SERVICES PARTAGÉS CANADA

Demande de renseignements pour le processus d'approvisionnement concernant le Besoin en matière de cartes à puces / jetons, Projet de l'infrastructure à clés publiques

Demande de renseignements n°	RAS 17-58040 /A	Date	September 1, 2017
Nº de dossier GCDocs	N/A	Nº de référence du SEAOG	PW-17-00793575

Bureau émetteur	Shared Services Canada | Services partagés Canada 180 rue Kent St, Ottawa, Ontario, K1G 4A8 Canada	
Autorité contractante (L'autorité contractante est le représentant de SPC pour tous les commentaires et toutes les questions portant sur ce document.)	Nom	Michelle Marengère
	Nº de téléphone	613-410-9077
	Courriel	Michelle.marengere@canada.ca
	Adresse postale	Shared Services Canada | Services partagés Canada 180 rue Kent St, 13-078 Ottawa, Ontario, K1G 4A8 Canada
Date et heure de clôture	2 octobre 2017 – 11:59 PM	
Fuseau horaire	Heure de l'Est (HE)	
Destination des biens ou des services	Sans objet – Demande de renseignements uniquement	
Courriel auquel la réponse doit être envoyée avant la date de clôture	Michelle.marengere@canada.ca	

TABLE DES MATIÈRES

1. Renseignements généraux

1.1 Introduction

a) **Phase 1 du processus d'approvisionnement :** La présente demande de renseignements constitue la première phase d'un processus d'approvisionnement mené par Services partagés Canada (SPC) concernant **le besoin en matière de cartes à puces / jetons, Projet de l'infrastructure à clés publiques** (le « **Projet** »). Les fournisseurs sont invités à présenter des réponses afin d'aider le gouvernement du Canada à préciser ses exigences concernant le projet. Les fournisseurs ne sont pas tenus de présenter une réponse à la DDR pour pouvoir participer aux phases suivantes du processus d'approvisionnement concernant le projet.

b) **L'étape de la DDR n'est pas une demande de soumissions** : La présente DDR ne constitue pas une demande de soumissions ou un appel d'offres. Aucun contrat ne sera attribué à la suite des activités tenues au cours de la présente DDR. Le gouvernement du Canada se réserve le droit d'annuler toute exigence préliminaire décrite comme faisant partie du projet à tout moment pendant la DDR ou toute autre étape du processus d'approvisionnement. Étant donné que le processus de la DDR et toute activité d'approvisionnement connexe sont susceptibles d'être partiellement ou entièrement annulés par le gouvernement du Canada, l'étape de la DDR peut ne pas aboutir à des processus d'approvisionnements subséquents.

c) **Coûts des réponses** : SPC ne remboursera pas au fournisseur ou à ses représentants les frais généraux ou les dépenses liées à la participation aux activités de l'étape de la DDR. Il leur incombe par ailleurs d'assurer leurs propres recherches indépendantes, processus de diligence raisonnable et enquêtes ainsi que d'obtenir les conseils indépendants qu'ils jugent nécessaires et souhaitables dans le cadre de leur participation au processus de la DDR et au processus d'approvisionnement futur.

1.2 Aperçu du projet

a) **Aperçu du projet** : La Direction de l'ingénierie et de l'intégration (Gestion de l'information) (DIIGI) est chargée de concevoir, de développer et de mettre en œuvre une infrastructure à clés publiques (ICP) dans deux domaines distincts de la sécurité du ministère de la Défense nationale (MDN). La capacité ICP sera mise en œuvre dans les applications (au moyen de signatures numériques) ainsi que dans l'infrastructure (au moyen de mécanismes d'authentification). Les fonctions de chiffrement de courriels ou de fichiers et de signature numérique de documents seront déployées auprès des utilisateurs. La solution actuelle du MDN est fondée sur une ICP Entrust. Le Ministère souhaite établir, en régime de concurrence, un ou plusieurs marchés ou arrangements en matière d'approvisionnement (AMA), de même qu'une ou plusieurs offres à commandes (OAC), pour la fourniture de jetons ICP matériels sur demande, selon les besoins. L'accent sera mis sur les cartes à puces, mais d'autres formats pourraient être envisagés, notamment les jetons USB et les cartes mémoire SD.

La conformité technique à des normes de sécurité solides est importante pour le MDN. Par conséquent, le Ministère exige une solution robuste offrant un niveau d'assurance élevé, permettant d'obtenir une provision de jetons ne dépendant pas entièrement d'une seule technologie ou d'un seul fabricant d'équipement d'origine (FEO).

b) **Portée du processus d'approvisionnement prévu**

i) **Utilisateurs clients potentiels** : La présente DDR est publiée par SPC. SPC prévoit utiliser le ou les contrat(s), offre(s) à commandes ou arrangement (s) en matière d'approvisionnement obtenus à la suite d'une demande de soumission subséquente pour fournir des services partagés à un ou à plusieurs de ses clients. Les clients de SPC comprennent SPC lui-même, les institutions fédérales pour qui ses services sont obligatoires à tout moment pendant la durée de l'instrument subséquent, ainsi que les autres organisations qui, sur une base facultative, choisissent de recourir à ses services de temps en temps, à tout moment pendant la durée de l'instrument subséquent. Tout processus d'approvisionnement subséquent n'empêchera pas SPC d'avoir recours à une autre méthode d'approvisionnement pour ses clients qui ont des besoins identiques ou semblables, à moins qu'une demande de soumission subséquente concernant ce projet indique expressément le contraire.

1.3 Soumission de questions

a) Les questions portant sur la DDR peuvent être envoyées à l'autorité contractante par courriel à l'adresse figurant sur la page de couverture au plus tard **[5]** jours ouvrables avant la date et l'heure limites indiquées sur la page de couverture du présent document. Le gouvernement du Canada peut ne pas répondre aux questions reçues après cette date.

b) Pour garantir l'uniformité et la qualité des renseignements communiqués aux fournisseurs, les questions importantes reçues ainsi que leurs réponses seront publiées dans le Service électronique d'appels d'offres du gouvernement (SEAOG) sous forme d'une modification de la présente DDR.

2. Renseignements demandés par le gouvernement du Canada

2.1 Commentaires au sujet des documents préliminaires

La présente DDR comprend les documents suivants à l'égard desquels le gouvernement du Canada sollicite les commentaires des fournisseurs :

a) Annexe A - Besoin

Tous les documents indiquant les exigences du gouvernement du Canada relatives au présent projet qui sont remis aux fournisseurs au cours du processus de DDR ne sont que des exigences préliminaires ou des ébauches de celles-ci et pourraient changer. Ces exigences, ou une partie de celles-ci pourraient être mises à jour avant ou pendant toute demande de soumissions subséquente.

Les fournisseurs sont invités à formuler des commentaires, à faire part de leurs préoccupations et, le cas échéant, faire des suggestions sur la façon de répondre aux exigences ou d'atteindre les objectifs décrits pour le projet. Les fournisseurs sont également invités à fournir leurs commentaires sur le contenu, la forme et la manière dont l'information est structurée dans les ébauches de documents fournies avec la présente DDR. Les fournisseurs doivent expliquer les hypothèses qu'ils avancent dans leur réponse.

2.2 Réponses aux questions à l'intention de l'industrie

Le gouvernement du Canada demande des réponses aux questions suivantes :

a) Quel produit commercial existant respecte ou surpasse les exigences du MDN visant l'assurance en sécurité?

b) Certains aspects des capacité exigées sont-ils indisponibles ou impossibles dans l'état actuel de la technologie?

c) Existe-t-il d'autres technologies pouvant respecter les exigences du MDN sur l'assurance en sécurité?

d) Vu l'investissement technologique (technologies dorsales), comment les fabricants de jetons ont-ils cherché à intégrer leur technologie aux plateformes actuelles du MDN (autorité de certification et système de gestion des cartes)?

e) Faudrait-il envisager des normes technologies existantes mais ignorées du MDN? Quelles sont-elles et quelle est leur pertinence à l'assurance en sécurité?

f) Quels autres formats (USB, carte à puce, etc.) sont-ils disponibles? Comment ces divers formats peuvent-ils respecter les exigences du MDN visant l'assurance en sécurité? "

3. Réponse des fournisseurs

3.1 Présentation d'une réponse

a) **Date et lieu de présentation des réponses :** Les fournisseurs qui souhaitent fournir une réponse doivent l'envoyer à l'autorité contractante par courriel à l'adresse électronique destinée à la présentation des réponses qui figure sur la page de couverture avant la date et l'heure limites indiquées sur la page de couverture du présent document.

b) **Responsabilités en ce qui a trait à la présentation des réponses dans les délais prescrits :** Il incombe à chaque fournisseur de s'assurer que sa réponse est livrée à la bonne adresse électronique et qu'elle est reçue dans les délais prescrits.

c) **Identification de la réponse** : Chaque fournisseur veillera à ce que son nom, l'adresse de l'expéditeur, le numéro de la demande d'information et la date de clôture apparaissent bien en vue dans la réponse. Le fournisseur doit également désigner un représentant avec lequel le gouvernement du Canada pourra communiquer au sujet de la réponse et indiquer le nom de la personne, son titre, son adresse, son numéro de téléphone et son adresse électronique.

3.2 Langue de la réponse

Les réponses peuvent être fournies en français ou en anglais, au choix du répondant.

3.3 Confidentialité

Si un fournisseur juge que certaines parties de ses réponses sont exclusives ou confidentielles, celles-ci doivent porter clairement la mention exclusive ou confidentielle. Le gouvernement du

Canada traitera les réponses conformément aux dispositions de la *Loi sur l'accès à l'information* et de toute autre loi en vigueur.

4. Examen des réponses par le gouvernement du Canada

4.1 Examen des réponses

Les réponses ne feront pas l'objet d'une évaluation officielle. Toutefois, le gouvernement du Canada pourra utiliser les réponses reçues afin d'élaborer ou de modifier les ébauches de documents fournies avec la DDR ainsi que sa stratégie d'approvisionnement. Le gouvernement du Canada examinera l'ensemble des réponses reçues avant l'heure et la date de la clôture de la DDR. Il peut, à sa discrétion, les examiner après la date de clôture de la DDR.

4.2 Équipe d'examen

Une équipe d'examen composée de représentants du gouvernement du Canada passera en revue et examinera les réponses. Le gouvernement du Canada peut faire appel à ses propres experts-conseils ou personnes-ressources pour examiner les réponses. Les membres de l'équipe d'examen ne participeront pas nécessairement tous à l'ensemble du processus d'examen.

4.3 Activité de suivi

a) Le gouvernement du Canada peut, à sa discrétion, communiquer avec tout fournisseur pour lui poser des questions supplémentaires ou demander des précisions concernant un aspect d'une réponse. Le suivi du gouvernement du Canada peut nécessiter une réponse écrite supplémentaire ou une réunion avec les représentants du gouvernement du Canada.

ANNEX A – BESOIN

Besoin en matière de clés à puces / jetons, Projet de l'infrastructure à clés publiques

1 CONTEXTE

La Direction de l'ingénierie et de l'intégration (Gestion de l'information) (DIIGI) est chargée de concevoir, de développer et de mettre en œuvre une infrastructure à clés publiques (ICP) dans deux domaines distincts de la sécurité du ministère de la Défense nationale (MDN). La capacité ICP sera mise en œuvre dans les applications (au moyen de signatures numériques) ainsi que dans l'infrastructure (au moyen de mécanismes d'authentification). Les fonctions de chiffrement de courriels ou de fichiers et de signature numérique de documents seront déployées auprès des utilisateurs. La solution actuelle du MDN est fondée sur une ICP Entrust. Le Ministère souhaite établir, en régime de concurrence, un ou plusieurs marchés ou arrangements en matière d'approvisionnement (AMA), de même qu'une ou plusieurs offres à commandes (OAC), pour la fourniture de jetons ICP matériels sur demande, selon les besoins. L'accent sera mis sur les cartes à puces, mais d'autres formats pourraient être envisagés, notamment les jetons USB et les cartes mémoire SD.

La conformité technique à des normes de sécurité solides est importante pour le MDN. Par conséquent, le Ministère exige une solution robuste offrant un niveau d'assurance élevé, permettant d'obtenir une provision de jetons ne dépendant pas entièrement d'une seule technologie ou d'un seul fabricant d'équipement d'origine (FEO).

2 NATURE DE LA DDR

Les présentes spécifications graphiques et exigences techniques avant de diffuser des demandes de soumissions sont publiées dans le but de permettre à l'industrie de fournir une rétroaction globale sur lesdites spécifications et exigences, qu'elles soient déjà élaborées ou en cours d'élaboration. La présente demande de renseignements (DR) s'adresse aux fabricants de jetons qui sont aptes à fournir des commentaires exhaustifs sur les spécifications graphiques et les exigences techniques énoncées ci-dessous; elle porte uniquement sur ces deux caractéristiques, et non pas sur les modèles de coûts.

3 SPÉCIFICATIONS GRAPHIQUES

Le MDN a établi les spécifications graphiques applicables aux cartes à puce, le principal format de jeton envisagé. L'image ci-dessous est un exemple des graphiques utilisés pour ce type de jeton. Les graphiques pour les autres formats éventuels n'ont pas encore été établis. On invite toutefois les répondants à proposer des spécifications graphiques distinctes pour chacun des formats potentiels.

3.1 Recto de la carte

3.2 Verso de la carte

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 EXIGENCES TECHNIQUES

En ce qui a trait aux critères d'évaluation, les propositions de modifications à apporter à l'infrastructure sous-jacente pourraient être restreintes. Les exigences énoncées ci-dessous décrivent l'environnement dans lequel les jetons doivent pouvoir fonctionner.

N°	Exigence
1	Le jeton doit prendre en charge les systèmes d'exploitation et les applications 32 bits et 64 bits.
2	La plateforme du jeton doit être certifiée/validée au moins de niveau 2 (Level 2) selon la norme 140-2 de la Federal Information Processing Standard (FIPS). Le niveau de sécurité physique doit être certifié/validé au moins de niveau 3 (Level 3) selon cette même norme. La prise en considération de certifications équivalentes dépendrait de leur conformité à la norme FIPS.

N°	Exigence
3	Toutes les applications de la plateforme du jeton doivent être conformes aux exigences en matière d'isolation définies dans les lignes directrices sur la plateforme (c.-à-d. [JCS OCPP], les exigences de la norme GlobalPlatform en matière de sécurité [GlobalPlatform Security Requirements, ou GP Security Requirements] et les lignes directrices en matière de cible de sécurité des cartes à puce de la norme GlobalPlatform [GlobalPlatform Smart Card Security Target Guidelines, ou GP Sec Target], les lignes directrices de la norme EMVCo relativement aux cartes Java et à la plateforme globale [EMVCo Java Card & Global Platform Guidelines, ou EMV JC GP] et [USIM PP]).
4	La plateforme du jeton doit être certifiée selon les schémas EMVCo ou CC au niveau CC EAL4+ (le signe « + » incluant la norme AVA_VAN.5) ou l'équivalent en mesure EMVCo.
5	L'applet du jeton doit avoir été certifié dans le cadre du modèle de composition GlobalPlatform (GlobalPlatform Composition Model) soit au moyen de la méthodologie d'évaluation composite des critères communs (CC) sur une plateforme certifiée CC (voir [CC CEval]), soit au moyen d'une certification EMVCo effectuée sur une plateforme certifiée EMVCo. (La norme « CC Ceval » signifie « Composite Common Criteria Evaluation » et la norme « EMVCo » signifie « Europay, MasterCard and Visa Compliant ».)
6	Les applets du jeton doivent avoir été vérifiés dans le cadre du modèle de composition GlobalPlatform.
7	Le jeton doit prendre en charge la courbe p-256 en matière de cryptographie à courbe elliptique.
8	Le jeton doit prendre en charge Entrust Security Provider version 9.3 ou ultérieure.
9	Le jeton doit pouvoir contenir au moins 10 certificats de clés RSA (Rivest-Shamir-Adleman) à 2048 bits.
10	Le jeton doit prendre en charge les fonctions de hachage SHA-1 et SHA-256. (L'acronyme SHA signifie « Secure Hash Algorithm ».)
11	Le jeton doit prendre en charge la suppression des certificats des utilisateurs de la banque de certificats personnels de Microsoft lorsqu'il est retiré du lecteur ou du système.
12	Le jeton doit prendre en charge le chiffrement et le déchiffrement AES (norme de chiffrement avancé) avec des clés à 128/256 bits.
13	Le jeton doit prendre en charge le chiffrement et le déchiffrement triple DES.

N°	Exigence
14	Le jeton, sous la forme d'une 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).
15	Le jeton doit prendre en charge la signature et la vérification numériques RSA avec des clés à 1024/2048 bits.
16	Le jeton doit prendre en charge le chiffrement et le déchiffrement RSA avec des clés à 1024/2048 bits.
17	Le jeton doit prendre en charge la génération de clés RSA à 1024/2048 bits.
18	Le jeton doit prendre en charge les normes PIV-C, PIV et PIV-1 (le terme « PIV » correspond à « Personal Identification Verification Cards »). Pour obtenir des clarifications au sujet de ces normes FIPS 201, veuillez consulter le document suivant : http://www.fips201.com/resources/audio/iab_0810/iab_082510_baldridge.pdf.
19	Chaque carte à puce doit comporter une mémoire morte programmable effaçable électriquement (EEPROM) d'au moins 144 Ko.
20	La mémoire morte (EEPROM) du jeton doit prendre en charge un nombre illimité de cycles de lecture.
21	La mémoire morte (EEPROM) du jeton doit prendre en charge au moins 500 000 cycles d'écriture/effacement.
22	La mémoire morte (EEPROM) du jeton doit offrir une période de rétention des données d'au moins 25 ans.
23	Le jeton doit prendre en charge la création, la mise à jour et la récupération de certificats numériques lorsqu'il est utilisé conjointement avec Entrust Entelligence Security Provider (ESP) 9.3 pour Windows, Entrust IdentityGuard 12 et le module Entrust Self-Service Module 10.2, correctif 196240.
24	Le jeton, utilisé conjointement avec un intergiciel ou avec les capacités natives du système d'exploitation, doit prendre en charge la connexion à différents niveaux aux fins de dépannage ou d'écriture dans l'Observateur d'événements.
25	Le jeton doit permettre de forcer les utilisateurs à modifier leur numéro d'identification personnel (NIP) la première fois qu'ils ouvrent une session.

N°	Exigence
26	Le jeton, utilisé conjointement avec Entrust Entelligence Security Provider (ESP) 9.3 pour Windows, Entrust IdentityGuard 12 et le module Entrust Self-Service 10.2, correctif 196240, doit prendre en charge les règles suivantes en matière de configuration du mot de passe du jeton : a) le mot de passe doit être formé d'au moins 6 caractères; b) il ne peut pas compter plus de 15 caractères; c) il doit compter au moins un caractère alphabétique en majuscule; d) il doit compter au moins un caractère alphabétique en minuscule; e) il doit compter au moins une valeur numérique.
27	Le jeton doit prendre en charge les certificats signés SHA-1 et SHA-256.
28	Le jeton doit prendre en charge le protocole d'échange de clés Diffie-Hellman à courbe elliptique.
29	Le jeton doit utiliser les mini-pilotes de Microsoft Windows 7 et 8.
30	Le jeton doit prendre en charge l'entreposage numérique d'une image faciale signée numériquement.
31	Le jeton doit prendre en charge l'entreposage électronique d'empreintes digitales et de l'iris signées numériquement.
32	Le jeton doit être doté de coprocesseurs DES, AES, RSA et ECC. (Chiffrement à courbe elliptique)
33	Le jeton 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.
34	L'imprimé du jeton doit être de 300 points par pouce (PPP) ou d'une résolution supérieure. À l'adjudication du marché, le fournisseur doit présenter une épreuve définitive aux fins d'approbation avant l'envoi à la production.
35	Le numéro de série de la puce sera imprimé au verso du jeton.
36	Les numéros de série des puces des jetons seront séquentiels, afin de faciliter la gestion des stocks et de charger des lots de jetons dans le système de gestion des justificatifs.
37	Les jetons doivent être expédiés dans des boîtes, classés par ordre séquentiel. Cette mesure est nécessaire pour faciliter la gestion des stocks et la distribution des jetons aux unités opérationnelles.

5 CALENDRIER DE LIVRAISON

La date estimative de livraison de la première commande de jetons doit être au plus tard le 31 mars 2018.