Report of Independent Certified Public Accountant

To the management of the National Development Council：

We have examined the assertion by the management of the National Development Council (NDC) that in providing its Government Root Certification Authority (GRCA) services in Taipei, Taiwan and Taichung, Taiwan during the period from April 1, 2016 through March 31, 2017, the NDC has：

- Disclosed its key and certificate life cycle management business and information privacy practices in its Certification Practice Statement on the GRCA website and provided such services in accordance with its disclosed Certificate Policy and Certification Practice Statement;
- Maintained effective controls to provide reasonable assurance that：
  - Subscriber information was properly authenticated for the registration activities performed by the GRCA; and
  - The integrity of key and certificate it managed was established and protected throughout their life cycles.
- Maintained effective controls to provide reasonable assurance that：

- Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA business practices disclosure;
- The continuity of key and certificate life cycle management operations was maintained; and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the Trust Service Principles and Criteria for Certification Authorities V2.0.

The management of the NDC is responsible for its assertion. Our responsibility is to express an opinion on management assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, and accordingly, included (1) obtaining an understanding of GRCA's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity; over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance and operation of systems integrity; (2) selectively testing transactions executed in accordance with the disclosed key and certificate life cycle management business and information privacy 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 our examination provides a reasonable basis for our opinion.

In our opinion, for the period from April 1, 2016 through March 31, 2017, the NDC management assertion, as set forth above, is fairly stated, in all material respects, based on the Trust Service Principles and Criteria for Certification Authorities V2.0.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls; (2) changes in processing requirements; (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust seal of assurance for certification authorities on GRCA's Website 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.

The relative effectiveness and significance of specific controls at the GRCA 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.

This report does not include any representation as to the quality of the GRCA services beyond those covered by the Trust Service Principles and Criteria for Certification Authorities V2.0, nor the suitability of any of the GRCA services for any customer's intended purpose. This report does not include the system development and test conducted by outsourcing subcontractor, either.

KPMG

KPMG

Certified Public Accountants

68F, TAIPEI 101 TOWER, No.7, Sec. 5, Xinyi Road,
Taipei 11049, Taiwan (R.O.C.)

24 May, 2017

Appendix

	Root CA Certificate	
GRCA	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	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

<table>
<tr><td rowspan="6">GRCA - G2</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: 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</td><td>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)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td></td><td>■ Self-signed by 2nd Generation of GRCA Root Certification Authority
■ Cross Signed with GRCA</td></tr>
</table>

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	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

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: 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	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

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, 2016 through March 31, 2017

May 24, 2017

The National Development Council（NDC）provides the following certification authority（CA） services through the Government Root Certification Authority（GRCA）:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

The management of the NDC is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in its Certification Practice Statement on the

GRCA website, service integrity （including key and certificate life cycle management controls）, and CA environmental 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 provide only reasonable assurance with respect to GRCA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of the NDC has assessed the controls over the GRCA operations. Based on that assessment, in management opinion, in providing GRCA services in Taipei, Taiwan and Taichung, Taiwan during the period from April 1, 2016 through March 31, 2017, the NDC has：

- Disclosed its key and certificate life cycle management business and information privacy practices in its Certification Practice Statement on the website of the GRCA and provided such services in accordance with its disclosed practices;
- Maintained effective controls to provide reasonable assurance that：
  - Subscriber information was properly authenticated for the registration activities performed by the GRCA; and
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles.

- Maintained effective controls to provide reasonable assurance that：
  - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA business practices disclosure;
  - The continuity of key and certificate life cycle management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

Gour-Tsair Pan

National Development Council

Appendix

<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: 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</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>

<table>
<tr><td rowspan="7">GRCA - G2</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: 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</td><td>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)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td></td><td>■ Self-signed by 2nd Generation of GRCA Root Certification Authority
■ Cross Signed with GRCA</td></tr>
</table>

<table>
<tr><td rowspan="6">GRCA
(Old with New)</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: 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</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>

<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</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>