The Readiness Assessment Report based on "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security"

September 30, 2015

Administrative Management Bureau,
Ministry of Internal Affairs and Communications

The Application CA 2(“APCA2”) and a Local Registration Authority (“LRA”) of the Governmental Public Key Infrastructure (“GPKI”) had the Readiness Assessment based on “WebTrust Principles and Criteria for Certification Authorituies – SSL Baseline with Network Security” by KPMG AZSA LLC.

Please refer to the following.

1 Purpose

This assessment is to report the result of assessment for any gaps on design and implementation of requirements by comparing "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security" with rules of the Certificate Policy (CP) and Certification Practice Statement (CPS) ,etc. and other related documents of the Application CA 2("APCA2") and a Local Registration Authority ("LRA") of the Governmental Public Key Infrastructure ("GPKI") as of September 16, 2015.

This assessment report described the gaps found at this assessment.

2 Overview of this assessment

2.1 Criteria

The criteria used at this assessment is "CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0" ("this criteria").

Principles of this criteria are as follows:

PRINCIPLE 1	Baseline Requirements Business Practices Disclosure
PRINCIPLE 2	Service Integrity
PRINCIPLE 3	CA Environmental Security
PRINCIPLE 4	Network and Certificate Systems Security

2.2 Scope

The scope of this assessment is below:

CA	APCA2 (Root) APCA2 (Sub)
Ministry LRA	LRA of the Ministry of Internal Affairs and Communications

2.3 Procedures

At this assessment, in order to assess how meet the requirements described in this criteria for the above CAs and LRA, our procedures include reading related rules, inspecting one sample of evidence for each requirement, interviewing their personnel and observing related facilities. The findings at this assessment are described in section 3.

3 Results

Refer to the attachment

Attachment: Findings Description

No.	Baseline Requirements		Findings
	Ref.	Criteria	
1	1.1 1.4	The CA discloses on its website its: (snip) its commitment to conform to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum. The Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describes how the CA implements the latest version of the Baseline Requirements are updated annually.	According to WTBR, the CA shall develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. The CP/CPS provide the Application CA2 complies with guidelines of the latest version of the"AICPA/CICA WebTrust Program for Certification Authorities " and "CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ", and that these guidelines have a priority to the CP/CPS if there is any inconsistency between these guidelines' requirements and the CP/CPS. However, there are several inconsistencies not complying with WTBR. These inconsistencies are as described below. Therefore, the CAs and LRA shall operate in accordance with all WTBR requirements.
2	2.3.4	Subscriber Agreement and Terms of Use The CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the SSL Baseline Requirements Section 10.3.1. That agreement contains provisions imposing obligations and warranties on the Application relating to: (snip) ・ responsiveness ・ acknowledgement and acceptance.	According to WTBR, a Subscriber Agreement and/or Terms of Use shall contain the following two items, an obligation to respond to the CA's instructions and an entitlement to revoke the certificate. However, the two items mentioned above are not described in the Terms of Use. Therefore, the CAs shall update the Terms of Use to contain an obligation to respond to the CA's instructions and an entitlement to revoke the certificate.
3	2.5.2	The CA maintains controls to provide reasonable assurance that it: (snip) begin investigation of Certificate Problem Reports within 24 hours:	According to WTBR, the CA shall begin investigation of Certificate Problem Report within 24 hours of receipt. The above requirement is established for problem reports between LRA and CA, however as to the CA (GPKI) response to problem reports from subscription users, investigation of Certificate

No.	Baseline Requirements		Findings
	Ref.	Criteria	
			Problem Report is designed to start within 24 hours of receipt in business days, but not on holidays. Therefore, CAs shall establish a process that the CA (GPKI) response to problem reports from subscription users can begin investigation within 24 hours on holidays.
4	2.6.2	The CA maintains controls to provide reasonable assurance that: (snip) the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements.	According to WTBR, the LRA shall require all Validation Specialists to pass an examination provided by the LRA on the information verification requirements. However, the LRA only requires all Validation Specialists to participate in a training (basic education, security training, privacy data protection, requirements of verification), but passing an examination after training is not required. Therefore, the LRA shall document and implement a policy to have all Validation Specialists passing an examination provided by the CA after participating the training.
5	2.6.2	The CA maintains controls to provide reasonable assurance that: (snip) the CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.	According to WTBR, the CA shall document each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. However, the LRA has not a rule to document skills required for a specific task for each Validation Specialist before he/she performs the task. Therefore, the LRA shall document skill required for specific tasks for each Validation Specialist.
6	2.6.6	The CA maintains controls to provide reasonable assurance that the CA internally audits each Delegated Third Party's compliance with the Baseline Requirements on an annual basis.	According to WTBR, the CA shall internally audit each Delegated Third Party's compliance with WTBR on an annual basis. However, the CAs do not perform the WTBR compliance audit for neither IA nor LRA, whereas they perform the internal audits for WebTrust and their CP/CPS. Therefore, the CAs shall include the WTBR compliance for IA and LRA in the scope of their internal audit.
7	2.7.2	The CA maintains controls to provide	According to WTBR, the CA and each Delegated

No.	Baseline Requirements		Findings
	Ref.	Criteria	
		reasonable assurance that the following events are recorded: (snip) CA and Subscriber Certificate lifecycle management events, including: ・Certificate Requests, renewal and re-key requests, and revocation ・ all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement ・ date, time, phone number used, persons spoken to, and end results of verification telephone calls ・acceptance and rejection of certificate requests ・ issuance of Certificates ・ generation of Certificate Revocation Lists (CRLs) and OCSP entries.	Third Party shall record details of the actions taken to process a certificate request, including (1)Time of processing a certificate request (2)Communications with the applicant. There is no field to record the processing time and communication description with the applicants on the form ruled by the LRA internal operation procedures, although the form has the date field. In addition, although their internal operation procedures require that the Validation Specialist should record the results of verification on this form, they do not use it, but use a different form. The LRA shall add the fields to this form in order to record the processing time and communication description with the applicants and operate to use this form effectively.
8	2.7.3	The CA has a policy and maintains controls to provide reasonable assurance that audit logs generated after the effective date of the Baseline Requirements are retained for at least seven years.	According to WTBR, the CA shall retain any audit logs generated after the effective date for at least seven years. However, the policy has documented that firewall log is retained at three years. Therefore, the CAs shall update the rule to retain firewall log at least seven years.
9	2.8.1	The CA maintains controls to provide reasonable assurance that the following requirements are followed for Subordinate CAs: (snip) for a Subordinate CA that is not technically constrained: ・the CA verifies that Subordinate CAs that are not technically constrained are audited in accordance with SSL Baseline Requirements 17.1.	According to WTBR, the CA shall ensure that the Subordinate CA meets all applicable Baseline Requirements. However, the subordinate CA (APCA2 (Sub)) has not been audited in accordance with these requirements. Therefore, the APCA2 (Sub) in addition to the APCA2 (Root) shall be taken the WTBR audit.
10	2.8.3	The CA maintains controls to provide reasonable assurance that: ・it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three	According to WTBR, the CA shall monitor adherence to its CP/CPS and WTBR and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of certificate.

No.	Baseline Requirements		Findings
	Ref.	Criteria	
		percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken.	However, as to the sample based self audits including LRA, performed by the CAs, there are no rules to audit whether the RA procedures were performed in compliance with WTBR. And also, the CAs did not retain sufficient evidence of these audits. Therefore, the CAs shall document the audit procedures to monitor their RA process in compliance with WTBR, and retain sufficient audit evidence.
11	3.9	The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	According to WTBR, the CA shall provide all personnel performing information verification duties with skills-training. However, the CA internal operation procedures require that the members' training should be determined by the LRA controller, and that each LRA member should study the knowledge and techniques needed at starting the LRA work. Therefore, they do not have a unified education standard and do not have any curriculum for training the all LRA personnel including LRA controllers. Therefore, the CAs shall document the rule that they establish the unified training plan in the internal operation procedures, and the LRA shall implement those processes covering the controller and all other personnel in LRA.
12	4.1	The CA maintains controls to provide reasonable assurance that: (snip) Authentication keys and passwords for any privileged account or service account on a Certificate System is changed, when a person's authorization to administratively access that account on the Certificate System is changed or revoked;	According to WTBR, each CA or Delegated Third Party shall change authentication keys and passwords for any privileged accounts or service account on a Certificate System whenever a person's authorization to administrative access is changed or revoked. However, the CAs and LRA's internal operation procedures require that the LRA personnel have to change the password only but do not have to change the authentication key when a personnel is replaced or terminated. Therefore, the CAs and LRA shall document and implement the rule of authentication key change of IC authentication card, not only password change, when a personnel is replaced or terminated.
13	4.1	The CA maintains controls to provide reasonable assurance that:	According to WTBR 4.1, each CA or Delegated Third Party shall implement multi-factor

No.	Baseline Requirements		Findings
	Ref.	Criteria	
	4.2	(snip) Multi-factor authentication is implemented to each component of the Certificate System that supports it; The CA maintains controls to provide reasonable assurance that: (snip) Enforce multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems;	authentication to each component of the Certificate System. According to WTBR 4.2, the CAs shall implement multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems. The CAs implement multi-factor authentication to Issuing Systems by password and IC card. However, for some administrator accounts on Certificate Management Systems the CAs do not implement the logical multi-factor authentication, whereas they implement the physical facility access control and the logical password authentication. Therefore, the CAs shall implement multi-factor authentication for these accounts to Certificate Management Systems.
14	4.2	The CA maintains controls to provide reasonable assurance that: (snip) Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations;	According to WTBR, each CA or Delegated Third Party shall review all system accounts at least every 90 days. However, the review of all operator user accounts is performed every 6 months for the CAs. Therefore, the CAs shall update the rule to perform the accounts review every 90 days.
15	4.2	The CA maintains controls to provide reasonable assurance that: (snip) Disable all privileged access of an individual to Certificate Systems within 24 hours upon termination of the individual’s employment or contracting relationship with the CA or Delegated Third Party;	According to WTBR, each CA or Delegated Third Party shall implement a process that disables all privileged access of an individual to Certificate Systems within 24 hours upon termination of the individual’s employment or contracting relationship with the CA or Delegated Third Party. However, the CAs disable privileged access of the individual’s employment or contracting relationship by deleting the physical access of their facilities. Therefore, the CAs shall document the rule and implement to delete not only the physical access, but also the logical access, e.g. the administrator's password change, within 24 hours upon termination of the individual’s employment or contracting relationship with them.
16	4.2	The CA maintains controls to provide reasonable assurance that:	According to WTBR, each CA or Delegated Third Party shall implement the controls to require that

No.	Baseline Requirements		Findings
	Ref.	Criteria	
		(snip) Trusted Role using an username and password to authenticate shall configure accounts to include but not be limited to ・Passwords have at least twelve (12) characters for accounts not publicly accessible (accessible only within Secure Zones or High Security Zones); ・Configure passwords for accounts that are accessible from outside a Secure Zone or High Security Zone to have at least eight (8) characters, be changed at least every 90 days, use a combination of at least numeric and alphabetic characters, and not be one of the user's previous four passwords; and implement account lockout for failed access attempts; OR ・Implement a documented password management and account lockout policy that the CA has determined provide at least the same amount of protection against password guessing as the foregoing controls.	passwords have at least twelve (12) characters for accounts that are not publicly accessible (accessible only within Secure Zones or High Security Zones). However, for some user accounts, the internal operation procedures require at least 8 characters and 8 characters are actually implemented. Therefore, the CAs shall update the rule and implement to have at least 12 characters for all accounts.
17	4.2	The CA maintains controls to provide reasonable assurance that: (snip) Trusted Role use a unique credential created by or assigned to that person for authentication to Certificate Systems;	According to WTBR, each CA or Delegated Third Party shall require that each individual in a Trusted Role use a unique credential created by or assigned to that person for authentication to Certificate Systems. However, the users of a LRA system can spoof the others because of improper control of their IC authentication cards and passwords. Therefore, the LRA shall perform proper management of IC authentication cards and passwords.
18	4.4	The CA maintains controls to provide reasonable assurance that: (snip) A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities;	According to WTBR, the CA and Delegated Third Party shall document a vulnerability correction process including identification, review, response, and remediation of vulnerabilities. The CAs collect vulnerability information on a daily basis and also perform the vulnerability identification, review, response, and remediation against the vulnerability scan and penetration test

No.	Baseline Requirements		Findings
	Ref.	Criteria	
			results. However, the CA does not have any documentation of policies for these activities. Therefore, the CAs shall document the rule that vulnerability correction process and improve the process to include the penetration test results.
19	4.4	The CA maintains controls to provide reasonable assurance that: (snip) Perform a Vulnerability Scan on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following: ・Within one week of receiving a request from the CA/Browser Forum, ・After any system or network changes that the CA determines are significant, and ・At least once per quarter;	According to WTBR, the CA and Delegated Third Parties shall perform a Vulnerability Scan based on the following: ・Target system All related Certificate Systems ・Target IP Address Public and private IP addresses ・Frequency Within one week of receiving a request from the CA/Browser Forum, After any system or network changes that the CA determines are significant, and At least once per quarter, on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems. However, per inspection of the scan report, the frequency of the scan is annual, and targeted servers and IP addresses are limited. Therefore, the CAs shall document and implement the vulnerability scan policy based on WTBR including their target systems, target IP addresses and frequency.
20	4.4	The CA maintains controls to provide reasonable assurance that: (snip) Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant;	According to WTBR, the CA and Delegated Third Party shall undergo a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant. However, per inspection of the report, they perform these tests as a part of the vulnerability scan on an annual basis, these tests are insufficient against the Penetration Test requirements in WTBR. Therefore, the CAs shall document the rule and implement to undergo Penetration Test of which contents are in conformity with WTBR.
21	4.4	The CA maintains controls to provide reasonable assurance that:	According to WTBR, the CA and Delegated Third Party shall record evidence that each Vulnerability

No.	Baseline Requirements		Findings
	Ref.	Criteria	
		(snip) Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test;	Scan and Penetration Test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test. However, per inspection of the report of Vulnerability Scan and Penetration Test, there were not any records of the above items required by WTBR. Therefore, the CAs shall document and implement the rule of recording the above items in Vulnerability Scan and Penetration Test reports.
22	4.4	The CA maintains controls to provide reasonable assurance that: (snip) Perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: ・Remediate the Critical Vulnerability; ・If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: ・Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and ・Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: ・The CA disagrees with the NVD rating; ・The identification is a false positive; ・The exploit of the vulnerability is	According to WTBR, the CA and Delegated Third Parties shall perform one of the following (i) – (iii) within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: (i) Remediate the Critical Vulnerability; (ii) If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: (1) Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical; and (2) Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or (iii) Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: (a) The CA disagrees with the NVD rating; (b) The identification is a false positive; (c) The exploit of the vulnerability is prevented by compensating controls or an absence of threats; (d) Other similar reasons. The CA's internal operation procedures document a correction process based on materiality and priority of correction. However, there are some gaps between the actual correction process and WTBR, such as no rules of the correction process within 96 hours.

No.	Baseline Requirements		Findings
	Ref.	Criteria	
		prevented by compensating controls or an absence of threats; or Other similar reasons.	Therefore, the CAs shall update and implement the rules of vulnerability correction process based on WTBR.