- Disclosed its SSL certificate lifecycle management business practices in its:
  - Government Root Certification Authority Certification (GRCA) Practice Statement V1.5; and
  - Government Certification Authority Certification (GCA) Practice Statement V1.9; and
  - Certificate Policy for the Government Public Key Infrastructure (GPKI) V2.0

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the GRCA and GCA websites, 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 GCA.

- 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

NDC'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 for Certification Authorities – SSL Baseline with Network Security Version 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 behavior.

The firm applies International Standard on Quality Control, 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.

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 attestation standards established by the American Institute of Certified Public Accountants/CPA Canada. 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 GCA'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 GRCA and GCA'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 GRCA and GCA 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, GRCA and GCA'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 April 1, 2018 to March 31, 2019, NDC 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 GRCA and GCA'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 GRCA and GCA's services for any customer's intended purpose.

Use of the WebTrust seal

GRCA and GCA's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security 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

Certified Public Accountants

Taipei, Taiwan, ROC

June 14, 2019

Appendix – List of Root and Subordinate CAs[1] in Scope

GRCA	Root CA Certificate	
	Subject	Issuer
	O=Government Root Certification Authority C=TW	O=Government Root Certification Authority C=TW
	Certificate Related Information	Key Related Information
	Serial Number: 1f 9d 59 5a d7 2f c2 06 44 a5 80 08 69 e3 5e f6 Signature Algorithm: sha1RSA Not Before: 2002-12-05 09:23:33 p.m.(UTC+8:00) Not After: 2032-12-05 09:23:33 p.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: f4 8b 11 bf de ab be 94 54 20 71 e6 41 de 6b be 88 2b 40 b9 Thumbprint Algorithm: sha2 Thumbprint: 76 00 29 5e ef e8 5b 9e 1f d6 24 db 76 06 2a aa ae 59 81 8a 54 d2 77 4c d4 c0 b2 c0 11 31 e1 b3	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: cc cc ef cc 29 60 a4 3b b1 92 b6 3c fa 32 62 8f ac 25 15 3b
	Additional Information	Remark
		■ Self-signed by 1st Generation of GRCA Root Certification Authority ■ Cross Signed with GRCA-G2

[1] There are 3 other Sub-CAs, MOICA, MOEACA, and HCA, owned by different Government Agencies will covered by other independent audits.

GRCA - G2	Root CA Certificate	
	Subject	Issuer
	O=Government Root Certification Authority C=TW	O=Government Root Certification Authority C=TW
	Certificate Related Information	Key Related Information
	Serial Number: 00 b6 4b 88 07 e2 23 ee c8 5c 12 ad a6 0e 06 a1 f2 Signature Algorithm: sha256RSA Not Before: 2012-09-28 04:58:51 p.m.(UTC+8:00) Not After: 2037-12-31 11:59:59 p.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: b0 91 aa 91 38 47 f3 13 d7 27 bc ef c8 17 9f 08 6f 3a 8c 0f Thumbprint Algorithm: sha2 Thumbprint: 70 b9 22 bf da 0e 3f 4a 34 2e 4e e2 2d 57 9a e5 98 d0 71 cc 5e c9 c3 0f 12 36 80 34 03 88 ae a5	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: d5 67 1d e0 9c 7a 2c 9c cb c5 98 e7 1d 07 26 2a 86 ec 74 cd Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
		■ Self-signed by 2nd Generation of GRCA Root Certification Authority ■ Cross Signed with GRCA

GRCA (Old with New)	Root CA Certificate(Cross Signed)	
	Subject	Issuer
	O=Government Root Certification Authority C=TW	O=Government Root Certification Authority C=TW
	Certificate Related Information	Key Related Information
	Serial Number: 34 75 6f 0a 69 75 80 f7 55 3d 9b e9 1c ca 1e a4 Signature Algorithm: sha256RSA Not Before: 2012-09-28 05:13:29 p.m.(UTC+8:00) Not After: 2032-12-05 09:23:33 p.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: 2d 25 79 12 db 3d a9 bb fb ad 28 14 47 22 fc f6 d7 de 02 cb Thumbprint Algorithm: sha2 Thumbprint: fe bf 42 f9 be 5a bf dd b8 17 5d 01 02 39 f9 03 6f e9 0d 33 3e 70 8e 13 cc 5e ed ff d5 2d 0a 97	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: cc cc ef cc 29 60 a4 3b b1 92 b6 3c fa 32 62 8f ac 25 15 3b Subject Key Identifiers: d5 67 1d e0 9c 7a 2c 9c cb c5 98 e7 1d 07 26 2a 86 ec 74 cd Basic Constraint: Subject Type=CA Path Length Constraint=None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL_SHA2/CA.crl Certificate Policy: [1]2.16.886.101.0.3.1 [2]2.16.886.101.0.3.2 [3]2.16.886.101.0.3.3 [4]2.16.886.101.0.3.4 [5]2.16.886.101.0.3.0 [6]2.23.140.1.2.2	■ CA certificate of 1st Generation of GRCA Certification Authority signed by GRCA-G2

<table>
<tr><td rowspan="6">GRCA
(New with Old)</td><td colspan="2">Root CA Certificate(Cross Signed)</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>O=Government Root Certification Authority
C=TW</td><td>O=Government Root Certification Authority
C=TW</td></tr>
<tr><td>Certificate Related Information</td><td>Key Related Information</td></tr>
<tr><td>Serial Number: 32 5c 89 3b 26 38 91 0c 25 77 64 f3 48 d0 ad a5
Signature Algorithm: sha256RSA
Not Before: 2012-09-28 05:07:12 p.m.(UTC+8:00)
Not After: 2032-12-05 09:23:33 p.m.(UTC+8:00)
Thumbprint Algorithm: sha1
Thumbprint: ce ef 60 1f 67 b1 33 a5 08 75 dd c5 82 6b 0d 22 cb 41 e9 e9
Thumbprint Algorithm: sha2
Thumbprint: 90 fa 98 d6 46 dd 5f 00 60 2d 68 d1 7d d7 6b 55 ee 51 cd a3 d3 92 2f 0d bd d1 04 80 f5 99 0a cd</td><td>Subject Public Key: RSA(4096 bits)
Authority Key Identifiers: d5 67 1d e0 9c 7a 2c 9c cb c5 98 e7 1d 07 26 2a 86 ec 74 cd
Subject Key Identifiers: cc cc ef cc 29 60 a4 3b b1 92 b6 3c fa 32 62 8f ac 25 15 3b
Basic Constraint: Subject Type=CA
Path Length Constraint=None
Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td>CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL2/CA.crl
Certificate Policy:
[1]2.16.886.101.0.3.1
[2]2.16.886.101.0.3.2
[3]2.16.886.101.0.3.3
[4]2.16.886.101.0.3.4
[5]2.16.886.101.0.3.0</td><td>■ CA certificate of 2nd Generation of GRCA Certification Authority signed by GRCA</td></tr>
</table>

GRCA (G1.5 with G1)	Root CA Certificate(Cross Signed)	
	Subject	Issuer
	CN = Government Root Certification Authority - G1.5 O = 行政院 C = TW	O=Government Root Certification Authority C=TW
	Certificate Related Information	Key Related Information
	Serial Number: 33 e5 4a d1 c0 6f 18 31 4a 9c 89 4e 02 8b cc f3 Signature Algorithm: sha256RSA Not Before: 2017-07-19 10:43:37 a.m.(UTC+8:00) Not After: 2020-07-19 10:43:37 a.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: 83 cc 39 95 70 a3 b4 e9 7e a9 d9 62 31 0c b1 c6 86 ca 92 9a Thumbprint Algorithm: sha2 Thumbprint: a4 23 a3 34 93 b3 19 53 22 6d f9 64 77 62 7d bd 05 67 56 70 42 11 00 1b 61 61 fb 5f 82 99 dc 3a	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: cc cc ef cc 29 60 a4 3b b1 92 b6 3c fa 32 62 8f ac 25 15 3b Subject Key Identifiers: cf ea 9e 13 53 05 f1 34 7b 7d bf a5 ad 1f e1 06 ce 4f 00 91 Basic Constraint: Subject Type=CA Path Length Constraint=None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL_SHA2/CA.crl Certificate Policy: [1]2.16.886.101.0.3.1 [2]2.16.886.101.0.3.2 [3]2.16.886.101.0.3.3 [4]2.16.886.101.0.3.4 [5]2.16.886.101.0.3.0 [6]2.23.140.1.2.2	■ CA certificate of 1.5 Generation of GRCA Certification Authority signed by GRCA

GRCA (G2 with G1.5)	Root CA Certificate(Cross Signed)	
	Subject	Issuer
	O=Government Root Certification Authority C=TW	CN = Government Root Certification Authority O = 行政院 C = TW
	Certificate Related Information	Key Related Information
	Serial Number: 00 a3 94 3b 6f 10 26 51 ce ba 53 91 23 74 9a 2a 2a Signature Algorithm: sha256RSA Not Before: 2017-07-19 10:51:48 a.m.(UTC+8:00) Not After: 2020-07-19 10:51:48 a.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: 41 48 5f fb a2 3d 55 25 50 2f 9a 9a 42 c5 4e 01 0c 34 e7 cf Thumbprint Algorithm: sha2 Thumbprint: dd 9c 54 5d 6b 64 5c 2b fb e1 b6 ec b6 03 76 00 64 64 e9 7b b1 30 4b 79 78 cf e8 3a 40 99 b2 27	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: cf ea 9e 13 53 05 f1 34 7b 7d bf a5 ad 1f e1 06 ce 4f 00 91 Subject Key Identifiers: d5 67 1d e0 9c 7a 2c 9c cb c5 98 e7 1d 07 26 2a 86 ec 74 cd Basic Constraint: Subject Type=CA Path Length Constraint=None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL1_5/CA.crl Certificate Policy: [1]2.16.886.101.0.3.1 [2]2.16.886.101.0.3.2 [3]2.16.886.101.0.3.3 [4]2.16.886.101.0.3.4 [5]2.16.886.101.0.3.0 [6]2.23.140.1.2.2	■ CA certificate of 2nd Generation of GRCA Certification Authority signed by GRCA-G1.5

GCA	Subordinate CA Certificate	
	Subject	Issuer
	OU=政府憑證管理中心 O=行政院 C=TW	O=Government Root Certification Authority C=TW
	Certificate Related Information	Key Related Information
	Serial Number: 00 ff bd e2 d9 bc a9 4a ed 15 26 1c 41 f0 78 7e 55 Signature Algorithm: sha1RSA Not Before:2003-03-03 02:51:23 p.m.(UTC+8:00) Not After: 2023-03-03 02:51:23 p.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: 55 c3 23 9b 77 6c f6 e3 53 e9 7b e8 44 f5 55 93 cb 51 12 bb Thumbprint Algorithm: sha2 Thumbprint: 30 ce 40 96 31 12 0a 0c 5a c5 48 ab fb 23 17 89 a8 47 41 1c 38 18 a5 6e 9b 06 fe b1 72 3c e7 97	Subject Public Key:RSA(2048 bits) Authority Key Identifiers: cc cc ef cc 29 60 a4 3b b1 92 b6 3c fa 32 62 8f ac 25 15 3b Subject Key Identifiers: e4 dc 17 6f 22 aa ce f8 c8 21 1a d2 ab ce 53 8e 4e da 18 7c Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL/CA.crl Certificate Policy: 2.16.886.101.0.3.3	■ CA certificate of 1st Generation of GCA Certification Authority signed by GRCA

GCA – G2	Subordinate CA Certificate	
	Subject	Issuer
	OU=政府憑證管理中心 O=行政院 C=TW	O=Government Root Certification Authority C=TW
	Certificate Related Information	Key Related Information
	Serial Number: 31 ee 58 ef b5 c1 a4 8f 9a ed f4 75 dd b8 a5 c1 Signature Algorithm: sha256RSA Not Before: 2013-01-31 11:22:34 a.m.(UTC+8:00) Not After: 2033-01-31 11:22:34 a.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: 44 b9 ed e7 b3 f9 ed 56 ff 53 b7 e9 1e 40 31 f5 17 e7 8d b8 Thumbprint Algorithm: sha2 Thumbprint: 1f 99 2b 63 59 05 fc 0e ec ed aa bc ea f9 74 1d 77 77 8d d8 38 de 92 b5 bb 51 11 72 2f 46 31 d6	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: d5 67 1d e0 9c 7a 2c 9c cb c5 98 e7 1d 07 26 2a 86 ec 74 cd Subject Key Identifiers: d1 18 67 c3 57 fe 12 9a 91 6b 5f 5f 31 ea 3e c2 84 87 fb bd Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL2/CA.crl Certificate Policy: 2.16.886.101.0.3.3	■ CA certificate of 2nd Generation of GCA Certification Authority signed by GRCA-G2

XCA[2]	Subordinate CA Certificate	
	Subject	Issuer
	OU=組織及團體憑證管理中心 O=行政院 C=TW	O=Government Root Certification Authority C=TW
	Certificate Related Information	Key Related Information
	Serial Number: 56 78 ec df 55 41 78 30 bc 1e dc 8f dd 94 8e ad Signature Algorithm: sha1RSA Not Before: 2004-03-11 03:00:22 p.m.(UTC+8:00) Not After: 2024-03-11 03:00:22 p.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: d6 b8 9a 04 45 95 fd 46 ff 2a da 02 ba c0 1a 0f c9 79 7a 00 Thumbprint Algorithm: sha2 Thumbprint: 52 ef 98 1b a8 5b c0 54 c5 97 f0 9c 6c ac b1 34 b7 df 97 d6 1f ea ee 25 17 f4 db d8 2b f8 ec ca	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: cc cc ef cc 29 60 a4 3b b1 92 b6 3c fa 32 62 8f ac 25 15 3b Subject Key Identifiers: 64 7e 3f e8 07 ef b7 22 e7 02 72 63 1f 28 40 6e 63 e1 cc a6 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL/CA.crl Certificate Policy: 2.16.886.101.0.3.3	■ CA certificate of 1st Generation of XCA Certification Authority signed by GRCA

[2] XCA does not issue SSL certificate and only follow SSL Baseline Requirements and Network Security Principle IV Requirements.

XCA – G2	Subordinate CA Certificate	
	Subject	Issuer
	OU=組織及團體憑證管理中心 O=行政院 C=TW	O=Government Root Certification Authority C= TW
	Certificate Related Information	Key Related Information
	Serial Number: 00 c2 a5 ac 51 04 01 d3 90 f4 26 00 36 5f 8a 86 3c Signature Algorithm: sha256RSA Not Before: 2014-01-02 02:37:36 p.m.(UTC+8:00) Not After: 2034-01-02 02:37:36 p.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: 20 c8 87 e6 50 21 8e 33 43 ac e1 c1 20 81 ef 90 27 fd 34 60 Thumbprint Algorithm: sha2 Thumbprint: b2 ee 26 fd 0b e0 f8 0c c2 47 37 85 cf 9e 98 90 5a 73 63 0e 8d ab f1 2a eb 96 8b b4 d8 1a 2d d6	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: d5 67 1d e0 9c 7a 2c 9c cb c5 98 e7 1d 07 26 2a 86 ec 74 cd Subject Key Identifiers: 5b ee 15 6a 49 17 1c 6a 80 4d e8 5e e7 45 aa ff 80 c7 a0 40 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL2/CA.cr l Certificate Policy: 2.16.886.101.0.3.3	■ CA certificate of 2nd Generation of XCA Certification Authority signed by GRCA-G2