Préavis d'adjudication de contrat (PAC)

Un PAC est un avis public informant la collectivité des fournisseurs qu'un ministère ou organisme a l'intention d'attribuer un contrat pour des biens, des services ou des travaux de construction à un fournisseur sélectionné à l'avance, ce qui permet aux autres fournisseurs de signaler leur intérêt à soumissionner en présentant un énoncé des capacités. Si aucun fournisseur ne présente un énoncé des capacités qui satisfait aux exigences établies dans le PAC, au plus tard à la date de clôture indiquée dans le PAC, l'agent de négociation des contrats peut procéder à l'attribution du contrat au fournisseur sélectionné à l'avance.

1. Définition des besoins

L'Agence des services frontaliers du Canada (ASFC) ont besoin d'obtenir deux (2) Golden Reader Tool (GRT) Platinum Edition logicielles pour quatre (4) ans y compris la maintenance et l'assistance, afin d'effectuer une analyse approfondie des circuits intégrés en laboratoire, à l'aide de lecteurs de documents existants (Thales-AT10k and HID-5422).

2. **Critères d'évaluation de l'énoncé des capacités (Exigences essentielles minimales)**

Tout fournisseur intéressé doit démontrer au moyen d'un énoncé des capacités qu'il satisfait aux exigences suivantes :

a. Extraction et affichage des données biométriques trouvées sur la puce, incluant l'information de la ZLM (Zone lisible à la machine) (DG01), la photographie du titulaire (DG02), l'empreinte digitale (DG03 lorsqu'accessible), la signature affichée (DG07) et autres renseignements personnels (DG11, DG12, etc);

b. Affichage du protocole sécuritaire utilisé pour communiquer avec la puce, que ce soit BAC (Basic Access Control) ou PACE (Password Authenticated Connection Establishment), ou que la communication ne soit pas protégée;

c. Affichage de la sécurité anti-clonage effectuée telle que l'authentification active (via DG15) ou l'authentification de puce (via DG14);

d. Affichage en détails des étapes effectuées dans l'authentification passive, incluant la vérification des résultats de hachage de chacun de DG lus, la conformité de la signature électronique (trouvée sur EF.SOD), la comparaison entre les DG alimentés sur EF.COM et ceux alimentés sur EF.SOD, affichage de tous les détails du certificat de signataire de document (DSC), soient les dates de validité, détails sur sujet, détails de l'émetteur, le numéro de série, l'identifiant de clé du sujet (subject key identifier), l'identifiant de clé de l'autorité (Authority key identifier), affichage de tous ces mêmes détails mais pour le certificat du pays signataire (CSCA or Country Signing Certificate Authority) lorsqu'il est disponible, l'algorithme de signature utilisé pour le EF.SOD, pour le certificat de signataire de document (DSC), pour le certificat du pays signataire (CSCA), l'algorithme utilisé pour le hachage des DG alimentés, et finalement l'affichage des données hachées ainsi que la comparaison entre ce résultat et le hachage des données (DG) lues sur la puce généré par le logiciel;

e. Affichage de tous les fichiers trouvés sur la puce, incluant les DG (data groups), EF.COM, EF.SOD, EF.ATR (lorsque présent) et EF.CardAccess (lorsque présent);

f. Possibilité d'extraire le registre de toutes les commandes APDU (Application protocol data unit) entre le lecteur et la puce lorsque requis par l'utilisateur;

g. Possibilité d'utiliser les certificats extraits de ML (Master List) de certificats de pays signataires (CSCA), de listes de révocation publiées telles que celles de l'OACI, ainsi que possibilité d'utilisation de certificats obtenus d'autres sources de confiance dans le format approprié;

h. Possibilité d'extraire soit le fichier complet EF.SOD (en données brutes) ou le certificat de signataire de document (DSC) de la puce.

i. Au minimum le logiciel doit-être disponible dans une des deux langues officielles au Canada (Anglais ou Français);

j. Le logiciel doit nous permettre d'utiliser un ou l'autre de c'est lecteur de puce 3M-Gemalto-Thales ou un HID Omnikey 5422CL;

k. Le support technique doit-être disponible en Français ou en Anglais par courriel et par téléphone;

l. Le logiciel doit-être utilisable même si il n'est pas connecté à internet après son activation; et

m. La méthode d'activation doit nous être fourni par courriel ou par courrier.

2.1. Justification de l'expérience pour l'énoncé des capacités

Les fournisseurs doivent fournir une justification pour chaque exigence d'expérience ci-dessus (article a. à m.). Les fournisseurs doivent fournir un récit (ou une référence à un récit) fournissant une description suffisante, une description du service, de la documentation et/ou d'autres informations nécessaires pour justifier, à la seule satisfaction des évaluateurs gouvernementaux, de la façon dont chaque critère d'expérience est satisfait. Les fournisseurs sont avertis qu'une simple reformulation selon laquelle le fournisseur se conforme à l'exigence ne sera pas considérée comme une justification. Il est recommandé aux fournisseurs de fournir le nom du client et les dates pour lesquelles l'expérience a été acquise.

3. Applicabilité des accords commerciaux à l'achat

Le présent achat n'est assujetti à aucune des accords commerciaux.

4. Justification du recours à un fournisseur sélectionné à l'avance

À la connaissance du Canada, Secunet Security Networks AG est le seul fournisseur qui offre ce service.

5. Exception(s) au Règlement sur les marchés de l'État

L'exception suivante (ou les exceptions suivantes) au *Règlement sur les marchés de l'État* est (sont) invoquée(s) pour cet achat : paragraphe 6d) - « une seule personne est capable d'exécuter le marché ».

6. Période du contrat proposé ou date de livraison

Le contrat proposé est d'une durée de quatre (4) ans sans option pour prolonger.

Date de début estimé : 15 mars 2024
Date d'expiration du contrat estimé : 15 mars 2028

7. Exigences de sécurité

Il n'y a aucune exigence de sécurité associé à ce contrat.

8. Coût estimatif du contrat proposé

La valeur estimée du contrat, est de 16 740,86$ (CDN) (TPS/TVH en sus).

9. Nom et adresse du fournisseur sélectionné à l'avance

Secunet Security Networks AG
Kurfuerstenstasse 58
45138 Essen
Germany

10. Droit des fournisseurs de présenter un énoncé des capacités

Les fournisseurs qui estiment être pleinement qualifiés et prêts à fournir les biens, les services ou des services de construction décrits dans ce PAC peuvent présenter par écrit un énoncé des capacités à la personne-ressource dont le nom figure dans cet avis d'ici la date de clôture, laquelle est aussi précisée dans cet avis. L'énoncé de capacités doit clairement démontrer que le fournisseur satisfait aux exigences publiées.

11. Date de clôture pour la présentation des énoncés des capacités

La date et l'heure de clôture pour l'acceptation d'énoncés des capacités sont 6 mars 2024 à 14h EST.

12. Demande de renseignements et présentation des énoncés des capacités

Les demandes de renseignements et les énoncés des capacités doivent être présentés à :

Autorité Contractante :	Sophia Kuca
Titre :	Agente d'approvisionnement
Adresse :	355 rue North River Ottawa, Ontario K1A 0L8 Canada
Courriel :	CBSA-ASFC_Solicitations-Demandes_de_soumissions@cbsa-asfc.gc.ca