SHARED SERVICES CANADA

Amendment No. 003
to the
Request for Information
For the Procurement Process for
Smart Card/Token Requirement, Public Key Infrastructure

Request for Information No.	RAS 17-58040 /A	Date	October 10, 2017
GCDocs File No.	N/A	GETS Reference No.	PW-17-00793575

This Amendment addresses the second set of Suppliers' Q&As.

Issuing Office	Shared Services Canada | Services partagés Canada 180 rue Kent St, Ottawa, Ontario, K1G 4A8 Canada	
Contracting Authority (The Contracting Authority is SSC's representative for all questions and comments about this document.)	Name	Michelle Marengère
	Telephone No.	613-410-9077
	Email Address	michelle.marengere@canada.ca
	Postal Address	Shared Services Canada | Services partagés Canada 180 rue Kent St, 13-078 Ottawa, Ontario, K1G 4A8 Canada
Closing Date and Time	**October 18, 2017 – 11:59 PM**	
Time Zone	Eastern Standard Time (EST)	
Destination of Goods/Services	Not applicable – Request for Information Only	
Email Address for Submitting your Response by the Closing Date	michelle.marengere@canada.ca	

QUESTION 1

In Section 2.2d you have asked “how have token manufacturers worked to integrate their technologies with DND’s current platforms (Certificate Authority and Card Management System)? “. From the RFI, I can see that the Certificate Authority (CA) is Entrust. Is Entrust also providing the Card Management System (CMS)? I ask because typically Entrust only acts as the (CA) while the CMS vendor is usually HID(ActivIDentity) or Intercede or the like.

ANSWER 1

DND has deployed the Entrust Identity Guard solution. Please see requirement 23 that clearly identifies this CMS within the statement of requirements.

QUESTION 2

In Section 4, you’ve mentioned the following technical requirements which seem to contradict each other. #5 states “The token applet has been certified in the contest of the GlobalPlatform(GP) Composition Model “; #18 states “The token must support the PIV-C, PIV and PIV-1 standards” The Personal Identify Verification (PIV)(FIPS201) standard requires the certification of the platform and applet together and does not follow the GP Composition Model. Also typically either the PIV certification is used or Common Criteria or EMVCo. The certifications are not mixed. Could you clarify?

ANSWER 2

DND’s intention is to present the incongruence of the over-lapping certifications, and request that the industry provide a solution which would achieve the required specifications.

QUESTION 3

Do you need a PIV certified applet or simply a PKI applet? In our experience, the use cases that you have mentioned, namely email, file encryption and signature need PIV rather than CC or EMVCo?

ANSWER 3

DND maintains two environments, one which utilizes X.509 smart cards (low side), and the other PIV tokens/smart cards (high side). The high side PIV applet token is used with Entrust Identity Guard CMS. The Entrust Identity Guard CMS is quite limited on the low side. The vast majority of users are not managed with CMS, outside of a proof of concept with Entrust Identity Guard.

QUESTION 4

In section 5, you have mentioned “estimated delivery date for the tokens will be on or before 31 March 2018 for the first order” Can you give us an idea of the volume for the first order? Silicon lead times can be very long, typically, 16-20 weeks; hence we need to plan accordingly.

ANSWER 4

The delivery date has been changed and will be indicated in the RFP (request for proposal). The resulting solicitation will take into account the applicable production time.

Except as expressly amended by this document, the RFI remains unchanged.

Please note that this completes the Q&A period for this RFI.