# SHARED SERVICES CANADA

## Request for Information
## For the Procurement Process for
## Smart Card/Token Requirement, Public Key Infrastructure

| | | | |
|---|---|---|---|
| Request for Information No. | RAS 17-58040<br>/A | Date | September 1, 2017 |
| GCDocs File No. | N/A | GETS Reference No. | PW-17-00793575 |

| | | |
|---|---|---|
| Issuing Office | Shared Services Canada \| Services partagés Canada<br>180 rue Kent St,<br>Ottawa, Ontario,<br>K1G 4A8<br>Canada | |
| Contracting Authority<br>(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<br>180 rue Kent St, 13-078<br>Ottawa, Ontario,<br>K1G 4A8<br>Canada |
| Closing Date and Time | October 2, 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 | |

# TABLE OF CONTENTS

**ANNEXES**

# 1. General Information

## 1.1 Introduction

a) **Phase 1 of Procurement Process**: This Request for Information (RFI) is the first phase of a procurement process by Shared Services Canada (SSC) of **a Smart Card/Token Requirement, Public Key Infrastructure** (the "**Project**"). Suppliers are invited to submit responses to assist Canada in refining its requirements for the Project. Suppliers are not required to submit a response to this RFI in order to participate in any later phases of the procurement process for the Project.

b) **RFI Phase is not a Bid Solicitation**: This RFI is not a solicitation of bids or tenders. No contract will be awarded as a result of the activities undertaken during this RFI. Canada reserves the right to cancel any of the preliminary requirements described as part of the Project at any time during the RFI or any other phase of the procurement process. Given that the RFI process and any related procurement activity may be partially or completely cancelled by Canada, it may not result in any subsequent procurement processes.

c) **Response Costs**: SSC will not reimburse any supplier or any of its representatives for any overhead or expenses incurred in participating in or responding to any part of the RFI phase. Suppliers are also responsible for carrying out their own independent research, due diligence and investigations (including seeking independent advice) that they consider necessary or advisable in connection with their participation in the RFI process and any future procurement process.

## 1.2 Overview of the Project

a) **Overview of Project**: The Directorate of Information Management Engineering and Integration (DIMEI) have been tasked to design, develop, and deploy a Public Key Infrastructure (PKI) within two separate security domains at the Department of National Defence (DND). PKI enablement will be implemented both within applications through digital signature(s) as well as with infrastructure through authentication(s). Email, file encryption and digital signature will be rolled out to users. DND's current solution is based on an Entrust PKI. DND intends to competitively establish a Contract(s), Standing Offer(s) (SO(s)), and/or Supply Arrangement(s) (SA(s)) providing the required PKI hard tokens as and when required. The primary focus will be smart cards, however alternate form factors, such as but not restricted to Universal Serial Bus (USB) tokens and SD cards (Secure Digital Memory Cards) will be considered.

Technical compliance to strong security standards is important to DND. Therefore, a robust and high assurance solution, which establishes a supply of tokens that is not wholly dependent upon a single technology or single Original Equipment Manufacturer (OEM), is required.

b) **Scope of Anticipated Procurement:**

i) **Potential Client Users**: This RFI is being issued by SSC. It is intended that the contract(s), standing offer(s) or supply arrangement(s) resulting from any subsequent solicitation would be used by SSC to provide shared services to one or more of its clients. SSC's clients include SSC itself, those government institutions for which SSC's services are mandatory at any point during the life of any resulting instrument(s), and those other organizations for which SSC's services are optional at any point during the life of any resulting instrument(s) and that choose to use those services from time to time. Any subsequent procurement process will not preclude SSC from using another method of supply for any of its clients with the same or similar needs, unless a subsequent solicitation for this Project expressly indicates otherwise.

### 1.3 Submitting Questions

a) Questions about this RFI can be submitted to the Contracting Authority at his or her email address identified on the cover page up until **[5]** working days before the closing date and time indicated on the cover page of this document. Canada may not answer questions received after that time.

b) To ensure the consistency and quality of information provided to suppliers, significant questions received and the answers will be posted on the Government Electronic Tendering Service (GETS) as an amendment to this RFI.

## 2. Information Requested by Canada

### 2.1 Comments on Preliminary Documents

This RFI includes the following documents with respect to which Canada is seeking comments from suppliers:

a) Annex A - Statement of Requirement

All documents reflecting Canada's anticipated requirements for this Project that are provided to suppliers during the RFI process are preliminary or draft requirements only and are subject to change. These requirements, or parts of them, may be updated before or during any subsequent solicitation.

Suppliers are requested to provide their comments, concerns and, where applicable, alternative suggestions regarding how the requirements or objectives described for the Project could be satisfied. Suppliers are also invited to provide comments regarding the content, format and/or organization of any draft documents provided with this RFI. Suppliers should explain any assumptions they make in their responses.

### 2.2 Responses to Questions for Industry

Canada requests responses to the following questions:

a) Which commercial products currently exist that meet or exceed the security assurance required by DND?

b) Are any of the required capabilities unavailable, or not possible given the technology?

c) Do alternative technologies exist which address the security assurance standards required by DND?

d) Because of technology investment (back-end technologies), how have token manufacturers worked to integrate their technologies with DND's current platforms (Certificate Authority and Card Management System)?

e) Do technology standards not identified by DND exist which should be considered? What are they and what is the applicability to security assurance?

f) Which different form factors are available (USB, smart card etc.) and how can the different form factors meet DND's assurance requirements?

## 3. Supplier Responses

### 3.1 Submitting a Response

a) **Time and Place for Submission of Responses**: Suppliers interested in providing a response should submit it by email to the Contracting Authority at the email address for submitting a response identified on the cover page by the closing date and time identified on the cover page of this document.

b) **Responsibility for Timely Delivery**: Each supplier is solely responsible for ensuring its response is delivered on time to the correct email address.

c) **Identification of Response**: Each supplier should ensure that its name and return address, the solicitation number, and the closing date are included in the response in a prominent location. The supplier should also identify a representative whom Canada may contact about the response, including the person's name, title, address, telephone number and email address.

### 3.2 Language of Response

Responses may be submitted in French or English, at the preference of the respondent.

### 3.3 Confidentiality

If a supplier considers any portion of its response to be proprietary or confidential, the supplier should clearly mark those portions of the response as proprietary or confidential. Canada will treat the responses in accordance with the *Access to Information Act* and any other laws that apply.

## 4. Canada's Review of Responses

### 4.1 Review of Responses

Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify any draft documents provided with this RFI and its procurement strategy. Canada will review all responses received by the RFI closing date and time. Canada may, in its discretion, review responses received after the RFI closing date and time.

### 4.2 Review Team

A review team composed of representatives of Canada will review and consider the responses. Canada may hire any independent consultant(s), or use any Government resource(s), to review any response. Not all members of the review team will necessarily participate in all aspects of the review process.

### 4.3 Follow-up Activity

a) Canada may, in its discretion, contact any suppliers to follow up with additional questions or for clarification of any aspect of a response. Canada's follow-up may involve a request for a further written response or for a meeting with representatives.

# ANNEX A – STATEMENT OF REQUIREMENT

## Smart Card/Token Requirement, Public Key Infrastructure Project

## 1 BACKGROUND

The Directorate of Information Management Engineering and Integration (DIMEI) have been tasked to design, develop, and deploy a Public Key Infrastructure (PKI) within two separate security domains at the Department of National Defence (DND). PKI enablement will be implemented both within applications through digital signature(s) as well as with infrastructure through authentication(s). Email, file encryption and digital signature will be rolled out to users. DND's current solution is based on an Entrust PKI. DND intends to competitively establish a Contract(s), Standing Offer(s) (SO(s)), and/or Supply Arrangement(s) (SA(s)) providing the required PKI hard tokens as and when required. The primary focus will be smart cards, however alternate form factors, such as but not restricted to Universal Serial Bus (USB) tokens and SD cards (Secure Digital Memory Cards) will be considered.

Technical compliance to strong security standards is important to DND. Therefore, a robust and high assurance solution, which establishes a supply of tokens that is not wholly dependent upon a single technology or single Original Equipment Manufacturer (OEM), is required.

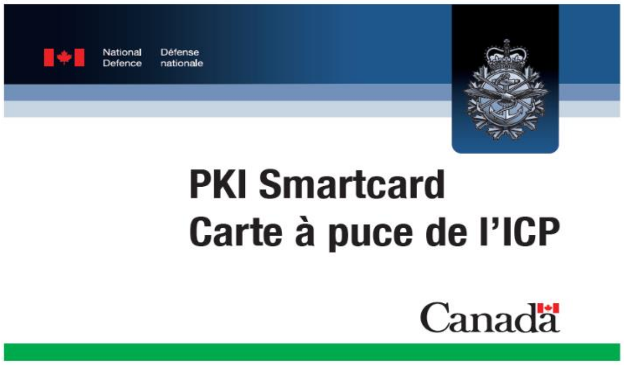
## 2 PURPOSE

The purpose of sharing these graphical specifications and technical requirements prior to any solicitation is to allow industry to provide comprehensive feedback on developed and/or developing specifications. This Request for Information (RFI) should be restricted to token manufacturers who can provide comprehensive feedback on the graphics specifications and technical requirements found below.

## 3 GRAPHICS SPECIFICATIONS

DND has established graphics specifications for the smart card, the primary token form factor. The following image is a sample of the graphics used for smart cards. The graphics for other form factors have not yet been established. Respondents are encouraged to suggest graphics specifications for separate form factors.

### 3.1 Front of Card



### 3.2 Back of Card

**Reminder**
Keep your smartcard secured
Do not leave unattended while in use

If found drop in any Canadian mailbox
K1A 0K2

**Rappel**
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

## 4 TECHNICAL REQUIREMENTS

As part of the evaluation criteria, there may be restrictions on changes that can be made to the underlying infrastructure. The requirements below indicate the environment in which the tokens must be operable.

| No. | Requirement |
|---|---|
| 1 | The token must support Windows 32 bit and 64 bit operating systems and applications. |
| 2 | The token platform must be minimum Federal Information Processing Standard (FIPS) 140-2 Level 2 certified/validated with the physical security at FIPS 140-2 Level 3 or higher. Consideration for equivalent certifications would depend on the ability to map compliance to the FIPS standard. |
| 3 | All applications on the token platform must conform to isolation requirements as defined in the platform guidelines (i.e. [JCS OCPP], GlobalPlatform Security Requirements [GP Security Requirements] and GlobalPlatform Smart Card Security Target Guidelines [GP Sec Target] , EMVCo Java Card & Global Platform Guidelines [EMV JC GP], and [USIM PP]). |
| 4 | The token platform must be certified within either the EMVCo or the CC schemes at the CC EAL4+ level (where the + includes AVA_VAN.5) or the equivalent in EMVCo metrics. |

| No. | Requirement |
|---|---|
| 5 | The token applet has been certified in the contest of the GlobalPlatform Composition Model either using the CC composite evaluation methodology on a CC-certificate platform (see [CC CEval]) or by an EMVCo certification on an EMVCo-certified platform. (where CC CEval is Common Criteria Composite Evaluation and EMVCo is Europay, MasterCard and Visa Compliant) |
| 6 | The token applet(s) must have been verified in the context of the GlobalPlatform Composition Model. |
| 7 | The token must support Elliptic curve cryptography curve p-256. |
| 8 | The token must support Entrust Security Provider 9.3 and later. |
| 9 | The token must be able to hold at least 10 certificates of 2048-bit Rivest-Shamir-Adleman (RSA) keys. |
| 10 | The token must support SHA-1 and SHA-256 hash functions. (Secure Hash Algorithm = SHA) |
| 11 | The token must support the removal of user certificates from the Microsoft Personal certificate store when removed from the reader/system. |
| 12 | The token must support Advanced Encryption Standard (AES) encryption and decryption with 128 bit and 256 bit key lengths. |
| 13 | The token must support Triple Data Encryption Standard(DES) encryption and decryption. |
| 14 | The token 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) for the smart card form factor. |
| 15 | The token must support  Rivest-Shamir-Adleman (RSA) signing and verification with 1024/2048 bit keys. |
| 16 | The token must support RSA encryption and decryption with 1024/2048 bit keys. |
| 17 | The token must support RSA 1024/2048 bit key generation. |
| 18 | The token must support the PIV-C, PIV and PIV-1 standards (Personal Identification Verification Cards).  Clarification of these FIPS 201 standards can be found at: http://www.fips201.com/resources/audio/iab_0810/iab_082510_baldridge.pdf. |
| 19 | The smart card EEPROM must have a minimum of 144 kB capacity (Electrically Erasable Programmable Read Only Memory). |
| 20 | The token EEPROM must support unlimited memory read cycles. |
| 21 | The token EEPROM must support write/erase cycles of 500,000 or more. |

| No. | Requirement |
|---|---|
| 22 | The token EEPROM must have a data retention time of 25 years or more. |
| 23 | The token must support creating, updating and recovering digital certificates when used in combination with Entrust Entelligence Security Provider (ESP) for Windows 9.3, Entrust Identity Guard 12, and Entrust Self Service Module 10.2 Patch 196240. |
| 24 | The token in combination with middleware or native OS capabilities must support logging to various levels for troubleshooting purposes and /or write to Event viewer. |
| 25 | The token must allow forcing users to change Personal Identification Number (PIN) on first-time login. |
| 26 | The token in combination with Entrust Entelligence Security Provider (ESP) for Windows 9.3, Entrust Identity Guard 12 and Entrust Self Service Module 10.2 Patch 196240 must support the following configurable token password policies:<br>a. Minimum character length of 6;<br>b. Maximum character length of 15;<br>c. Must have minimum of 1 Upper case alpha character;<br>d. Must have a minimum of 1 lower case alpha character; and<br>e. Must have 1 numeric value. |
| 27 | The token must support SHA-1 and SHA-256 signed certificates. |
| 28 | The token must support Elliptic Curve Diffie-Hellman key agreement protocol. |
| 29 | The token must utilize mini-drivers included in Microsoft Window 7 and 8. |
| 30 | The token must support storage of a digitally signed facial image. |
| 31 | The token must support storage of a digitally signed fingerprint/iris scan. |
| 32 | The token must have DES, AES, RSA, and ECC co-processors. (Elliptic Curve Cryptography) |
| 33 | The token must be able to pass Supply Chain Integrity (SCI) as defined at: https://www.cse-cst.gc.ca/en/page/technology-supply-chain-guidance. |
| 34 | The token printing must be at 300 dots per inch (dpi) or higher resolution. On contract award, the vendor must submit a final proof for approval prior to production. |
| 35 | On the back of the token, the chip serial number will be printed. |
| 36 | The token chip serial numbers will be sequential. The purpose of sequential serial numbers is to manage inventory and to load batches of tokens into the Credential Management System. |
| 37 | The tokens must be shipped in boxes with the tokens arranged in sequential order. This is necessary to support inventory management and facilitate distributing tokens to operational units. |

## 5 DELIVERY SCHEDULE

The estimated delivery date for the tokens will be on or before 31 March 2018 for the first order.