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 Carte à puce D-PKI	
Solicitation No. - N° de l'invitation W8474-167124/A	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client W8474-167124	**Date** 2015-10-23
GETS Reference No. - N° de référence de SEAG PW-$$QE-071-25431	
File No. - N° de dossier 071qe.W8474-167124	**CCC No./N° CCC - FMS No./N° VME**
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: Munro, Celine	**Buyer Id - Id de l'acheteur** 071qe
Telephone No. - N° de téléphone (819) 956-0586 ( )	**FAX No. - N° de FAX** (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

Modification no. 01 de la solicitation est soumis pour incorporer l’annexe B - Énoncé de travail et l’annexe C - L’évaluation de la comformité technique.

MINISTÈRE DE LA DÉFENSE NATIONALE (MDN)

Énoncé des travaux (ET)
W8474-16-7124/A
13 octobre 2015

Projet de remplacement provisoire de la carte à puce pour l'infrastructure à clés publiques désignée (ICP-D)

pour le

Directeur – Ingénierie et intégration (Gestion de l'information)

Table des matières

1 CONTEXTE

Le Directeur – Ingénierie et intégration (Gestion de l'information) (DIIGI) a reçu comme tâche de mettre à jour et de moderniser l'infrastructure à clés publiques (ICP) existante du ministère de la Défense nationale (MDN). Cette ICP désignée (ICP-D) est utilisée depuis plus de 10 ans par plus de 50 000 utilisateurs. La capacité ICP a été mise en œuvre tant dans les applications (signature numérique) que dans l'infrastructure (authentification). Les fonctions de chiffrement de courriels ou de fichiers et de signature numérique de documents ont été déployées auprès des utilisateurs. Dans ses interactions futures avec ses partenaires au ministère de la Défense américain (DoD), le MDN aura recours à l'ICP pour s'authentifier auprès de leurs ressources. La solution du MDN est basée sur l'ICP d'Entrust.

De nouveaux projets comme celui du Renouvellement du système de pension militaire (RSPM) et du Commandement et contrôle de l'interopérabilité alliée de la Défense (DC2AI) font en sorte que l'ICP-D et le niveau de confiance qu'elle procure doivent être étendus au-delà du MDN et donc à d'autres intranets n'appartenant pas à ce dernier, à savoir ceux d'autres ministères (AM) canadiens et d'alliés ainsi que de l'industrie. Ce faisant, les certificats délivrés par le MDN pourront être reconnus et acceptés par ces organisations externes. Grâce à l'interopérabilité de l'ICP-D, l'accès à l'information et l'échange de celle-ci sont sécurisés avec les organisations externes (p. ex., courriels sécurisés, authentification poussée dans un site Web sécurisé). L'interopérabilité nécessaire à l'externe ne peut être obtenue au moyen de l'ICP-D existante. Un aspect qui requiert une résolution immédiate est lié au remplacement de la carte à puce de l'ICP. En effet, pour soutenir la migration vers le futur algorithme de hachage sécurisé 256 (SHA-2) et pour redresser la situation en raison de la baisse des stocks de la solution actuelle, on doit pouvoir recourir à une carte à puce afin de remplacer celle déjà existante.

2 BESOINS

Les besoins en matière de carte à puce pour l'ICP-D sont fondés sur un certain nombre de composantes préexistantes de l'infrastructure qui sont à la fois matérielles et logicielles. La carte à puce sera utilisée dans un environnement AC Entrust et prendra en charge les utilisateurs actuels. Son impression doit intégrer un graphique précis fourni par le MDN. Les deux sections qui suivent présentent les spécifications liées au graphique et les exigences techniques propres à l'acquisition de la carte.

3 SPÉCIFICATIONS LIÉES AU GRAPHIQUE

Le MDN a établi les spécifications liées au graphique pour la carte à puce. L'image qui suit est le modèle qui sera utilisé. Un fichier graphique dans Adobe Illustrator sera fourni sur demande. Un léger décalage des mots peut être approuvé afin de tenir compte de l'emplacement de la puce intégrée. Le soumissionnaire retenu doit fournir une épreuve qui sera soumise à l'acceptation par le MDN dans le cadre de la demande de propositions.

3.1 Recto de la carte

3.2 Verso de la carte

L'information suivante doit être imprimée au verso de la carte (lettres noires sur fond blanc) :

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

L'espacement des mots peut être ajusté afin que ceux-ci ne se superposent pas au numéro de série de la puce intégrée.

4 EXIGENCES TECHNIQUES

Les besoins en matière de carte à puce pour l'ICP-D sont fondés sur un certain nombre de composantes préexistantes de l'infrastructure qui sont à la fois matérielles et logicielles. La demande de propositions lancée en vue d'acquérir la carte à puce doit donner lieu à une technologie qui peut être intégrée à l'environnement existant. Les spécifications qui suivent représentent l'environnement actuel. La carte à puce proposée doit pouvoir fonctionner dans celui-ci moyennant des changements minimums seulement à apporter à la configuration. Une carte à puce qui nécessite des changements profonds (changements au matériel, aux logiciels ou aux processus) de l'environnement actuel sera jugée non conforme. On considère qu'il s'agit d'un changement minimum à la configuration quand celui-ci a l'une ou plusieurs des particularités suivantes :

a. Changement dont la mise en œuvre coûte moins de 10 000 $;
b. Changement dont le coût de fonctionnement récurrent est de moins de 5000 $ par année; et (ou)
c. Changement dont la mise en œuvre nécessite de la part du MDN moins de deux semaines de travaux d'intégration, et ce, au moyen des ressources existantes au MDN.

Le MDN évaluera quels sont les changements nécessaires et déterminera si ceux-ci sont considérés ou non comme étant « minimums ».

Dans le cadre du processus de demande de soumissions, les entrepreneurs doivent fournir un suivi de la conformité aux spécifications techniques présentées ci-dessous en utilisant le Formulaire de justification de la conformité sur le plan technique joint à la présente DP. Les entrepreneurs verront à joindre à leur soumission cinq (5) cartes à puce (sans frais pour le

gouvernement du Canada) accompagnées de l'information nécessaire afin que le MDN puisse procéder à des essais à l'interne par rapport aux spécifications techniques énoncées dans le tableau. Les entrepreneurs sont aussi invités à fournir un point de contact au sein de leur personnel de soutien à l'ingénierie du produit, si le MDN devait avoir des questions lors des essais effectués à l'interne. Toute assistance portée pendant l'examen et la préparation des essais de validation liés aux exigences seront aux frais du soumissionnaire.

La liste des exigences obligatoires correspond aux essais que le MDN mènera afin de déterminer si la technologie de carte à puce proposée est conforme.

N°	Exigence
1	La carte à puce doit être certifiée/validée au moins de niveau 2 (Level 2) selon la norme 140-2 de la Federal Information Processing Standard (FIPS). Fournir la référence d'un site du National Institute of Standards and Technology (NIST) comme le suivant : http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm où le produit est présenté.
2	La carte à puce doit comporter une mémoire disponible de plus de 48 kilo-octets pour le stockage des certificats une fois que tous les applets et tout fichier nécessaire ont été placés sur le jeton.
3	La carte à puce doit permettre de stocker au moins 10 certificats de clés Rivest-Shamir-Adleman (RSA) à 2048 bits.
4	La carte à puce doit permettre de créer, récupérer et mettre à jour les certificats numériques avec le Service Pack 1 (SP1) d'Entrust Security Manager Administration (SMA) 8.1.
5	La carte à puce doit permettre de créer, récupérer et mettre à jour les certificats numériques avec Entrust Security Provider (ESP) for Windows 9.2 et ESP for Outlook 9.1.
6	La carte à puce doit prendre en charge les versions 32 et 64 bits de Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012.
7	En coordination avec SafeNet Authentication Client (SAC) version 8.2, la carte à puce doit permettre d'établir des connexions selon divers niveaux afin de procéder à du dépannage et (ou) d'écrire dans l'observateur d'événements (Event Viewer).
8	En coordination avec SAC version 8.2, la carte à puce doit permettre de contraindre les utilisateurs à changer leur numéro d'identification personnel (NIP) lorsqu'ils se connectent pour la première fois.
9	En coordination avec SAC version 8.2, la carte à puce doit permettre de supprimer les certificats des utilisateurs du dépôt de l'interface CAPI (Cryptographic Application Programming Interface) lorsque la carte à puce est retirée du lecteur.
10	En conformité avec SAC version 8.2, la carte à puce doit prendre en charge les politiques en matière de mots de passe configurables, soit : a. Longueur minimale de caractères de 6; b. Longueur maximale de caractères de 15; c. Il doit y avoir au moins 1 caractère alphabétique en majuscule; d. Il doit y avoir au moins 1 caractère alphabétique en minuscule; e. Il doit y avoir 1 valeur numérique.
11	La carte à puce doit prendre en charge SHA-1 et SHA-2 pour les signatures numériques. (L'algorithme de hachage sécurisé SHA-1 correspond à une valeur de hachage de 160 bits tandis que la norme SHA-2 avec la valeur de hachage de 256 bits constitue le condensé nécessaire pour la présente demande de soumissions.)
12	En coordination avec SAC version 8.2 et ESP for Windows 9.2, la carte à puce doit prendre en charge les certificats signés SHA-1 et SHA-256.
13	La carte à puce doit prendre en charge la génération de clés RSA à 1024/2048 bits.
14	La carte à puce doit prendre en charge la fonctionnalité de chiffrement sur puce, y compris Advanced Encryption Standard (AES), Triple DES (Data Encryption Standard) et RSA à 1024/2048 bits.

N°	Exigence
15	En coordination avec SAC version 8.2, il doit pouvoir être possible d'initialiser la carte à puce.
16	En coordination avec SAC version 8.2, la carte à puce doit permettre de changer le NIP d'un utilisateur.
17	En coordination avec SAC version 8.2, la carte à puce doit permettre de changer le NIP d'un administrateur/agent de sécurité (admin/AS).
18	La carte à puce doit respecter les spécifications 1 à 4 de la norme 7816 de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI) (spécifications 1 à 4 de la norme ISO/CEI 7816).
19	La carte à puce doit respecter l'approche liée à l'Intégrité de la chaîne d'approvisionnement (ICA) telle qu'elle est définie à l'adresse https://www.cse-cst.gc.ca/fr/page/conseils-chaine-dapprovisionnement-technologies.
20	L'imprimé de la carte à puce doit être de 300 points par pouce (PPP) ou d'une résolution supérieure.

MINISTÈRE DE LA DÉFENSE NATIONALE (MDN)

Formulaire de justification de la conformité sur le plan technique
W8474-16-7124/A
13 octobre 2015

Projet de remplacement provisoire de la carte à puce pour l'infrastructure à clés publiques désignée (ICP-D)

pour le

Directeur – Ingénierie et intégration (Gestion de l'information)

1. OBJECTIF

Ce document décrit le processus d'évaluation des soumissions pour la fourniture de l'ICP - cartes à puce pour le ministère de la Défense nationale.

2. MÉTHODOLOGIE DE L'ÉVALUATION

La soumission recevable avec **le prix le plus bas agrégée** sera recommandée pour attribution d'un contrat unique. Les soumissionnaires doivent fournir une proposition technique et fonctionnelle qui doit décrire en détail la façon dont ils répondent aux critères obligatoires suivants. Les soumissionnaires doivent indiquer où cette information peut être trouvée dans leur proposition.

CANADA EVALUERA UNIQUEMENT LA DOCUMETATION FOURNI AVEC L'OFFRE. LES SOUMISSIONNAIRES DOIVENT FOURNIR LA DOCUMENTATION POUR APPUYER LA CONFORMITE A CHACUN DES CRITERES OBLIGATOIRES.

CANADA NE VA PAS EVALUER L'INFORMATION TELLE LES RENVOIS A DES ADRESSES WEB DE SITE OU DES INFORMATIONS SUPPLEMENTAIRES QUI PEUVENT ETRE TROUVES, OU LES MANUELS OU LES BROCHURES TECHNIQUES PAS FOURNIES AVEC LA SOUMISSION.

LES RÉFÉRENCES DE SITES WEB UTILES PEUT ETRE IMPRIME ET INCLUS DANS LA PROPOSITION POUR SOUTENIR CONFORMITE TECHNIQUE.

Le soumissionnaire doit démontrer la conformité avec les critères suivants. Les soumissionnaires sont priés de remplir le tableau suivant. Le non-respect entraînera le rejet automatique de l'offre.

3. BID MATRIX

Le soumissionnaire doit répondre à toutes les exigences obligatoires identifiées dans le tableau 1 dans leur soumission. Pour faciliter l'examen de l'offre, le soumissionnaire doit soumettre une copie dûment remplie de Tableau 1 - Exigences obligatoires avec soumission de l'offre, afin de valider la conformité.

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	La carte à puce doit être certifiée/validée au moins de niveau 2 (Level 2) selon la norme 140-2 de la Federal Information Processing Standard (FIPS). Fournir la référence d'un site du National Institute of Standards and Technology (NIST) comme le suivant : http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm où le produit est présenté.			
M2	La carte à puce doit comporter une mémoire disponible de plus de 48 kilo-octets pour le stockage des certificats une fois que tous les applets et tout fichier nécessaire ont été placés sur le jeton.			
M3	La carte à puce doit permettre de stocker au moins 10 certificats de clés Rivest-Shamir-Adleman (RSA) à 2048 bits.			
M4	La carte à puce doit permettre de créer, récupérer et mettre à jour les certificats numériques avec le Service Pack 1 (SP1) d'Entrust Security Manager Administration (SMA) 8.1.			
M5	La carte à puce doit permettre de créer, récupérer et mettre à jour les certificats numériques avec Entrust Security Provider (ESP) for Windows 9.2 et ESP for Outlook 9.1.			
M6	La carte à puce doit prendre en charge les versions 32 et 64 bits de Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012.			
M7	En coordination avec SafeNet Authentication Client (SAC) version 8.2, la carte à puce doit permettre d'établir des connexions selon divers niveaux afin de procéder à du dépannage et (ou) d'écrire dans l'observateur d'événements (Event Viewer).			
M8	En coordination avec SAC version 8.2, la carte à puce doit permettre de contraindre les utilisateurs à changer leur numéro d'identification personnel (NIP) lorsqu'ils se connectent pour la première fois.			
M9	En coordination avec SAC version 8.2, la carte à puce doit permettre de supprimer les certificats des utilisateurs du dépôt de l'interface CAPI (Cryptographic Application Programming Interface) lorsque la carte à puce est retirée du lecteur.			

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	En conformité avec SAC version 8.2, la carte à puce doit prendre en charge les politiques en matière de mots de passe configurables, soit : a. Longueur minimale de caractères de 6; b. Longueur maximale de caractères de 15; c. Il doit y avoir au moins 1 caractère alphabétique en majuscule; d. Il doit y avoir au moins 1 caractère alphabétique en minuscule; e. Il doit y avoir 1 valeur numérique.			
M11	La carte à puce doit prendre en charge SHA-1 et SHA-2 pour les signatures numériques. (L'algorithme de hachage sécurisé SHA-1 correspond à une valeur de hachage de 160 bits tandis que la norme SHA-2 avec la valeur de hachage de 256 bits constitue le condensé nécessaire pour la présente demande de soumissions.)			
M12	En coordination avec SAC version 8.2 et ESP for Windows 9.2, la carte à puce doit prendre en charge les certificats signés SHA-1 et SHA-256.			
M13	La carte à puce doit prendre en charge la génération de clés RSA à 1024/2048 bits.			
M14	La carte à puce doit prendre en charge la fonctionnalité de chiffrement sur puce, y compris Advanced Encryption Standard (AES), Triple DES (Data Encryption Standard) et RSA à 1024/2048 bits.			
M15	En coordination avec SAC version 8.2, il doit pouvoir être possible d'initialiser la carte à puce.			
M16	En coordination avec SAC version 8.2, la carte à puce doit permettre de changer le NIP d'un utilisateur.			
M17	En coordination avec SAC version 8.2, la carte à puce doit permettre de changer le NIP d'un administrateur/agent de sécurité (admin/AS).			
M18	La carte à puce doit respecter les spécifications 1 à 4 de la norme 7816 de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI) (spécifications 1 à 4 de la norme ISO/CEI 7816).			
M19	La carte à puce doit respecter l'approche liée à l'Intégrité de la chaîne d'approvisionnement (ICA) telle qu'elle est définie à l'adresse https://www.cse-cst.gc.ca/fr/page/conseils-chaine-dapprovisionnement-technologies.			
M20	L'imprimé de la carte à puce doit être de 300 points par pouce (PPP) ou d'une résolution supérieure.			