Ministry of Information and Communications Technology

Web Trust Readiness Assessment

Microsoft Action Plan

May, 2018

Draft for discussion purpose

1.1 Summary of Gaps

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
64	5.2.1 5.2.4-10	MoICT Issuing G2G CA doesn't keep a copy of the subscriber's private keys for Encryption Certificates.	**Major**	We recommend MoICT to maintain a copy of the subscriber's private keys for Encryption Certificates, which are used for decryption purposes.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	MS has agreed to resolve this observation.	Confirmed	N/A
71	6.1.1 6.1.5 6.4.7	MoICT doesn't have RA to verify the subscribers certificate requests to G2G issuing CA.	**Major**	We recommend MoICT to establish RA to verify the subscribers certificate requests to G2G issuing CA and sign the requests that are being sent to Issuing G2G CA.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	MS has agreed to do the following to address the observation: 1- Disable of auto-enrollment. 2- Create an enrollment agent which would act as RA 3- MS will provide details of	Process will be implemented in the following way: 1. Absolutely all certificate auto-enrollment will be disabled. 2. Enrollment Agents will have to be appointed by MoICT 3. Every enrollment agent will be	N/A

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
						certificate approval process	issued an Enrollment Agent certificate via the process, which requires certificate request approval by the CA Certificate Manager in the ADCS management console (MMC). 4. All certificate templates (except for the Enrollment Agent certificate template) will be changed to require 2 enrollment agent signatures on the request (can be decreased to 1 if deemed	

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
							appropriate), to be considered valid. 5. Once the valid certificate request, signed by at least the required number of Enrollment Agent certificates, is received, CA will automatically issue the certificate. It is considered, that additional approval, by the CA Certificate Manager is not required, as it will be a responsibility of the Enrollment Agent to verify the	

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
							validity of the request. CA Certificate Manager approval, can, however be turned on, if required.	
74	6.1.6	Issuing G2G CA doesn't verify the uniqueness of the subscriber's common name and allows multiple certificates of the same type to be issued to the same user if they have more than one machines.	**Major**	We recommend MoICT updating the configuration of Issuing G2G CA to implement the uniqueness functionality for the subscriber's common name and doesn't allow multiple certificates of the same type to be issued to the same user.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	WebTrust clauses 6.1.6 states the following: "The CA verifies the uniqueness of the subscriber's distinguished name within the boundaries or community defined by the CP. And since MOICT CP mandates this, so it has to either comply with this requirement or change the CP	Our suggestion is to either update the CP, or to implement the RA, which would perform said verification, CA service implements the core functionality of the PKI, i.e. issuance of certificates, based on the valid certificate requests, more advanced business rule verifications are to implemented on the RA level. ***07-02-2017:*** RA implementation option is acceptable, this should be treated as a change request	Auditor suggest to implement RA or enrolment agent (if it satisfy this requirement to verify the uniqueness). Currently MoICT doesn't implement RA and manual verification for uniqueness is not fool-proof or accurate. So if this can be thru RA/enrolment agent it would be ideal.

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
						to allow this if MoICT has business needs for accepting that. Refer to Appendix in the last page).	for the existing project scope. ***Needs discussion with MoICT.***	
78	6.1.16 6.3.10 3.10.12-13	MoICT CA/RA doesn't sign the audit logs for subscriber registration events.	**Minor**	We recommend MoICT CA/RA signing the audit logs for subscriber registration events to ensure the integrity of these logs.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project If needed Microsoft will work with gemalto for RA/CSPD audit logs	The following are implanted: - DB is signed by CA. - In case of deletion of audit logs, the deletion event will be logged. However, in accordance to WebTrust clause 3.10.12-13 (refer to Appendix in the last page), the audit logs should be signed.	Subscribers are not registered firsthand in the Microsoft developed part of the solution, those are, supposedly, registered in the RA, therefore, it is a responsibility of the RA to perform audit signing operations. ***07-02-2017:*** RA implementation option is acceptable, this should be treated as a change request for the existing project scope. ***Needs discussion with MoICT.***	As suggested by MS, if it is the current function of RA to sign the audit logs and RA is not implemented, what is the ideal solution recommended by MS. Auditor suggest to implement RA or enrolment agent (if it satisfy this requirement).
79	6.3.1	Certificate Rekey Process is not	**Minor**	We recommend MoICT to define the	WS1: Point-In Time	However, during our meetings	Microsoft team was not implementing the	N/A

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
		clear and not documented. We couldn't confirm the time of requesting certificate rekey for the government employees' subscribers.		certificate rekey process and communicate it to related parties, including the process of automatic certificate rekey for the government employees' subscribers covering the time of requesting certificate rekey	Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	last year, MoICT didn't confirm if rekey implemented or not, So MS/MOICT to confirm that; if it's not implemented this observation would be removed.	certificate rekey processes.	
80	6.3.2 6.3.9	MoICT doesn't have RA to verify the subscriber rekey requests and sign the request that is being sent to Issuing G2G CA.	**Major**	We recommend MoICT to establish RA to verify the subscribers rekey requests to G2G issuing CA and sign the request that is being sent to Issuing G2G CA.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	However, during our meetings last year, MoICT didn't confirm if rekey implemented or not, So MS/MOICT to confirm that; if it's not implemented this observation would be removed.	Microsoft team was not implementing the certificate rekey processes.	N/A
82	6.3.13	The Issuing G2G and G2BC CA doesn't notify the	**Minor**	We recommend MoICT updating the configuration of the	Two parts: WS1: Point-In Time	If the rekey implemented, MS to provision	Microsoft team was not implementing the certificate rekey	We suggest to enable the notification functionality for expiry

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
		subscribers prior to the expiration of their certificate or if there's a need for rekey.		Issuing G2G and G2BC CAs to send notifications for subscribers prior to the expiration of their certificate and if there's a need for rekey.	Assessment (PITA) for all PKI projects – Microsoft CA enhancement project WS1: Point-In Time Assessment (PITA) for all PKI projects – Gemalto RA with CA communication enhancement project	the notification for the rekey. Auditor reviewed the CP and CPS and found out that no stipulations in place for notifications of re-key	processes. Moreover, in the design documents as well as e-mail communication, it has been mentioned several times, that the part of the solution, developed by the Microsoft team, will not have any notification functionality, all notification functionality should be implemented in the RA. Implementation of notifications in the solution components, developed by the Microsoft should be treated as a change request to the existing solution. ***07-02-2017:*** RA implementation option is acceptable, this should be treated as a change request for the existing project scope. If	of normal certificates (as rekey is not applicable for MoICT).

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
							notification functionality is to be implemented on the CA side, this should be treated as a change request for the existing project scope. ***Needs discussion with MoICT.***	
86	6.4.6 6.4.8 6.4.9	The process of sending notification from CA to RA, when a certificate is issued to a subscriber, is not activated as defined in the Issuing CP.	**Minor**	We recommend MoICT to activate the process of sending signed notification from CA to RA/subscriber as defined in the issuing CP.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	MS has agreed to establish RA and this observation will be resolved during the RA implementation.	MS did not agree to establish the RA, MS suggested, that this is a potential option for addressing the recommendation – implementing the RA. Our team will need to review possible options and offer a solution, which should be treated as a separate project. ***07-02-2017:*** RA implementation option is acceptable, this should be treated as a change request for the existing project scope. If	Auditor suggest to implement RA or enrolment agent (if it meet this requirement) or any other option which meet this requirement. It's MoICT decision if they agree to consider it as change request or not.

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
							notification functionality is to be implemented on the CA side, this should be treated as a change request for the existing project scope. ***Needs discussion with MoICT.***	
87	6.5.3	MoICT has not implemented a process to monitor the performance of the CA's repository (LDAP).	**Minor**	We recommend MoICT to monitor the performance of the CA's repository (LDAP) regularly and configure it to send notifications to administrator in case of any error or failure.	Two parts: -WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project for configuration part - MoICT responsibility to monitor and implement the process	MoICT /Abdullah will provide his input.	N/A	N/A
91	6.6.3	MoICT doesn't have RA to verify the subscriber	**Major**	We recommend MoICT to establish RA to verify the	WS1: Point-In Time Assessment		The functionality should be considered as a part of the	Auditor suggest to implement RA or enrolment agent (if it

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
		certificate revocation requests submitted to G2G Issuing CA.		subscribers certificate revocation requests to G2G issuing CA and sign the request that is being sent to Issuing G2G CA.	(PITA) for all PKI projects – Microsoft CA enhancement project for configuration part	MoICT has to develop a web page where the subscribers filling the details for the revocation request. G2G CA verify/ validate the subscriber's revocation requests using windows credentials or using the current process of revocation.	overall RA implementation, if RA is chosen to be implemented. Also, from the observation it is not really clear, what kind of information is to be submitted in the request? If Windows authentication of the revocation requestor is enough, then it is already implemented, only CA Certificate Manager group members, authenticated, using Windows integrated authentication can perform revocation. ***07-02-2017:*** From the comment it seems, that the revocation request in question is not an API call, but a document, which then is processed by either an operator or the RA solution. RA	meet this requirement) or any other option which meet this requirement. Ideally, the revocation request contains the Certificate serial number and the reason for revocation.

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
							implementation option is acceptable, this should be treated as a change request for the existing project scope. ***Needs discussion with MoICT.***	
92	6.6.3	CSPD RA doesn't sign the subscriber certificate revocation requests that are being sent to Issuing G2BC CA.	**Minor**	We recommend MoICT updating the configuration of Issuing G2BC CA to ensure that CSPD RA signing the subscriber certificate revocation request that is being sent to G2BC Issuing CA.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Gemalto RA with CA communication enhancement project	Since, the CSPD is external RA, the following WebTrust clause has to be implemented by Gemalto: "If an external RA accepts revocation requests, the CA requires that the RA submit signed certificate revocation requests to the CA in an authenticated manner in accordance with the CP".	Because any requests, traveling between CSPD and PKI solutions are API calls, please elaborate, what exactly "signed certificate request"? is it enough for the channel to be SSL protected? If not, then how in your opinion is the signed API call should look like? ***07-02-2017:*** It is not clear, what SafeNet has to do with this functionality, as neither of the SafeNet technology is a part of the solution. We can suggest performing certificate	No, SSL is not enough. The request would need to have details of the requestor's certificate (Serial number), reason for revocation. The ideal situation is where the CA recognizes that the revocation requests is from the authorized RA who has signed so that CA can process. I suggest to discuss this approach with SafeNet. **8-02-2018:**

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
						MS has to confirm if it's responsibility of MS or Gemalto to implement the above	authentication of the RA, developed by Gemalto, then recording API call from the RA to the CA integration service into the AuditLog with the details of the authentication certificate and revocation request details. AuditLog records are protected from tampering by signing.	The suggestion is a workable solution in case there is NO way that they can use a RA signature to sign the API call.
94	6.6.9	MoICT CA/RA doesn't notify the subscriber when their certificates are revoked.	**Minor**	We recommend MoICT notifying the subscribers when their certificates are revoked.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project WS1: Point-In Time Assessment (PITA) for all PKI projects – Gemalto RA with CA	• Microsoft will take care of G2G CA part • Gemalto shall take care of G2C CA part	In the design documents as well as e-mail communication, it has been mentioned several times, that the part of the solution, developed by the Microsoft team, will not have any notification functionality, all notification functionality should be implemented in the RA. Implementation of	We suggest to enable the notification functionality for the revoked certificates. It's MoICT decision if they agree to consider it as change request or not.

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
					communication enhancement project		notifications in the solution components, developed by the Microsoft should be treated as a change request to the existing solution. ***07-02-2017:*** ***RA changes need discussion with MoICT.*** If notification functionality is to be implemented on the CA side, this should be treated as a change request for the existing project scope. ***Needs discussion with MoICT.***	
95	6.8.1 6.8.11 6.8.12 6.8.13	MoICT has not configured and implemented Online Certificate Status Protocol (OCSP), which provide information about the subscriber	**Major**	We recommend MoICT configuring and implementing OCSP to provide the relying party with the subscriber certificate status when requested.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	MS will confirm if OCSP was implemented or not for G2G and G2C	Agreed	N/A

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
		certificate status.						
96	6.8.1 6.8.2 6.8.3	The validity period of Issuing CAs CRL is 10 days which is too long. The frequency of publishing Issuing CAs CRL is once a day, which is not effective.	**Major**	We recommend MoICT updating the validity period of Issuing CA CRL to be 1 day. In addition, we recommend MoICT updating the frequency of publishing CRL to be at least once a day, or immediately up on revocation of any subscriber certificate, whichever is earlier.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	MS will confirm if OCSP was implemented or not for G2G and G2C	Agreed	N/A
97	6.8.6 6.8.9 6.8.10	MoICT has not maintained archival of CRLs , expired, revoked and suspended certificates, as defined in the related CPs.	**Minor**	We recommend MoICT to maintain archival of CRLs and expired, revoked and suspended certificates as defined in the related CP, which is 10 years.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	MS has agreed to implement it.	Agreed	N/A

#	Ref. #	Summary of Identified Gaps	Severity	Recommendations	Proposed Action Plan	Action Plan for Microsoft	Microsoft comments	Auditor Feedback
102	7.1.13	MoICT has not configured and implemented Online Certificate Status Protocol (OCSP), which provide information about the certificate status.	**Major**	We recommend MoICT configuring and implementing OCSP to provide the relying party with the sub-CAs certificate status when requested.	WS1: Point-In Time Assessment (PITA) for all PKI projects – Microsoft CA enhancement project	MS will confirm if OCSP was implemented or not for G2G and G2C	Agreed	N/A

- **The below requirement moved from Gemalto Action Plan to MS action Plan, as agreed during our phone call today – April 11:**

73	6.1.5 6.1.11 6.1.13 6.1.14 6.1.15 6.1.17	Civil Status and Passports Department (CSPD) RA doesn't sign the subscriber certificate request that is going to G2BC Issuing CA.	**Major**	We recommend MoICT to make CSPD RA signing the subscriber certificate request that are being sent to G2BC Issuing CA.	**Shared responsibility between Microsoft and Gemalto.**

94	6.6.9	MoICT CA/RA doesn't notify the subscriber when their certificates are revoked.	**Minor**	We recommend MoICT notifying the subscribers when their certificates are revoked.	• Microsoft agreed that they will take care of this observation and will be handled from CA side.

In accordance to the phone call on May 14, 2018 with MS and MoICT team, the following will be Joint efforts between Gemalto and MS:

73	Civil Status and Passports Department (CSPD) RA doesn't sign the subscriber certificate request that is going to G2BC Issuing CA.	Joint efforts between Gemlato and MS. - MS will add the related portion to SOW.
92	CSPD RA doesn’t sign the subscriber certificate revocation requests that are being sent to Issuing G2BC CA.	Joint efforts between Gemlato and MS. - MS will add the related portion to SOW.

In accordance to the confirmation from MS on May 29, 2018 for the discussion points and feedback shared with them, the following will be considered:

- MS will include the implementation of OCSP as part of SOW **(Obs # 95 & 102)**
- A cleanup of duplicate certificates in CRL will be implemented in order to address the issue of CRL size **(Obs #96)**
- MS will involve in the following technical components which will used as an input for BCP/DRP **(Obs # 38, 39, 54 & 55):**
  - Disaster recovery procedure in case of the primary site go down or part of PKI solution should be developed and included the following:
    - Recovery procedures to be executed in case computing resources, software, and/or data are corrupted or suspected to be corrupted;
    - How secure key usage in the environment is re-established;
    - How the CA's old public key is revoked;
    - How the CA's new public key is provided to the end entities and relying parties together with the mechanism for their authentication;
    - How the subscriber's public keys are re-certified;
    - The procedures of handling the operations at the time of key compromise includes who should get notifications and the actions taken to recover the operations and what actions are taken with system software and hardware and previously generated signatures and encrypted data; and
    - Procedures for the secure and authenticated revocation of the following in the event that the CA has to replace its Root CA private key):
      - The old CA Root public key;
      - The set of all certificates (including any self-signed) issued by a Root CA or any CA based on the compromised private key; and Any subordinate CA public keys and corresponding certificates that require recertification.
- Explicitly mention in the SOW that enrollment agent implementation will address signing the audit logs for G2G subscriber registration events **(Obs # 78).**
- MS will share with MoICT the limitations that will result from remediation of the below observation **(Obs #74):**

  "Issuing G2G CA doesn't verify the uniqueness of the subscriber's common name and allows multiple certificates of the same type to be issued to the same user if they have more than one machines."