



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 SSL Certification Authority Operations

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

Ministry of the Interior as a Certification Authority (CA) Known as MOI provides SSL Certification Authority services through Root Certification Authority (GPKIRootCA1) and two subordinate CAs (CA131100001 for Government Administration and CA131100002 for Government Finance);

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.

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 SSL 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-SSL operations. Based on that assessment, in MOI Management’s opinion, in providing its SSL Certification Authority services at <https://www.gpki.go.kr/> , during the period December 1, 2015 through November 30, 2016

- 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.
 - CA’s network and certification systems security were properly managed.

in accordance with the [WebTrust for Certification Authorities – SSL Baseline Requirements with Network Security](#)(version 2.0);

Ministry of the Interior,

26th January, 2017



행정자치부

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

행정자치부는 최상위 인증기관(GPKIRootCA1)과 행정(CA131100001)/공공(CA131100002) CA를 통해 웹서비스 인증서(SSL) 서비스를 제공하고 있습니다.

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

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

행정자치부와 위탁기관인 한국지역정보개발원은 웹서비스 인증서(SSL) 운영에 대한 통제를 평가하였습니다. 이러한 평가결과에 근거하고, 행정자치부의 의견에 기초하여 2015년 12월 1일부터 2016년 11월 30일까지 <http://www.gpki.go.kr> 에서 제공된 웹서비스 인증서(SSL) 서비스는,

- 적용 가능한 CA/Browser 포럼 가이드라인에 부합되는 보안서버(SSL) 인증서를 제공하기 위한 인증업무 준칙 공개
- 아래에 대해 합리적 확신을 제공하는 효과적인 통제를 유지함
 - 인증서 정책과 인증업무준칙은 24x7 기반으로 이용 가능하며 매년 갱신
 - 가입자 정보는 적절히 수집되고 확인되며 유효성이 검증 (인증기관, 등록기관 및 하위 계약자에 의해 수행되는 등록 활동 관련)
 - 수명주기 전반에 걸쳐 키 및 인증서의 무결성 관리가 수립되고 보호
 - CA 시스템과 데이터에 대한 논리적, 물리적 접근을 권한 있는 자로 제한
 - 키 및 인증서 관리 작업에 대한 연속성 유지
 - CA 시스템 무결성 유지를 위한 CA시스템 개발, 유지보수 및 운영이 적절한 승인받고 수행
 - CA 네트워크와 인증시스템 보안은 적절히 관리.

행정자치부는 WebTrust for Certification Authorities - SSL Baseline Requirements with Network Security (버전 2.0)에 부합하도록 서비스를 제공합니다.

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 SSL Certification Authority (“CA”) services through Root Certification Authority (GPKIRootCA1) and two subordinate CAs (CA131100001 for Government Administration and CA131100002 for Government Finance) at Seoul, Korea, during the period December 1, 2015 through November 30, 2016, MOI has

- 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.
 - CA's network and certification systems security were properly managed.

based on the [WebTrust Principle and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security 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 SSL certificate life cycle management business practice 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 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 the [WebTrust Principle and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security 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 – SSL Baseline Requirements with Network Security 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