KPMG

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 Mixed Organization Certification Authority (XCA) services in Taipei, Taiwan and Tai Chung, 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 XCA 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 XCA; 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 XCA'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 relative effectiveness and significance of specific controls at the XCA 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 XCA services beyond those covered by the Trust Service Principles and Criteria for Certification Authorities V2.0, nor the suitability of any of the XCA services for any customer's intended purpose.

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

	Subordinate CA Certificate	
	Subject	Issuer
XCA	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	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: 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	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