Public Works and Government Services Canada

Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

Title - Sujet
DESIGNATED PKI SMART CARD

Solicitation No. - N° de l'invitation	Amendment No. - N° modif.
W8474-167124/A	001
Client Reference No. - N° de référence du client	**Date**
W8474-167124	2015-10-23

GETS Reference No. - N° de référence de SEAG
PW-$$QE-071-25431

File No. - N° de dossier	CCC No./N° CCC - FMS No./N° VME
071qe.W8474-167124	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2015-11-09

Time Zone
Fuseau horaire
Eastern Standard Time
EST

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Munro, Celine	071qe
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(819) 956-0586 ( )	(819) 956-6907

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
Canadian Forces Crypto Support Unit PKI CRA Svsc
Building 512
265 DeNivervielle Private
Ottawa, Ontario
K1V 7N5

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	Delivery Offered - Livraison proposée

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm
(type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/
de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Issuing Office - Bureau de distribution
Security and Information Operations Division/Division de la securite et des operations d'information
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Canada

Amendment no. 01 to the solitation is issued to include the Annex B - Statement of Work and Annex C - Technical Compliance Evaluation.

DEPARTMENT OF NATIONAL DEFENCE (DND)

Statement of Work (SOW)
W8474-16-7124/A
13 October 2015

Interim Smart Card Replacement for the Designated Public Key Infrastructure (D-PKI) Project

for

Directorate of Information Management Engineering and Integration

Table of Contents

1 BACKGROUND

The Directorate of Information Management Engineering and Integration (DIMEI) has been tasked to update and modernize the existing Department of National Defence (DND) Public Key Infrastructure (PKI). This Designated PKI (D-PKI) has been in operation for over 10 years and supports over 50,000 users. PKI enablement has been implemented both within applications (digital signature) as well as with infrastructure (authentication). Email, file encryption and digital signature have been rolled out to users. For future interoperability with its US partners at the Department of Defense (DoD), PKI will be used when authenticating to DoD resources. The Department of National Defence (DND) solution is based on an Entrust PKI.

New projects such as Military Pension Renewal (MPR) and Defence Command and Control Allied Interoperability (DC2AI) require D-PKI to extend D-PKI trust beyond DND for use with other non-DND intranets including Canadian Other Government Departments (OGD), Allies OGDs and industry in order for DND-issued certificates to be recognized and accepted by these external organizations. D-PKI interoperability enables secure information access and exchange with external organizations (e.g. secure email, strong authentication to a secure website). The required external interoperability cannot be achieved with the existing D-PKI. One area requiring immediate resolution is the replacement of the PKI smart card. A replacement smart card is necessary to support the upcoming Secure Hash Algorithm 256 (SHA2) migration as well as to address a declining inventory of the current solution.

2 REQUIREMENTS

The D-PKI smart card requirements are based on a number of pre-existing infrastructure components that include both hardware and software. The smart card will be used within an Entrust CA environment and support the existing users. The smart cards must be printed with a specific graphics provided by DND. The following two sections identify both the graphics and technical specifications for the procurement.

3 GRAPHICS SPECIFICATIONS

DND has established the graphics specifications for the smart card. The following image is the design that will be used. A graphic file in Adobe Illustrator shall be provided upon request. Slight moving of words may be approved to accommodate the location of the embedded chip. The winning Bidder must provide a proof for DND acceptance as part of the bid process.

3.1 Front of Card

3.2 Back of Card

The following information is to be printed on the back of the card (black letters on white background):

Reminder	Rappel
Keep your smartcard secured Do not leave unattended while in use If found drop in any Canadian mailbox K1A 0K2	Gardez votre carte en lieu sûr Ne la laissez pas sans surveillance pendant son utilisation Si on trouve cette carte la déposer dans une boîte à lettres canadienne K1A 0K2

The spacing of the wording may be adjusted so that it does not conflict with the serial number or the embedded chip.

4 TECHNICAL REQUIREMENT

The D-PKI smart card requirements are based on a number of pre-existing infrastructure components that include both hardware and software. The procurement of the smart card must result in a technology that can be incorporated into the existing environment. The following specifications represent the current environment. The proposed smart card must be able to function within this environment with only minimum configuration changes. A smart card requiring substantive modifications (changes to hardware, software, or processes) to the current environment shall be deemed non-compliant. A minimum configuration change is defined as any one or more of the following:

a. A change that costs less than $10,000 to implement;
b. A change that has a recurring operational cost of less than $5,000 per year; and/or
c. A change that requires less than two weeks of integration work for DND to implement using existing DND resources.

DND will assess any change requirements and determine whether or not required changes are “minimum”.

As part of the bid evaluation process, Bidders must provide compliance tracking to the technical specifications below in the Substantiation of Technical Compliance Form attached within the RFP. Accompanying the bid submission, Bidders shall supply five (5) smart cards (at no charge to the Government of Canada) with information necessary so that DND is able to conduct internal testing against the technical specifications listed within the table. Bidders are also encouraged to supply a point of contact within their product engineering support staff in case DND has a question while conducting the internal tests. Any assistance provided in the examination and preparation of the requirements validation testing shall be at the Bidder’s cost.

The list of mandatory requirements constitutes the testing DND will perform in order to determine if the proposed smart card technology is compliant.

No.	Requirement
1	The smart card must be minimum Federal Information Processing Standard (FIPS) 140-2 Level 2 certified/validated. Provide reference from National Institute of Standards and Technology (NIST) site such as: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm where the product is listed.
2	The smart card must have greater than 48 kilobytes memory available for certificate storage after all applets and any required files are placed on the token.
3	The smart card must be able to hold at least 10 certificates of 2048-bit Rivest-Shamir-Adleman (RSA) keys.
4	The smart card must support creating, recovering and updating digital certificates with Entrust Security Manager Administration (SMA) 8.1 Service Pack 1 (SP1)

No.	Requirement
5	The smart card must support creating, updating and recovering digital certificates with Entrust Security Provider (ESP) for Windows 9.2 and ESP for Outlook 9.1
6	The smart card must support 32 bit and 64 bit Windows 7, Windows 8, Windows Server 2008 and Windows Server 2012.
7	In coordination with SafeNet Authentication Client (SAC) version 8.2, the smart card must support logging to various levels for troubleshooting purposes and /or write to Event viewer.
8	In coordination with SAC version 8.2, the smart card must allow forcing users to change Personal Identification Number (PIN) on first-time login.
9	In coordination with SAC version 8.2, the smart card must support the removal of user certificates from the Cryptographic Application Programming Interface (CAPI) store when a smart card is removed from the smart card reader
10	In compliance with SAC version 8.2, the smart card must support configurable password policies: a. Minimum character length of 6 b. Maximum character length of 15 c. Must have minimum of 1 Upper case alpha character d. Must have a minimum of 1 lower case alpha character e. Must have 1 numeric value
11	The smart card must support SHA-1 and SHA-2 for digital signatures. (Secure Hash Algorithm 1 corresponds to 160-bit hash value while the Secure Hash Algorithm 2 standard with the 256-bit hash value is the required digest for this solicitation)
12	In coordination with SAC version 8.2 and ESP for Windows 9.2, the smart card must support SHA-1 and SHA-256 signed certificates
13	The smart card must support RSA 1024/2048 bit key generation
14	The smart card must support on-chip cryptographic functionality including Advanced Encryption Standard (AES), Triple DES (Data Encryption Standard), RSA 1024/2048 bit.
15	Capability to initialize the smart card must be supported in coordination with SAC version 8.2.
16	In coordination with SAC version 8.2, the smart card must support changing of a user's PIN
17	In coordination with SAC version 8.2, the smart card must support changing the smart card Administrator/Security Officer (Admin/SO) PIN
18	The smart card must support International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 7816 1 to 4 specifications(ISO/IEC 7816 1 to 4 specifications).
19	The smart card must be able to pass Supply Chain Integrity (SCI) as defined at https://www.cse-cst.gc.ca/en/page/technology-supply-chain-guidance
20	The smart card printing must be at 300 dots per inch (dpi) or higher resolution.

DEPARTMENT OF NATIONAL DEFENCE (DND)

W8474-167124

Annex C – BID EVALUATION
Substantiation of Technical Compliance Form

13 October 2015

Interim Smart Card Replacement for the Designated Public Key Infrastructure (D-PKI) Project

for

Directorate of Information Management Engineering and Integration

1. PURPOSE

This document outlines the bid evaluation process for the provision of PKI – Smart Cards for the Department of National Defence.

2. EVALUATION METHODOLOGY

Contract award shall be based on the lowest cost compliant bid submission. Bidders must provide a complete technical and functional specification proposal which shall describe in detail how they meet the following mandatory criteria. The Bidders must identify where this information can be found in their proposal.

CANADA WILL EVALUATE ONLY THE DOCUMETATION PROVIDED WITH A BIDDER`S BID. BIDDER IS TO PROVIDE DOCUMENTATION TO SUPPORT COMPLIANCE TO EACH OF THE MANDATORY CRITERIA.

CANADA WILL NOT EVALUATE INFORMATION SUCH AS REFERENCES TO WEB SITE ADDRESSES WHERE ADDITIONAL INFORMATION CAN BE FOUND, OR TECHNICAL MANUALS OR BROCHURES NOT SUBMITTED WITH THE BID.

RELEVANT WEBSITE REFERENCES MAY BE PRINTED AND INCLUDED IN THE BIDDER`S PROPOSAL TO SUPPORT TECHNICAL COMPLIANCE.

The Bidder must demonstrate compliance with the following criteria. Bidders are requested to complete the following table. Failure to comply will result in the automatic rejection of the bid.

3. BID MATRIX

The bidder must address all of the Mandatory Requirements identified in Table 1 within their bid submission. To facilitate bid review, Bidder should submit a completed copy of Table 1 – Mandatory Requirements with bid submission, in order to validate compliance.

4. **MANDATORY REQUIREMENTS**

Article of Statement of Requirement that requires substantiation by the Bidder		Compliance		Reference to additional Substantiating Materials Included in Offer / Bid reference
		Yes	No	
M1	The smart card must be minimum Federal Information Processing Standard (FIPS) 140-2 Level 2 certified/validated. Provide reference from National Institute of Standards and Technology (NIST) site such as: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm where the product is listed.			
M2	The smart card must have greater than 48 kilobytes memory available for certificate storage after all applets and any required files are placed on the token.			
M3	The smart card must be able to hold at least 10 certificates of 2048-bit Rivest-Shamir-Adleman (RSA) keys.			
M4	The smart card must support creating, recovering and updating digital certificates with Entrust Security Manager Administration (SMA) 8.1 Service Pack 1 (SP1).			
M5	The smart card must support creating, updating and recovering digital certificates with Entrust Security Provider (ESP) for Windows 9.2 and ESP for Outlook 9.1.			
M6	The smart card must support 32 bit and 64 bit Windows 7, Windows 8, Windows Server 2008 and Windows Server 2012.			
M7	In coordination with SafeNet Authentication Client (SAC) version 8.2, the smart card must support logging to various levels for troubleshooting purposes and /or write to Event viewer.			
M8	In coordination with SAC version 8.2, the smart card must allow forcing users to change Personal Identification Number (PIN) on first-time login.			
M9	In coordination with SAC version 8.2, the smart card must support the removal of user certificates from the Cryptographic Application Programming Interface (CAPI) store when a smart card is removed from the smart card reader.			

Article of Statement of Requirement that requires substantiation by the Bidder		Compliance		Reference to additional Substantiating Materials Included in Offer / Bid reference
		Yes	No	
M10	In compliance with SAC version 8.2, the smart card must support configurable password policies: a. Minimum character length of 6 b. Maximum character length of 15 c. Must have minimum of 1 Upper case alpha character d. Must have a minimum of 1 lower case alpha character e. Must have 1 numeric value			
M11	The smart card must support SHA-1 and SHA-2 for digital signatures. (Secure Hash Algorithm 1 corresponds to 160-bit hash value while the Secure Hash Algorithm 2 standard with the 256-bit hash value is the required digest for this solicitation).			
M12	In coordination with SAC version 8.2 and ESP for Windows 9.2, the smart card must support SHA-1 and SHA-256 signed certificates.			
M13	The smart card must support RSA 1024/2048 bit key generation.			
M14	The smart card must support on-chip cryptographic functionality including Advanced Encryption Standard (AES), Triple DES (Data Encryption Standard), RSA 1024/2048 bit.			
M15	Capability to initialize the smart card must be supported in coordination with SAC version 8.2.			
M16	In coordination with SAC version 8.2, the smart card must support changing of a user's PIN.			
M17	In coordination with SAC version 8.2, the smart card must support changing the smart card Administrator/Security Officer (Admin/SO) PIN.			
M18	The smart card must support International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 7816 1 to 4 specifications(ISO/IEC 7816 1 to 4 specifications).			
M19	The smart card must be able to pass Supply Chain Integrity (SCI) as defined at https://www.cse-cst.gc.ca/en/page/technology-supply-chain-guidance .			
M20	The smart card printing must be at 300 dots per inch (dpi) or higher resolution.			