KPMG

Report of Independent Certified Public Accountant

To the management of the National Development Council :

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

- Disclosed its Certificate Policy, Certification Practice Statement and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
  - The Certificate Policy and/or Certification Practice Statement are available on a 24x7 basis and updated annually;
  - Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of key and certificate it manages was established and protected throughout their life cycles;
  - Logical and physical access to CA systems and data was restricted to authorized individuals;

- The continuity of key and certificate management operations was maintained; and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

for GCA and Government Root Certification Authority (GRCA), based on the WebTrust for Certification Authorities – SSL Baseline with Network Security Version 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, and accordingly, included (1) obtaining an understanding of GCA key and SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and certificate life cycle management operations, and over the development, maintenance, and operation of systems integrity; (2) selectively testing transactions executed in accordance with 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's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the WebTrust for Certification Authorities – SSL Baseline with Network Security Version 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 relative effectiveness and significance of specific controls at the 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.

This report does not include any representation as to the quality of the GCA services beyond those covered by the WebTrust for Certification Authorities - SSL Baseline with Network Security Version V2.0., or the suitability of any of GCA services for any customer's intended purpose.

KPMG

Certified Public Accountants

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

24 May, 2017

Appendix

	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
GCA	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	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	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

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) has assessed the disclosure of its certificate practice and its controls over its following SSL certification services through the Government Certification Authority (GCA) :

- Disclosed its Certificate practices and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
  - ✓ The Certificate Policy and/or Certificate Practice Statement are available on a 24x7 basis and updated annually;
  - ✓ Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;

- ✓ The integrity of keys and certificates it manages was established and protected throughout their life cycles;
- ✓ Logical and physical access to CA systems and data was restricted to authorized individuals;
- ✓ The continuity of key and certificate management operations was maintained; and
- ✓ CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the AICPA/CPA WebTrust for Certification Authorities - SSL Baseline with Network Security version 2.0.

National Development Council 國家發展委員會

Gour-Tsair Pan

National Development Council

Appendix

<table>
<tr><td rowspan="6">GCA</td><td colspan="2">Subordinate CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>OU=政府憑證管理中心
O=行政院
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 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</td><td>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)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td>CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL/CA.crl
Certificate Policy: 2.16.886.101.0.3.3</td><td>■ CA certificate of 1st Generation of GCA Certification Authority signed by GRCA</td></tr>
</table>

<table>
<tr><td rowspan="6">GCA – G2</td><td colspan="2">Subordinate CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>OU=政府憑證管理中心
O=行政院
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: 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</td><td>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)</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: 2.16.886.101.0.3.3</td><td>■ CA certificate of 2nd Generation of GCA Certification Authority signed by GRCA-G2</td></tr>
</table>