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, 2019 through March 31, 2020 for its CAs as enumerated in Appendix, the NDC has：

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Government Root Certification Authority Certification (GRCA) Practice Statement V1.5; and
  - Government Certification Authority Certification (GCA) Practice Statement V1.9; and
  - miXed Organizations Certification Authority (XCA) Certification Practice Statement V1.8; and
  - Certificate Policy for the Government Public Key Infrastructure (GPKI) V2.0
- Maintained effective controls to provide reasonable assurance that：
  - GRCA, GCA, and XCA Certification Practice Statements are consistent with GPKI Certificate Policy

- GRCA, GCA, and XCA provide their services in accordance with its Certificate Policy and Certification Practice Statements

- 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;
  - subscriber information is properly authenticated for the registration activities performed by GRCA, GCA, and XCA; and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- 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 V2.2.

GRCA, GCA, and XCA do not escrow its CA keys, and does not provide subscriber key generation services. Accordingly, our procedures did not

extend to controls that would address those criteria.

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 WebTrust Principles and Criteria for Certification Authorities V2.2.

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 GRCA, GCA, and XCA's key and certificate life cycle management business 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 life cycle 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.

Inherent limitations

Because of the nature and inherent limitations of controls, GRCA, GCA, and XCA'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, 2019 to March 31, 2020, the NDC management 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.

This report does not include any representation as to the quality of GRCA, GCA, and XCA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities V2.2, nor the suitability of any of GRCA, GCA, and XCA's services for any customer's intended purpose.

Use of the WebTrust seal

GRCA, GCA, and XCA'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.

KPMG

Certified Public Accountants

Taipei, Taiwan, ROC

May 25, 2020

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

<table>
<tr><td rowspan="6">GRCA</td><td colspan="2">Root CA Certificate</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
1f9d595ad72fc20644a5800869e35ef6
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
f48b11bfdeabbe94542071e641de6bbe882b40b9
Thumbprint Algorithm: sha2
Thumbprint
7600295eefe85b9e1fd624db76062aaaae59818a54d2774cd4c0b2c01131e1b3</td><td>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</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td></td><td>■ Self-signed by 1st Generation of GRCA Root Certification Authority
■ Cross Signed with GRCA-G2</td></tr>
</table>

[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 00b64b8807e223eec85c12ada60e06a1f2 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 b091aa913847f313d727bcefc8179f086f3a8c0f Thumbprint Algorithm: sha2 Thumbprint 70b922bfda0e3f4a342e4ee22d579ae598d071cc5ec9c30f123680340388aea5	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

<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
34756f0a697580f7553d9be91cca1ea4
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
2d257912db3da9bbfbad28144722fcf6d7de02cb
Thumbprint Algorithm: sha2
Thumbprint
febf42f9be5abfddb8175d010239f9036fe90d333e708e13cc5eedffd52d0a97</td><td>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)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td>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</td><td>■ CA certificate of 1st Generation of GRCA Certification Authority signed by GRCA-G2</td></tr>
</table>

GRCA (New with Old)	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 325c893b2638910c257764f348d0ada5 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 ceef601f67b133a50875ddc5826b0d22cb41e9e9 Thumbprint Algorithm: sha2 Thumbprint 90fa98d646dd5f00602d68d17dd76b55ee51cda3d3922f0dbdd10480f5990acd	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)
	Additional Information	Remark
	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	■ CA certificate of 2nd Generation of GRCA Certification Authority signed by GRCA

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 33e54ad1c06f18314a9c894e028bccf3 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 83cc399570a3b4e97ea9d962310cb1c686ca929a Thumbprint Algorithm: sha2 Thumbprint a423a33493b31953226df96477627dbd056756704211001b6161fb5f8299dc3a	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 00a3943b6f102651ceba539123749a2a2a 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 41485ffba23d5525502f9a9a42c54e010c34e7cf Thumbprint Algorithm: sha2 Thumbprint dd9c545d6b645c2bfbe1b6ecb60376006464e97bb1304b7978cfe83a4099b227	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

GRCA (New-with-Old SHA1)	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: 00fee626678141435c5faea9f2db4ba66f Signature Algorithm: sha1RSA 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: 361366368816ac3b016f92eeff83ea5fc3dab2f2 Thumbprint Algorithm:sha2 Thumbprint: d87aad615fe7c2385032244d08cdfe06eb005675aa1892d6e5b82780f19fb87f	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/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	■ CA certificate of 2nd Generation of GRCA Certification Authority signed by GRCA

GRCA (New with Old SHA256 with no OV OID)	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: 00b559e7070725ad626294d512e7771554 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: 5c9137b9cfa3901f01693a2be12a964bcb3823f9 Thumbprint Algorithm:sha2 Thumbprint: 72ac428bb715df5dc1af87579308e8cc2ebfa588686b567292fd70eeb0fee8b7	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)
	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	■ CA certificate of 2nd Generation of GRCA Certification Authority signed by GRCA

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 00ffbde2d9bca94aed15261c41f0787e55 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 55c3239b776cf6e353e97be844f55593cb5112bb Thumbprint Algorithm: sha2 Thumbprint 30ce409631120a0c5ac548abfb231789a847411c3818a56e9b06feb1723ce797	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 31ee58efb5c1a48f9aedf475ddb8a5c1 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 44b9ede7b3f9ed56ff53b7e91e4031f517e78db8 Thumbprint Algorithm: sha2 Thumbprint 1f992b635905fc0eecedaabceaf9741d77778dd838de92b5bb5111722f4631d6	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

GCA – G2 (with no OV OID)	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: 088dd2963b8b629c194e3200da77ce2c 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: d234ec3a5a85471c265edaf9811bead817ac9bcc Thumbprint Algorithm:sha2 Thumbprint: 5e9fccb153c7802bab1b5f5015c6643a8bd18ccefcaacedfbad4e21d67c3d5b	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	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 5678ecdf55417830bc1edc8fdd948ead 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 d6b89a044595fd46ff2ada02bac01a0fc9797a00 Thumbprint Algorithm: sha2 Thumbprint 52ef981ba85bc054c597f09c6cacb134b7df97d61feaee2517f4dbd82bf8ecca	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

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 00c2a5ac510401d390f42600365f8a863c 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 20c887e650218e3343ace1c12081ef9027fd3460 Thumbprint Algorithm: sha2 Thumbprint b2ee26fd0be0f80cc2473785cf9e98905a73630e8dabf12aeb968bb4d81a2dd6	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

國家發展委員會
NATIONAL DEVELOPMENT COUNCIL

Assertion of Management as to
its Disclosure of its Business Practices and it Controls Over
its Certification Authority Operations
during the period from April 1, 2019 through March 31, 2020

May 25, 2020

The National Development Council（NDC）operates the Certification Authorities（CAs） services known as Government Root Certification Authority（GRCA）, Government Certification Authority（GCA）, and miXed organization Certification Authority（XCA）. A full listing of the Root CAs and Subordinate CAs owned by NDC[1] and their respective functions is in appendix to this assertion letter. GRCA, GCA, and XCA provide the following CA services：

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

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

- Subordinate CA certification

The management of the NDC is responsible for establishing and maintaining effective controls over its CAs operation, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 GRCA, GCA & XCA's Certification Authorities operation. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

NDC management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in NDC management's opinion, in providing its Certification Authorities (CAs) services at in Taipei and Taichung, Taiwan, throughout the period April 1, 2019 to March 31, 2020, GRCA, GCA, and XCA have:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - GRCA Certification Practice Statement V1.5; and
  - GCA Certification Practice Statement V1.9; and
  - XCA Certification Practice Statement V1.8; and
  - Government Public Key Infrastructure Policy V2.0
- maintained effective controls to provide reasonable assurance that:
  - GRCA, GCA, and XCA's Certification Practice Statements are consistent with GPKI Certificate Policy
  - GRCA, GCA, and XCA provides its services in accordance with Gobernment PKI Certificate Policy and GRCA Certification Practice Statements
- 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;
  - subscriber information is properly authenticated (for the registration activities performed by GRCA, GCA, and XCA); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- Maintained effective controls to provide reasonable assurance that：
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities V2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

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

- Integrated Circuit Card (ICC) Lifecycle Management

Certificate Lifecycle Management Controls

- Subscriber Registration

- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

GRCA, GCA, and XCA does not provide subscriber key generation services. Accordingly, our assertion does not extend to controls that would address those criteria

National Development Council