SHARED SERVICES CANADA

Amendment No. 002
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 5, 2017
GCDocs File No.	N/A	GETS Reference No.	PW-17-00793575

This Amendment revises the RFI's previously amended closing date, released by SSC on September 29, 2017, and addresses the first set of Suppliers' Q&As~~-~~. Except as expressly amended by this document, the RFI remains unchanged.

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

Would a non-Java card smartcard be acceptable to DND?

ANSWER 1

The solution requirements focus entirely on security, performance and interoperability with existing solution components (Card Management System, Entrust CA etc.). So long at the card meets these requirements, DND would accept the card.

QUESTION 2

Does the government plan on keeping the Entrust smart card solution? Is this opportunity just a “token” purchase? My company, XTec, currently issues PIV smart cards to the US Government’s Dept. of Homeland Security, Dept. of State, others. We can offer the same secure technology and standards based solution that would ensure security, and interoperability with various logical access and physical access systems, as well as interoperability with US government solutions. Our solution allows for and manages derived credentials for use on mobile devices (phones, tablets, etc.) and other tokens (USB, etc.).

ANSWER 2

DND will maintain the Entrust CA solution and Entrust IdentityGuard solution. There is a need provide tokens for the expanding user base and replace or lost/damaged tokens, without completely replacing the Entrust tokens (smart cards) currently in circulation.

The intent is to develop a solicitation for tokens.

DND maintains two environments, one which utilizes smart cards, and the other Personal Identify Verification (PIV).

Yes, DND is considering other form factors, although other form factors will have more limited usage/distribution. DND already has a derived credential solution for use on mobile devices. Therefore, this is not within the scope of this RFI nor expected to be within the scope of a subsequent solicitation.