



## Report of the Independent Accountant

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

We have examined the assertions by the management of CrossCert, a subordinate Certification Authority of DigiCert, Inc. ("DigiCert"), that for its Certification Authority (CA) operations at Seoul, Republic of Korea; Suwon, Republic of Korea, throughout the period July 1, 2019 to June 30, 2020 for its CA services listed in Appendix A, CrossCert has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its CrossCert Certification Practices Statement and DigiCert Certificate Policy enumerated in Appendix B
- maintained effective controls to provide reasonable assurance that:
  - CrossCert's Certification Practice Statement is consistent with its Certificate Policy
  - CrossCert provides its services in accordance with its Certificate Policy and Certification Practice Statement
- 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 CrossCert); 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

based on the WebTrust Principles and Criteria for Certification Authorities, Version 2.2.

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

CrossCert does not escrow its CA keys, does not provide subscriber key lifecycle management services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and



Tel: +82 2 2112 0001  
Fax: +82 2 2112 0501  
<http://www.kpmg.com/kr>

Gangnam Finance Center, 152,  
Teheran-ro, Gangnam-gu,  
Seoul, Republic of Korea

perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- (1) obtaining an understanding of CrossCert's key and certificate lifecycle management business practices, policies, processes and controls, and its suitability of design and implementation of controls intended to achieve the Criteria and examining evidence supporting management's assertion and performing such other procedures 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 the development, maintenance and operation of systems integrity as we considered necessary in the circumstances;
- (2) selectively testing transactions executed in accordance with disclosed key and 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.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. 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 1, 2019 to June 30, 2020, CrossCert management's assertion, as referred above, is fairly stated, in all material respects, based on the WebTrust Principles and Criteria for Certification Authorities, Version 2.2.

This report does not include any representation as to the quality of CrossCert's services other than its Symantec CA operations at Seoul, Republic of Korea; Suwon, Republic of Korea, nor the suitability of any of CrossCert's services for any customer's intended purpose.

Crosscert'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.

Minsoo Kim, Partner  
Seoul, Republic of Korea  
September 25, 2020



Tel: +82 2 2112 0001  
 Fax: +82 2 2112 0501  
<http://www.kpmg.com/kr>

Gangnam Finance Center, 152,  
 Teheran-ro, Gangnam-gu,  
 Seoul, Republic of Korea

## Appendix A – List of CAs In-Scope

CA #	Cert #	Subject DN	Not Before	Not After	SHA 256 Fingerprint
1	1	CN = CrossCert Class 1 Consumer Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR	Tuesday, June 18, 2019, 12:00:00 AM GMT	Friday, March 31, 2023, 11:59:59 PM GMT	D4F4357C103B034382C5A0DBF454A9C72799A28CAB32CFCC28F80AA5C7B142A4
1	2	CN = CrossCert Class 1 Consumer Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR  (Expired on June 3, 2020)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	2D4C890F3DB517A2444A79E27BCF205941904D5AA510F8783BC6DB1AD368348
1	3	CN = CrossCert Class 1 Consumer Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR  (Revoked on May 8, 2019)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	32CEC48814C4427415FA5941DB175187E1B524D6B29A4CDFDE6D506B61C73966
2	1	CN = CrossCert Class 2 Managed PKI Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR	Tuesday, June 18, 2019, 12:00:00 AM GMT	Friday, March 31, 2023, 11:59:59 PM GMT	7AD6072874552470F8C3B78F75CD7E0A04E2A17BDA057B2C5E992FCE3C5BAB9C
2	2	CN = CrossCert Class 2 Managed PKI Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	CC59458524AD1B29F8705304006D89DF1FED617F029F0D3BD3F94DA21E96D6DA



Tel: +82 2 2112 0001  
 Fax: +82 2 2112 0501  
<http://www.kpmg.com/kr>

Gangnam Finance Center, 152,  
 Teheran-ro, Gangnam-gu,  
 Seoul, Republic of Korea

CA #	Cert #	Subject DN	Not Before	Not After	SHA 256 Fingerprint
2	3	CN = CrossCert Class 2 Managed PKI Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR  (Revoked on June 29, 2018)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	DE2A4A0C049E358BF2BFBA5A38AD7FAA55534221A021F9894474C146CB270922
3	1	CN = POSCO Online CA - G3 OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = POSCO C = KR	Thursday, June 4, 2015, 12:00:00 AM GMT	Monday, June 2, 2025, 11:59:59 PM GMT	A38872203A3FD6C62C674AD8EF2DB3BE48A74235354A66FB7F5FE3C615C38E7D
3	2	CN = POSCO Online CA - G3 OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = POSCO C = KR	Thursday, June 4, 2015, 12:00:00 AM GMT	Monday, June 2, 2025, 11:59:59 PM GMT	D629D188A2DA095E6FFF06A81BAADC25E0F6AC59BAE7413E20457609FE979B81
3	3	CN = POSCO Online CA - G3 OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = POSCO C = KR  (Revoked on May 8, 2019)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	6BA501267D83C0D78452F8F7AD9F80E6BE88572FC72BB165DF8C671E8AD9939D



Tel: +82 2 2112 0001  
Fax: +82 2 2112 0501  
<http://www.kpmg.com/kr>

Gangnam Finance Center, 152,  
Teheran-ro, Gangnam-gu,  
Seoul, Republic of Korea

CA #	Cert #	Subject DN	Not Before	Not After	SHA 256 Fingerprint
3	4	CN = POSCOPNS Online CA - G2 OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = POSCOPNS C = KR  (Revoked on April 13, 2018)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	BCB3DDDFE082D24C5EACBF2D29DE9E1E5F16C0A4BB53B6C723E033A2C00A453A
3	5	CN = POSCOPNS Online CA OU = Class 2 Managed PKI Individual Subscriber CA OU = Terms of use at <a href="https://www.crosscert.com/rpa">https://www.crosscert.com/rpa</a> (c)11 OU = VeriSign Trust Network O = POSCOPNS C = KR  (Revoked on June 29, 2018)	Thursday, January 15, 2015, 12:00:00 AM GMT	Tuesday, January 14, 2020, 11:59:59 PM GMT	1FA3BD5ABE51DD8BC67B3E493454D40D2C63A698F150810914BF0863644D63D1



Tel: +82 2 2112 0001  
Fax: +82 2 2112 0501  
<http://www.kpmg.com/kr>

Gangnam Finance Center, 152,  
Teheran-ro, Gangnam-gu,  
Seoul, Republic of Korea

**Appendix B – Certification Practice Statement and Certificate Policy Versions In-Scope**

Policy Name	Version	Date
<a href="#">CrossCert Certification Practices Statement</a>	5.0	March 30, 2020
<a href="#">CrossCert Certification Practices Statement</a>	3.11.1	June 30, 2019
<a href="#">DigiCert Certificate Policy</a>	5.2	May 22, 2020
<a href="#">DigiCert Certificate Policy</a>	5.1	March 27, 2020
<a href="#">DigiCert Certificate Policy</a>	5.0	February 6, 2020
<a href="#">Certificate Policy for Symantec Trust Network (STN)</a>	2.12	June 25, 2019

Notes: The CP are defined by the DigiCert, and CrossCert adheres to it as subordinate CA, under the DigiCert Roots



Assertion of Management as to  
its Disclosure of its Business Practices and its Controls Over  
its Certification Authority Operations  
throughout the period July 1, 2019 to June 30, 2020

September 25, 2020

Korea Electronic Certification Authority, Inc. ("CrossCert") operates the Symantec Certification Authority (CA) services as a subordinate CA of DigiCert, Inc ("DigiCert") for its CAs as enumerated in Appendix A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA certification

The management of CrossCert is responsible for establishing and maintaining effective controls over its CA operations, in its [repository](#), 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 CrossCert's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

CrossCert management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CrossCert management's opinion, in providing its Certification Authority (CA) services at Republic of Korea, CrossCert CA, throughout the period July 1, 2018 to June 30, 2019, CrossCert has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its CrossCert Certification Practices Statement and DigiCert Certificate Policy enumerated in Appendix B
- maintained effective controls to provide reasonable assurance that:
  - CrossCert's Certification Practice Statement is consistent with its Certificate Policy
  - CrossCert provides its services in accordance with its Certificate Policy and Certification Practice Statement
- 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 CrossCert); 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

based on the [WebTrust Principles and Criteria for Certification Authorities, Version 2.2.](#), including the following:

#### **CA Business Practices Disclosure**

- Certification Practice Statement (CPS)

#### **CA Business Practices Management**

- Certification Practice Statement Management
- CP and CPS Consistency

#### **CA Environmental Controls**

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and 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
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Escrow (not applicable – service not provided by CrossCert)
- CA Key Transportation
- CA Key Migration

#### **Subscriber Key Lifecycle Management Controls**

- CA-Provided Subscriber Key Generation Services (not applicable – service not provided by CrossCert)
- CA-Provided Subscriber Key Storage and Recovery Services (not applicable – service not provided by CrossCert)
- Integrated Circuit Card (ICC) Lifecycle Management (not applicable – service not provided by CrossCert)
- Requirements for Subscriber Key Management (not applicable – service not provided by CrossCert)





### **Certificate Lifecycle Management Controls**

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension (not applicable – service not provided by CrossCert)
- Certificate Validation

### **Subordinate CA Certificate Lifecycle Management Controls**

- Subordinate CA Certificate Lifecycle Management

CrossCert does not escrow its CA keys, does not provide subscriber key lifecycle management services to subscribers, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

David Ahn  
Vice President  
CrossCert

A handwritten signature in black ink, appearing to read "DAHN".



**Appendix A – List of CAs In-Scope**

CA #	Cert #	Subject DN	Not Before	Not After	SHA 256 Fingerprint
1	1	CN = CrossCert Class 1 Consumer Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR	Tuesday, June 18, 2019, 12:00:00 AM GMT	Friday, March 31, 2023, 11:59:59 PM GMT	D4F4357C103B034382C5A0DBF454A9C72799A28CAB32CFCC28F80AA5C7B142A4
1	2	CN = CrossCert Class 1 Consumer Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR  (Expired on June 3, 2020)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	2D4C890F3DB517A24444A79E27BCF205941904D5AA510F8783BC6DB1AD368348
1	3	CN = CrossCert Class 1 Consumer Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR  (Revoked on May 8, 2019)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	32CEC48814C4427415FA5941DB175187E1B524D6B29A4CDFDE6D506B61C73966
2	1	CN = CrossCert Class 2 Managed PKI Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR	Tuesday, June 18, 2019, 12:00:00 AM GMT	Friday, March 31, 2023, 11:59:59 PM GMT	7AD6072874552470F8C3B78F75CD7E0A04E2A17BDA057B2C5E992FCE3C5BAB9C



CA #	Cert #	Subject DN	Not Before	Not After	SHA 256 Fingerprint
2	2	CN = CrossCert Class 2 Managed PKI Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	CC59458524AD1B29F8705304006D89DF1FED617F029F0D3BD3F94DA21E96D6DA
2	3	CN = CrossCert Class 2 Managed PKI Individual Subscriber CA - G3 OU = Symantec Trust Network O = "KECA, Inc." C = KR  (Revoked on June 29, 2018)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	DE2A4A0C049E358BF2BFBA5A38AD7FAA55534221A021F9894474C146CB270922
3	1	CN = POSCO Online CA - G3 OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = POSCO C = KR	Thursday, June 4, 2015, 12:00:00 AM GMT	Monday, June 2, 2025, 11:59:59 PM GMT	A38872203A3FD6C62C674AD8EF2DB3BE48A74235354A66FB7F5FE3C615C38E7D
3	2	CN = POSCO Online CA - G3 OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = POSCO C = KR	Thursday, June 4, 2015, 12:00:00 AM GMT	Monday, June 2, 2025, 11:59:59 PM GMT	D629D188A2DA095E6FFF06A81BAADC25E0F6AC59BAE7413E20457609FE979B81



CA #	Cert #	Subject DN	Not Before	Not After	SHA 256 Fingerprint
3	3	CN = POSCO Online CA - G3 OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = POSCO C = KR  (Revoked on May 8, 2019)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	6BA501267D83C0D78452F8F7AD9F80E6BE88572FC72BB165DF8C671E8AD9939D
3	4	CN = POSCOPNS Online CA - G2 OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = POSCOPNS C = KR  (Revoked on April 13, 2018)	Thursday, June 4, 2015, 12:00:00 AM GMT	Wednesday, June 3, 2020, 11:59:59 PM GMT	BCB3DDDFE082D24C5EACBF2D29DE9E1E5F16C0A4BB53B6C723E033A2C00A453A
3	5	CN = POSCOPNS Online CA OU = Class 2 Managed PKI Individual Subscriber CA OU = Terms of use at <a href="https://www.crosscert.com/rpa">https://www.crosscert.com/rpa</a> (c)11 OU = VeriSign Trust Network O = POSCOPNS C = KR  (Revoked on June 29, 2018)	Thursday, January 15, 2015, 12:00:00 AM GMT	Tuesday, January 14, 2020, 11:59:59 PM GMT	1FA3BD5ABE51DD8BC67B3E493454D40D2C63A698F150810914BF0863644D63D1



**Appendix B – Certification Practice Statement and Certificate Policy Versions In-Scope**

Policy Name	Version	Date
<a href="#">CrossCert Certification Practices Statement</a>	5.0	March 30, 2020
<a href="#">CrossCert Certification Practices Statement</a>	3.11.1	June 30, 2019
<a href="#">DigiCert Certificate Policy</a>	5.2	May 22, 2020
<a href="#">DigiCert Certificate Policy</a>	5.1	March 27, 2020
<a href="#">DigiCert Certificate Policy</a>	5.0	February 6, 2020
<a href="#">Certificate Policy for Symantec Trust Network (STN)</a>	2.12	June 25, 2019

Notes: The CP are defined by the DigiCert, and CrossCert adheres to it as subordinate CA, under the DigiCert Roots