



Ministry of the Interior

Assertion by Management of Ministry of the Interior (“MOI”) Regarding its Disclosure of its Business Practices and its Controls over its Certification Authority Operations

during the period from December 1, 2015 through November 30, 2016

Ministry of the Interior (“MOI”) as a Certification Authority (CA) Known as MOI, as a Root CA, provides the following certification authority services;

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

MOI operations have been outsourced to Korea Local Information Research & Development Institute (“KLID”) for operating and maintaining the systems and services of MOI. MOI with KLID as its agent is responsible for the management assertion of the MOI operations.

MOI with KLID as its agent is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure at <https://www.gpki.go.kr/pds/WebTrustAction.action>, service integrity (including key and certificate life cycle management), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, 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 MOI’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

MOI with KLID as its agent has assessed the controls over its CA operations. Based on that assessment, in MOI Management’s opinion, in providing its Certification Authority services at <https://www.gpki.go.kr/>, during the period December 1, 2015 through November 30, 2016

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its
 - certification Practice Statement
- maintained effective controls to provide reasonable assurance that
 - MOI provides its services in accordance with its Certification Practice Statement
- maintained effective controls to provide reasonable assurance that
 - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
 - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
 - the Subscriber information was properly authenticated and
 - subordinate CA certificate requests were accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that
 - 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 the MOI, in accordance with the [WebTrust for Certification Authorities](#) (Version 2.0, 1 July 2011) including following;

CA Business Practice Disclosure

Certification Practice Statement

CA Business Practice Management

Certification Practice Statement Management

Service Integrity

CA Key Life Cycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Life Cycle Management Controls

Subordinate CA Certificate Life Cycle Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operation Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

Ministry of the Interior,

26th January, 2017





행정자치부

문서는 2015년 12월 1일부터 2016년 11월 30일까지 인증기관(CA)의 사업 운영 및 통제의 공개에 대한 행정자치부 인증기관 확인서임.

최상위 인증기관(Root CA)으로써 행정자치부는 다음의 인증서비스를 제공합니다.

- 인증서 등록
- 인증서 갱신
- 인증서 키 교체
- 인증서 발급
- 인증서 배포
- 인증서 폐기
- 인증서 유효성 검사

행정자치부는 한국지역정보개발원에 인증 시스템 및 서비스에 대한 운영 및 유지보수를 위탁하고 있습니다. 행정자치부와 위탁기관인 한국지역정보개발원은 본 인증기관 확인서에 대한 책임을 가지고 있습니다.

행정자치부와 위탁기관인 한국지역정보개발원은 공인인증업무준칙 (<https://www.gpki.go.kr/pds/WebTrustAction.action>), 서비스 무결성 (라이선스 키 및 인증서 수명주기 관리 포함) 및 CA 환경 통제를 포함한 CA 운영에 대한 책임을 가지고 있습니다. 이러한 통제들은 모니터링체계와 발견된 결함을 해결하기 위한 조치사항을 포함합니다.

통제는 인적 오류의 가능성 및 통제의 우회, 무시를 포함한 본질적인 한계를 가지고 있습니다. 따라서 효과적인 통제라 할지라도 행정자치부의 CA 운영업무에 대해서만 합리적인 확신을 제공할 수 있으며, 환경의 변화로 인해, 통제의 효과가 시간이 지남에 따라 변할 수 있습니다.

행정자치부와 위탁기관인 한국지역정보개발원은 CA 운영에 대한 통제를 평가하였으며, 이러한 평가에 근거하고, 행정자치부의 의견에 기초하여 2015년 12월 1일부터 2016년 11월 30일까지 <http://www.gpki.go.kr> 에서 제공된 CA 서비스,

- 인증 사업, 키 수명주기 관리, 인증서 수명주기 관리 및 CA 환경통제를 아래에 공개함
 - 인증 업무 준칙
- 아래에 대해 합리적 확신을 제공하는 효과적인 통제를 유지함
 - 행정자치부가 인증 업무 준칙에 따라 서비스를 제공
- 아래에 대해 합리적 확신을 제공하는 효과적인 통제를 유지함
 - 수명주기 전반에 걸쳐 키 및 인증서의 무결성 관리가 수립되고 보호
 - 수명주기 전반에 걸쳐 가입자 키 및 인증서 무결성 관리가 수립되고 보호
 - 가입자 정보가 적절히 증명

- 하위 CA 인증서 요청이 정확하고, 증명되고 승인
- 다음에 대해 합리적 확신을 제공하는 효과적인 통제를 유지함
 - CA 시스템과 데이터에 대한 논리적, 물리적 접근을 권한 있는 자로 제한
 - 키 및 인증서 관리 작업의 연속성 유지
 - CA 시스템 무결성 유지를 위한 CA시스템 개발, 유지보수 및 운영이 적절한 승인받고 수행

행정자치부는 아래의 활동을 포함하며 WebTrust for Certification Authorities (2011년 7월 1일 버전)에 부합하도록 서비스를 제공합니다.

CA 비즈니스 활동 공개

인증업무 준칙

CA 비즈니스 활동 관리

인증업무 준칙 관리

서비스의 무결성

CA 키 수명주기 관리 통제

- CA 키 생성
- CA 키 저장, 백업 및 복구
- CA 공개 키 분배
- CA 키 사용
- CA 키 보관 및 파기
- CA 키 손상
- CA 암호화 하드웨어 수명주기 관리

인증서 수명주기 관리 통제

- 인증서 등록
- 인증서 갱신
- 인증서 키 교체
- 인증서 발급
- 인증서 배포
- 인증서 해지
- 인증서 유효성 검사

CA 환경 통제

- 보안 관리
- 자산 분류 및 관리
- 인적 보안
- 물리적 및 환경적 보안
- 운영 관리
- 시스템 접근 관리
- 시스템 개발 및 유지보수
- 사업 연속성 관리
- 모니터링 및 규제 준수
- 감사 기록

행정자치부

2017년 1월 26일 

Independent Practitioner Report

To the Management of Ministry of the Interior (“MOI”);

We have examined the assertion by the Management of Ministry of the Interior (“MOI”), with Korea Local Information Research & Development Institute (“KLID”) as an agent of MOI, that in providing its Certification Authority (“CA”) services, as a Root CA (GPKIRootCA1), at Seoul, Korea, during the period December 1, 2015 through November 30, 2016, MOI has

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its
 - Certification Practice Statement
- maintained effective controls to provide reasonable assurance that
 - MOI provides its services in accordance with its Certification Practice Statement
- maintained effective controls to provide reasonable assurance that
 - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
 - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
 - the Subscriber information was properly authenticated and
 - subordinate CA certificate requests were accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that
 - 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

based on the [Webtrust Principle and Criteria for Certification Authorities version 2.0](#)

MOI with KLID as its agent is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

Our examination was conducted included (1) obtaining an understanding of MOI’s key and certificate life cycle management business practice and its controls over key and 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 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 MOI 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, MOI'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 period is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, for the period December 1, 2015 through November 30, 2016, MOI management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on [Webtrust Principle and Criteria for Certification Authorities version 2.0](#).

This report does not include any representation as to the quality of MOI's services beyond those covered by the [Webtrust Principle and Criteria for Certification Authorities version 2.0](#), nor the suitability of any of MOI's services for any customer's intended purpose.

Deloitte Anjin LLC

Deloitte Anjin LLC.
January 26, 2017