Ernst & Young Han Young
Taeyoung Building, 111, Yeouigongwon-ro,
Yeongdeungpo-gu, Seoul 150-777 Korea

Tel: +82 2 3787 6600
Fax: +82 2 783 5890
ey.com/kr

Report of the Independent Accountant

To the Management of Korea Electronic Certification Authority, Inc. (”CrossCert”):

We have examined the CrossCert management’s assertion that for its Certification Authority (“CA”) operations at Republic of Korea, throughout the period July 01, 2015 to June 30 2016 for its SSL CAs known as Secure Site and Secure Site Pro as subordinate CA of Symantec Corporation listed in Appendix A in scope for SSL Baseline Requirements and Network Security Requirements, CrossCert has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - CrossCert Certificate Practice Statement Version 3.8.8,

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the CrossCert website, 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 CrossCert)
- 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

based on the WebTrust for Certification Authorities – WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security – Version 2.0.

CrossCert’s management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

We conducted our examination in accordance with attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of CrossCert’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 CrossCert’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 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 our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at CrossCert 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.

Because of the nature and inherent limitations of controls, CrossCert'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.

In our opinion, throughout the period July 01, 2015 to June 30, 2016, CrossCert management's assertion, as referred to above, is fairly stated, in all material respects, based on the WebTrust for Certification Authorities – WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security – Version 2.0.

This report does not include any representation as to the quality of CrossCert's services beyond those covered by the WebTrust for Certification Authorities – WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security – Version 2.0, nor the suitability of any of CrossCert's services for any customer's intended purpose.

CrossCert'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.

Ernst & Young Han Young

Seoul, Republic of Korea
November 21, 2016

Appendix A – Symantec SSL CAs that accounts for CrossCert SSL CA Services:

Symantec Root CAs:	Symantec SSL Issuing CAs:
• VeriSign Class 3 Public Primary Certification Authority • VeriSign Class 3 Public Primary Certification Authority - G5	• VeriSign Class 3 Secure Server CA - G3 • VeriSign Class 3 International Server CA - G3 • Symantec Class 3 Secure Server CA - G4

7th Fl. Halim, 320 Seocho-daero
Seoul 137-725, Korea

The Intelligent Company
CROSSCERT
Founded 1999

Assertion of Management as to its Disclosure of its Certificate Practices and its Controls Over its SSL Certification Authority Services throughout the Period July 01, 2015 to June 30, 2016

November 21, 2016

Korea Electronic Certification Authority, Inc. ("CrossCert") operates the Certification Authority ("CA") services known as SSL CAs listed in Appendix A in scope for SSL Baseline Requirements and Network Security Requirements and provides SSL CA services namely Secure Site and Secure Site Pro, as a subordinate CA of Symantec Corporation.

The management of CrossCert is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL 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 CrossCert's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

CrossCert management has assessed the disclosure of its certificate practices and its controls over its SSL – Certification Authority ("CA") services known as Secure Site and Secure Site Pro, as a subordinate CA of Symantec Corporation. Based on that assessment, in CrossCert Management's opinion, in providing its SSL - CA services at Republic of Korea, throughout the period July 01, 2015 to June 30, 2016, CrossCert has:

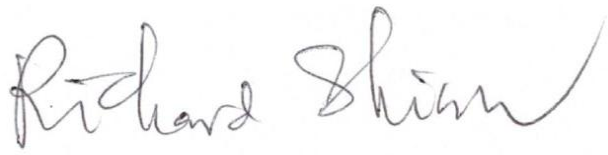
- disclosed its SSL certificate lifecycle management business practices in its:
    - CrossCert Certificate Practice Statement Version 3.8.8,

  Including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the CrossCert website, 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 CrossCert)

- 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

for its Secure Site and Secure Site Pro, based on the WebTrust for Certification Authorities – WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security – Version 2.0.



Richard H. Shinn
CEO
CrossCert

Appendix A – Symantec SSL CAs that accounts for CrossCert SSL CA Services:

Symantec Root CAs:	**Symantec SSL Issuing CAs:**
• VeriSign Class 3 Public Primary Certification Authority • VeriSign Class 3 Public Primary Certification Authority - G5	• VeriSign Class 3 Secure Server CA - G3 • VeriSign Class 3 International Server CA - G3 • Symantec Class 3 Secure Server CA - G4