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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet RFI- GIJIA	
Solicitation No. - N° de l'invitation W8474-19AM01/B	**Date** 2019-07-05
Client Reference No. - N° de référence du client W8474-19AM01	**GETS Ref. No. - N° de réf. de SEAG** PW-$$QE-063-27387
File No. - N° de dossier 063qe.W8474-19AM01	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2021-07-02**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Norris, Chantale	**Buyer Id - Id de l'acheteur** 063qe
Telephone No. - N° de téléphone (819) 420-1758 ( )	**FAX No. - N° de FAX** (819) 956-6907
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** Specified Herein Précisé dans les présentes	

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée See Herein	**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

Table des Matières

PARTIE I – INTRODUCTION

Contexte

Le ministère de la Défense nationale (MDN) a mis sur pied le projet de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) afin de fournir au Ministère des services centralisés de gestion de l'identité, des justificatifs et de l'accès.

À l'heure actuelle, les contrôles de l'identité, des justificatifs d'identité et de l'accès du MDN sont fortement cloisonnés et leur gestion, leur surveillance et leur contrôle devraient être centralisés. La situation actuelle est compliquée par les menaces externes permises par l'exposition des réseaux non classifiés du MDN à l'Internet public. La situation actuelle est complexe et insoutenable et expose les opérations du Ministère à un niveau élevé de risque pour la sécurité de l'information.

Objectif de la DDR

Services publics et Approvisionnement Canada (SPAC), au nom du MDN et des Forces armées canadiennes (FAC), publie la présente demande de renseignements (DDR) afin d'informer les membres de l'industrie et d'obtenir des commentaires sur l'approvisionnement prévu et l'établissement des coûts connexes au projet de GIJIA. La présente DDR sera continuellement modifiée pour informer l'industrie sur une base continue des activités de mobilisation de l'industrie et de la rétroaction qui en résulte. En vue de faciliter ce processus, le Canada a l'intention de maintenir la DDR ouverte jusqu'au moment où une demande de propositions (DP) finale sera publiée; par contre, les réponses à la DDR sont requises à la date indiquée au tableau 1 – Dates des activités d'approvisionnement et de mobilisation.

Le processus de DDR et de mobilisation offre aux membres de l'industrie l'occasion de présenter leurs capacités et leurs points de vue relativement aux exigences du Canada pour le projet de GIJIA. Le Canada peut utiliser les informations recueillies pour l'élaboration d'une DP. L'intention est de consulter activement les entreprises pendant tout le processus d'approvisionnement pour assurer une fin de projet réussie.

Processus de consultation et d'approvisionnement envisagé

Le processus de consultation et d'approvisionnement envisagé pour le projet est expliqué en détail à la partie 1 de la présente DDR et consiste en une approche en plusieurs phases, comme illustré ci-dessous. Les exigences en matière de sécurité pourraient être modifiées pendant le processus d'approvisionnement. La décision de mener d'autres activités d'approvisionnement n'a pas encore été prise.

Phase 1

Lettre d'intérêt : Une lettre d'intérêt (LI) pour ce projet a été émise le 7 novembre 2018 et a pris fin le 17 décembre 2018, sous le numéro d'appel d'offres W8474-19AM01/A d'Achatsetventes.gc.ca. Treize entreprises au total ont répondu à la LI. À l'issue du processus, il était évident qu'une DDR plus détaillée était nécessaire.

Demande de renseignements : Une DDR fournira plus de détails à l'industrie. Elle servira de point unique de communication officielle sur le projet avec l'industrie, de façon continue. Essentiellement, elle sollicitera des commentaires détaillés de l'industrie sur les exigences opérationnelles et techniques, les coûts et le calendrier.

Journée de l'industrie non classifiée : Pour présenter un aperçu des exigences et du processus de consultation.

Rencontres individuelles non classifiées : Des rencontres individuelles auront lieu pour discuter de la DDR.

Phase 2

Demande de renseignements : La DDR publiée au cours de la phase 1 demeurera ouverte jusqu'à l'étape de l'ébauche de la DP afin de permettre aux fournisseurs d'obtenir les autorisations de sécurité nécessaires.

Demande de propositions provisoire : Une version provisoire de la demande de propositions pour le projet pourra être transmise aux fournisseurs qui satisfont aux exigences de sécurité pour qu'ils puissent l'examiner et donner leurs impressions. La DP provisoire peut comporter une ou plusieurs annexes classifiées.

Phase 3

Demande de propositions : La version officielle de la demande de propositions pourra être publiée. La DP comportera une ou plusieurs annexes classifiées. Seuls les fournisseurs qui satisfont aux exigences relatives à la sécurité auront accès aux éléments classifiés de la version provisoire de la demande de propositions.

Évaluation : Les soumissions seront évaluées selon les modalités de la DP.

Phase 4

Attribution du contrat : Un ou plus d'un contrat pourrait être attribué au soumissionnaire retenu (ou aux soumissionnaires retenus) conformément aux exigences en matière de sécurité et aux modalités de la DP.

Calendrier d'approvisionnement

Le Canada en est à l'étape préliminaire de ce processus d'approvisionnement éventuel, mais se donne l'objectif de respecter les dates ci-dessous. Les fournisseurs sont priés de noter et de respecter les dates indiquées.

Tableau 1 – Dates des activités d'approvisionnement et de mobilisation

Activité d'approvisionnement et de mobilisation		Date
Parrainage d'autorisation de sécurité*		De la publication de la DDR à la publication de la DP
Phase 1	Lettre d'intérêt	Achevée le 17 décembre 2018
	DDR	Du 5 juillet 2019 à la date de publication de la DP
	• Date limite d'inscription pour assister à la journée de l'industrie	15 juillet 2019
	• Date limite d'inscription pour assister aux rencontres individuelles	15 juillet 2019
	• Journée de l'industrie non classifiée	22 juillet 2019
	• Rencontres individuelles non classifiées	Du 22 au 24 juillet 2019
	• Date de réponse à la DDR	30 août 2019
Phase 2	Version provisoire de la DP	Automne 2021
Phase 3	DP	Été 2022
	Évaluation	Été/automne 2022
Phase 4	Attribution du contrat	Été/automne 2023

* Les exigences en matière de sécurité du projet sont décrites à la section 3 du présent document.

PARTIE II – DEMANDE DE RENSEIGNEMENTS

1. Consignes à suivre pour répondre à la présente demande de renseignements

1.1 Nature de la demande demande de renseignements

On rappelle aux répondants que le document est une demande de renseignements uniquement et non une demande de propositions. Ainsi, les répondants sont invités à présenter leurs commentaires, leurs préoccupations et leurs recommandations quant à la façon de répondre aux exigences ou aux objectifs décrits dans cette DDR. Les répondants sont priés d'expliquer les hypothèses qu'ils avancent dans leur réponse.

Les réponses ne serviront pas à des fins de concours ou d'évaluation comparative et, par conséquent, le format des réponses n'est pas aussi rigoureusement défini qu'il le serait normalement pour une demande de propositions. Cependant, pour faciliter l'examen et pour maximiser la valeur des réponses, le Canada demande que les répondants suivent le format présenté à la section « Format des réponses ».

La participation ou la non-participation à la présente DDR d'un fournisseur potentiel n'empêchera aucunement celui-ci de contribuer à un approvisionnement dans l'avenir. En outre, la présente DDR n'entraînera pas nécessairement l'achat de l'un ou de l'autre des biens et des services qui y sont décrits.

1.2 Coûts associés aux réponses

Le Canada ne remboursera à aucune organisation les dépenses engagées pour répondre à la présente demande de renseignements, y compris les dépenses engagées pour participer aux activités de consultation supplémentaires ou au processus de parrainage en matière de sécurité.

1.3 Traitement des réponses

Utilisation des réponses : Les réponses ne seront pas évaluées. Toutefois, le Canada pourra les utiliser pour élaborer ou modifier son approche à l'égard de l'approvisionnement. Toutes les réponses reçues seront examinées. Cependant, s'il le juge opportun, il peut examiner les réponses reçues après la date de demande de réponse à la DDR.

Équipe d'examen : Une équipe d'examen composée de représentants du MDN et de SPAC examinera les réponses. Le Canada se réserve le droit d'embaucher des experts-conseils indépendants ou d'utiliser des ressources du gouvernement du Canada (GC), s'il le juge nécessaire, pour l'examen des réponses. Tous les membres de l'équipe d'examen n'examineront pas nécessairement toutes les réponses.

Confidentialité : Les répondants doivent indiquer les parties de leur réponse qu'ils jugent de nature exclusive ou confidentielle. Les réponses seront traitées conformément aux dispositions de la *Loi sur l'accès à l'information* (L.R. 1985, ch. A-1), de la *Loi sur la protection des renseignements personnels* (L.R.C. 1985, ch. P-21) et de la *Loi sur la production de défense* (L.R.C. 1985, ch. D-1).

Précisions : À sa discrétion, le Canada peut communiquer avec les répondants pour leur poser des questions additionnelles, obtenir des précisions relativement à tout aspect d'une réponse ou demander qu'une rencontre individuelle ait lieu.

1.4 Exception au titre de la sécurité nationale

Afin de protéger les intérêts de sécurité nationale, le Canada peut invoquer son droit prévu par les accords commerciaux nationaux et internationaux d'utiliser une exception au titre de la sécurité nationale (ESN) pour ce besoin.

L'exception permet au Canada de soustraire l'approvisionnement à certaines ou à l'ensemble des modalités d'un accord commercial pertinent lorsqu'il le juge nécessaire afin de protéger ses intérêts en matière de sécurité nationale ou des intérêts connexes précisés dans le texte des exceptions.

1.5 Nature et format des réponses demandées

Les répondants sont invités à présenter leurs commentaires, leurs préoccupations, et, le cas échéant, des recommandations pertinentes sur la façon de répondre aux besoins définis dans la présente DDR. Ils sont également

invités à fournir leurs commentaires sur le contenu, la forme et la manière dont l'information est structurée dans les documents préliminaires joints à la présente DDR. Les répondants doivent indiquer et expliquer les hypothèses qui ont guidé leurs réponses.

1.6 Contenu de la présente demande de renseignements

L'information contenue dans le présent document demeure un travail en cours et les répondants ne doivent pas présumer que de nouvelles exigences ne seront pas ajoutées à toute demande de soumissions publiée par le Canada ni que des exigences indiquées ici ne seront supprimées ou révisées. Les répondants sont donc invités à faire part de leurs observations sur les exigences de la demande de renseignements. La présente DDR contient également des questions précises adressées à l'industrie.

1.7 Mise en garde relative aux invitations

La présente DDR ne signifie pas que le Canada a pris une décision définitive quant aux possibilités d'approvisionnement. Le MDN et les FAC peuvent décider de ne choisir aucune des solutions ni aucun équipement indiqués dans les réponses. En aucune circonstance le Canada n'aura de responsabilité à l'égard de tout fournisseur qui aura préparé une réponse à la présente DDR.

1.8 Format des réponses

Présentation des réponses L'industrie est invitée à répondre à cette demande de renseignements et à fournir les renseignements suivants au plus tard à la date précisée. Les répondants sont invités à tenir compte des éléments suivants dans leur réponse :

- **Page couverture :** Si la réponse comporte plusieurs documents, les répondants sont priés d'indiquer sur la page couverture de chaque document le titre de la réponse, le numéro de la demande, le numéro du document et le nom officiel complet du répondant.

- **Page titre :** La première page suivant la page couverture doit être une page titre. Celle-ci doit comporter les éléments suivants :
  1) le titre de la réponse et le numéro du document;
  2) le nom et l'adresse du répondant;
  3) le nom, l'adresse et le numéro de téléphone de la personne-ressource du répondant;
  4) la date;
  5) le numéro d'invitation de la demande de renseignements.

- **Mise en page et format de fichier :** Les répondants peuvent utiliser la mise en page de leur choix, mais ils doivent utiliser le modèle d'offres et d'évaluation des prix des produits fourni à l'annexe C et conserver la même numérotation pour faciliter l'examen et l'analyse de toutes les réponses par le Canada. Les réponses doivent être fournies par voie électronique en format MS Word, MS Excel ou PDF. La mise en page de la soumission doit être comme suit :
  1) Section 1 : Sommaire d'une à deux pages maximum, résumant la soumission globale;
  2) Section 2 : Profil de l'entreprise, maximum de deux pages;
  3) Section 3 : Concept de solution proposé, maximum de sept pages (sans compter les tableaux d'établissement des coûts de l'annexe C);
  4) Section 4 : Commentaires généraux et conseils, maximum de 20 pages;

- **Nombre de copies :** Le Canada demande que les répondants présentent leur réponse dans un format non protégé (c'est-à-dire sans mot de passe) MS Word, MS Excel ou PDF par courriel, si la taille du document est inférieure à 5 Mo, à l'adresse suivante : TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Autrement, le Canada demande aux répondants d'enregistrer une copie de leur document PDF (2003 ou version plus récente) sur quatre clés USB et d'envoyer celles-ci par la poste à l'agent de négociation des contrats mentionné à la section 1.9.

1.9 Demandes de renseignements

Toutes les demandes de renseignements et autres communications liées à la présente DDR doivent être transmises directement à l'autorité contractante de Services publics et Approvisionnement Canada (SPAC). Étant donné qu'il ne s'agit pas d'une invitation à soumissionner, le Canada ne répondra pas nécessairement par écrit et ne distribuera pas forcément les réponses aux répondants; néanmoins, les répondants qui ont des questions concernant la présente DDR peuvent les transmettre à : TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Un envoi par la poste est aussi possible :

Services publics et Approvisionnement Canada
Place du Portage, Phase III, bureau 8C2
11, rue Laurier, Gatineau (Québec) K1A 0S5
À l'attention de : Chantale Norris ou Patrick Scott

Les communications par courriel doivent être privilégiées. Veuillez indiquer ce qui suit dans l'objet : **DDR sur la GIJIA**

Les fournisseurs sont invités à soumettre des questions et à formuler des commentaires même s'ils ne participent pas à la Journée de l'industrie ou aux séances individuelles.

1.10 Langue de réponse

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

1.11 Transmission des réponses

Date et lieu de la présentation des réponses : Le Canada demande aux fournisseurs de soumettre leurs réponses au plus tard à la date de réponse à la demande de renseignements indiquée au tableau 1, Dates des activités d'approvisionnement et de consultation.

Identification des réponses : Chaque répondant devrait s'assurer que son nom, son adresse d'expéditeur et le numéro de la demande apparaissent lisiblement sur l'enveloppe contenant la réponse.

Renvoi des réponses : Les réponses à la présente DDR ne seront pas retournées. Les commentaires seront acceptés jusqu'à ce qu'une demande de soumissions soit publiée ou que le besoin soit annulé en tout ou en partie.

2. Objectifs de la présente demande de renseignements

2.1 But

La présente demande de renseignements est publiée avec les principaux objectifs suivants :

- Établir un point unique continu de communication officielle sur le ou les projets avec les fournisseurs éventuels.
- Solliciter des commentaires détaillés de fournisseurs éventuels sur les exigences opérationnelles et techniques, les coûts et le calendrier.
- Conseiller les fournisseurs éventuels au sujet des exigences de sécurité des demandes de propositions et des contrats qui en résultent, et fournir des directives et de l'aide aux fournisseurs qui n'ont pas d'attestation de sécurité pour qu'ils en obtiennent une.
- Solliciter des conseils sur la capacité des entreprises à rédiger la proposition de valeur des retombées industrielles et technologiques par des questions sur leur aptitude à exécuter les travaux de futurs contrats au Canada, à renforcer les chaînes d'approvisionnement canadiennes et à investir à long terme dans le secteur canadien de la TI.

- Répondre aux questions des fournisseurs éventuels lors d'une journée de l'industrie et de rencontres individuelles afin que tous les participants intéressés reçoivent la même information;
- La demande de renseignements restera ouverte jusqu'à la publication d'une demande de propositions formelle à la phase de définition.
- Proposer des coûts et un calendrier non contraignants pour le projet à titre indicatif.

- Informer les entreprises du mode d'approvisionnement proposé.
- Fixer les conditions des activités de suivi du projet.

3. Sécurité

3.1 Renseignements

L'un des principaux objectifs de la présente demande de renseignements est d'informer les fournisseurs des exigences en matière de sécurité associées aux diverses activités d'approvisionnement et de consultation et de permettre aux fournisseurs qui n'ont pas d'attestation de sécurité de demander à SPAC de les parrainer pour l'obtenir afin de pouvoir participer. Le Canada a l'intention de maintenir la demande de renseignements ouverte jusqu'à ce qu'une demande de renseignements soit publiée pour informer les fournisseurs des exigences en matière de sécurité et les parrainer auprès de la Direction de la sécurité industrielle canadienne (DSIC). SPAC cessera de parrainer l'obtention d'autorisations de sécurité lors de la publication de la DP finale. De plus, il ne retardera pas la publication ou la clôture d'une DP pour laisser aux fournisseurs le temps d'obtenir l'attestation de sécurité requise.

Pour en savoir plus sur les enquêtes de sécurité réalisées sur le personnel et les entreprises, ainsi que sur les clauses de sécurité, les soumissionnaires sont invités à consulter le site Web du Programme de sécurité des contrats de TPSGC (https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

3.2 Exigences en matière de sécurité de la GIJIA

Il est possible que les exigences en matière de sécurité suivantes s'appliquent à la demande de propositions provisoire, à la demande de propositions et au contrat :

Les fournisseurs intéressés pourraient être tenu de détenir une attestation de sécurité d'installation (ASI) valide de niveau SECRET et une autorisation de détenir des renseignements approuvée de niveau SECRET, ainsi que de fournir des membres du personnel qui détiennent des attestations de sécurité SECRET et sont citoyens du Canada et des États-Unis seulement.

Il est possible que les demandes de propositions provisoire et finale ainsi que les contrats qui en découleront nécessitent l'accès à des marchandises contrôlées. Avant d'obtenir l'accès, l'entrepreneur doit être inscrit au Programme des marchandises contrôlées de Travaux publics et Services gouvernementaux Canada (TPSGC).

Les attestations de sécurité doivent être délivrées par la Direction de la sécurité industrielle canadienne (DSIC) de SPAC. La Direction de la sécurité industrielle internationale (DSII) confirmera l'habilitation de sécurité des fournisseurs étrangers par l'entremise de leurs propres programmes nationaux de sécurité industrielle. Veuillez noter que les activités d'approvisionnement proposées au-delà de la demande de renseignements initiale ne peuvent faire l'objet que de discussions et peuvent être modifiées à tout moment. La décision de mener d'autres activités d'approvisionnement n'a pas encore été prise.

3.3 Parrainage d'autorisation de sécurité

Comme les exigences en matière de sécurité de la demande de proposition provisoire, de la demande de propositions et du contrat ne sont pas encore définitives, le Canada peut parrainer à une date ultérieure les fournisseurs intéressés ou les fournisseurs potentiels qui ne détiennent pas encore les autorisations escomptées. Si le Canada choisit de parrainer des fournisseurs, cette demande de renseignements sera modifiée pour ajouter la Liste de vérification des exigences relatives à la sécurité (LVERS) et les clauses de sécurité connexes. Les fournisseurs intéressés sont encouragés à amorcer le processus d'autorisation de sécurité dès que les exigences en matière de sécurité seront définitives. Le processus de demande de parrainage se trouve à l'annexe F. Il incombe au fournisseur de veiller à ce que l'information requise concernant l'autorisation de sécurité soit communiquée à temps à l'autorité contractante ou à la Direction de la sécurité industrielle canadienne (DSIC).

Nous invitons les soumissionnaires à présenter rapidement leurs demandes de cote de sécurité. Les fournisseurs sont également vivement encouragés à soumettre des demandes d'attestation de sécurité pour tous leurs principaux employés qui pourraient avoir besoin d'accéder à des renseignements de nature délicate ou d'accéder à des sites sécurisés au cours de toute phase du projet, en commençant par l'engagement actuel de l'industrie jusqu'à l'attribution et l'exécution du contrat.

Des processus semblables, à quelques différences près, s'appliquent à tous les pays avec lesquels le Canada a signé des instruments de sécurité bilatéraux. Nous encourageons les fournisseurs étrangers à déterminer quelles sont les exigences dans leur pays visant les programmes de sécurité industrielle, pour découvrir s'ils peuvent satisfaire à ces exigences, et quelles sont les procédures précises qui pourraient s'appliquer dans leur pays. Comme susmentionné, il est fortement recommandé de s'inscrire le plus tôt possible.

On ne retardera pas les activités de consultation et d'approvisionnement qui en résultent afin de laisser aux fournisseurs le temps d'obtenir les attestations de sécurité exigées.

4. Politique des retombées industrielles et technologiques (RIT)

La Politique des RIT, y compris la proposition de valeur, peut s'appliquer au projet de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA). Dans le cadre d'une demande de renseignements, la participation de l'industrie aidera à déterminer comment appliquer la Politique et la façon dont le Canada pourrait tirer profit des avantages économiques grâce à l'approvisionnement en question au moyen de la proposition de valeur. Les fournisseurs auront l'occasion de discuter de la politique des RIT, de la proposition de valeur et de la façon dont celles-ci pourraient s'appliquer à cet approvisionnement au cours de réunions individuelles tenues après la Journée de l'industrie.

5. Langues officielles

Tout marché éventuel pour une solution à ce projet exigera que l'entrepreneur fournisse tous les documents, le soutien technique et le soutien au client dans les deux langues officielles.

6. Mode de consultation

Le processus de consultation des entreprises a commencé par une lettre d'intérêt et se terminera lorsque des demandes de propositions verront le jour ou lorsque le Canada informera les fournisseurs d'une autre manière que le processus est terminé. Comme les documents définitifs liés à l'invitation seront peut-être classifiés, ils pourraient ne pas être accessibles au public. Soyez avisé que le mode de consultation et les activités d'approvisionnement proposés au-delà de la demande de renseignements initiale ne peuvent faire l'objet que de discussions et peuvent être modifiés à tout moment. La décision de mener d'autres activités d'approvisionnement n'a pas encore été prise.

Les fournisseurs qui désirent participer à l'une ou l'autre des activités de consultation sont invités à consulter les règles indiquées à l'annexe D.

Le Canada a l'intention d'adopter l'approche progressive suivante pour la consultation des entreprises :

Activités de la phase 1

Lettre d'intérêt (terminée)

Demande de renseignements : La présente DDR vise à fournir plus de détails à l'industrie quant au besoin du MDN en matière de GIJIA. Elle servira de point unique de communication officielle sur le projet avec l'industrie, de façon continue.

Journée de l'industrie non classifiée : Une journée de l'industrie non classifiée aura lieu à la salle Palladium, au 3e étage du Mess des caporaux et soldats du Canal Rideau situé au 4, promenade de la Reine-Elizabeth, à Ottawa, en Ontario. L'objectif de la journée est de présenter aux représentants de l'industrie inscrits les grandes lignes du processus d'approvisionnement, de la consultation effectuée auprès des entreprises, des exigences de sécurité et du contenu non classifié du projet. Cette journée vise à offrir une tribune où le Canada pourra faire connaître ses besoins à un haut niveau, et où l'industrie pourra poser des questions et recueillir de l'information afin de bien comprendre le besoin. En plus de l'événement en direct, la journée de l'industrie sera présentée sur WebEx.

L'ordre du jour de la journée de l'industrie va comme suit :

1. Mot d'ouverture;
2. Processus d'approvisionnement – Mode de consultation;
3. Politique des retombées industrielles et technologiques;
4. Sécurité;
5. Marchandises Controlées
6. Aperçu du projet
7. Période de questions

Les documents suivants seront remis aux participants à la journée de l'industrie :

a. Ordre du jour
b. Exemplaires du document de présentation

Rencontres individuelles : Le Canada pourra tenir des consultations individuelles avec les fournisseurs inscrits. Ces réunions ne seront pas classifiées et auront lieu à la salle Athena, au 3e étage du Mess des caporaux et soldats du Canal Rideau situé au 4, promenade de la Reine-Elizabeth, à Ottawa, en Ontario. Les fournisseurs qui demandent une rencontre obtiendront des renseignements supplémentaires et devront déterminer des dates possibles dans la fenêtre proposée pour rencontrer des représentants du Canada. Le Canada lui confirmera alors l'une des dates demandées ou encore lui en suggérera une autre. Les dates de réunion seront attribuées suivant le principe du « premier arrivé, premier servi ».

Toutes les consultations individuelles avec les fournisseurs seront terminées avant la date de réponse demandée de la DDR. Le Canada peut demander la tenue de consultations individuelles avec des fournisseurs en tout temps pendant ou après la date de réponse demandée pour obtenir des précisions sur les commentaires reçus.

Activités de la phase 2

Demande de renseignements : La DDR publiée au cours de la phase 1 demeurera ouverte jusqu'à l'étape de l'ébauche de la DP afin de permettre aux fournisseurs d'obtenir les autorisations de sécurité nécessaires.

Demande de propositions provisoire : Une version provisoire de la demande de propositions pour le projet pourra être transmise aux fournisseurs qui satisfont aux exigences de sécurité pour qu'ils puissent l'examiner et donner leurs impressions. La DP provisoire comportera une ou plusieurs annexes classifiées.

Phase 3

Demande de propositions : La version officielle de la demande de propositions pourra être publiée. La DP peut comporter une ou plusieurs annexes classifiées. Seuls les fournisseurs qui satisfont aux exigences relatives à la sécurité auront accès aux éléments classifiés de la version provisoire de la demande de propositions.

Évaluation : Les soumissions seront évaluées selon les modalités de la DP.

Phase 4

Attribution du contrat : Un ou plus d'un contrat pourrait être attribué au soumissionnaire retenu (ou aux soumissionnaires retenus) conformément aux exigences en matière de sécurité et aux modalités de la DP.

7. DEMANDES DE RENSEIGNEMENTS PAR LE CANADA

7.1 Documents d'intérêt

Les documents suivants, pour lesquels le Canada cherche à obtenir des commentaires des entreprises, sont joints à la présente demande de renseignements :

- Annexe A, Contexte du projet et énoncé des besoins opérationnels préliminaire;
- Annexe B, Description des systèmes et de l'architecture (actuels et futurs);
- Annexe C, Modèle d'offres et d'évaluation des prix des produits;

L'information contenue dans le présent document en est au stade préliminaire et demeure un travail en cours, et les répondants ne doivent pas présumer que de nouvelles exigences ne seront pas ajoutées à toute demande de soumissions publiée par le Canada. Il se peut également que des exigences soient retirées ou modifiées. Les répondants sont toutefois invités à formuler des commentaires sur n'importe quel élément des documents préliminaires.

7.2 Document d'orientation et d'inscription

Les annexes suivantes fournissent des conseils supplémentaires sur la façon de répondre à la présente DR, les règles relatives à l'engagement et le processus d'inscription pour les réunions :

- Annexe D, Règles d'engagement;
- Annexe E, Processus d'inscription à la journée de l'industrie et aux rencontres individuelles;
- Annexe F, Demande de parrainage de sécurité

7.3 Invitation à répondre

Tous les répondants intéressés sont invités à fournir une soumission écrite qui comprend notamment ce qui suit :

a. Une description des solutions et des produits proposés couvrant l'ensemble ou certains des composants fonctionnels théoriques décrits à l'annexe B dans la vision architecturale des composants théoriques;
b. Les prix indicatifs, la structure de répartition du travail et la planification des produits et solutions proposés, y compris les tâches d'intégration, d'installation, de configuration, de mise à l'essai et de formation liées à ces derniers;
c. Les prix indicatifs et le calendrier du soutien en service et des tâches d'entretien continu;
d. L'approche d'approvisionnement proposée avec des recommandations pour l'approvisionnement concurrentiel, les critères de sélection et la base de paiement; et
e. Des recommandations ou conseils additionnels concernant les exigences et les plans du projet.

7.4. Demande de renseignements

Le Canada demande des réponses comme suit, qui respectent le format décrit à la section 1.8 :

Section 1 – Sommaire :

Les répondants sont priés de fournir ce qui suit :

1) un résumé de la soumission du répondant.

Section 2 – Profil de l'entreprise :

Les répondants sont priés de fournir ce qui suit :

1) Donnez une brève introduction et une description des capacités de l'entreprise, en soulignant les produits, les services et les capacités basées au Canada ainsi que l'expérience dans la prestation de solutions de GIJIA pertinentes aux objectifs du projet. En ce qui concerne la fourniture de solutions de GIJIA, veuillez préciser ce qui suit, le cas échéant :
    a. Si vous avez de l'expérience en fourniture de solutions de GIJIA auprès d'organisations comptant plus de 25 000 utilisateurs répartis dans des complexes géographiquement très éloignés.
    b. Si vous avez de l'expérience acquise en prestation de services de GIJIA dans un environnement classifié.
2) Expliquez brièvement la fonction que vous vous attribuez (intégration de systèmes, fourniture de composantes, installation sur place, vérification et validation, formation, soutien en service, etc.) ainsi que l'expérience acquise et donnez des exemples de projets ou de contrats (maximum de trois exemples par fonction, le cas échéant), les noms et types de clients inclus (entreprise privée, organisme public).
3) Décrivez les partenariats établis avec d'autres entreprises, le cas échéant, qui seraient profitables pour réaliser les exigences du projet.
4) Indiquez le niveau d'habilitation de sécurité de votre organisation (s'il y a lieu), y compris l'attestation de sécurité d'installation (ASI), l'enregistrement des marchandises contrôlées et toute autorisation de détenir des renseignements (ADR); et

5) Décrivez les principales hypothèses, contraintes, préoccupations, conclusions et recommandations dont, selon vous, le Canada devrait tenir compte afin que le projet évalue les différentes options.

Section 3 – Concept de solution proposé.

Les répondants sont priés de fournir ce qui suit:

1. Aperçu du plan de solution – Un aperçu du concept, de la structure de répartition générale du travail et d'un calendrier pour un produit livrable ou tous les produits livrables définis à l'annexe B que le répondant prévoit fournir, décrivant les principaux produits et composants, le logiciel, le matériel, les services techniques, la formation et le soutien en service. Dans le contexte des renseignements contenus dans l'annexe B, les soumissionnaires devraient :
   i. fournir une description de leur vision de la ou des solutions proposées pour l'année 2025 qui répondraient à toutes les exigences et les capacités du projet ou à une partie d'entre elles, comme décrit dans la section portant sur l'architecture future de la GIJIA de l'annexe B;
   ii. fournir une description de la manière dont les caractéristiques et les capacités proposées de leur système proposé respecteraient ou dépasseraient les exigences énoncées dans l'annexe B (veuillez noter que les fournisseurs peuvent proposer des solutions qui ne sont pas nécessairement conformes aux composants décrits à la section portant sur l'architecture future de la GIJIA de l'annexe B, à condition que l'ensemble de la solution réponde aux exigences);
   iii. fournir des recommandations et de brèves justifications concernant les ensembles de capacités du projet proposé;
   iv. fournir des recommandations et de brèves justifications concernant les parties des capacités de GIJIA qui nécessiteront l'équipement matériel du MDN/FAC;
   v. formuler des recommandations et de brèves justifications concernant les parties des capacités de GIJIA que les FAC du MDN devraient mettre en œuvre à l'interne dans le cadre de la solution globale;
   vi. formuler des recommandations et de brèves justifications concernant les parties des capacités de GIJIA qui nécessiteront du soutien en service offert par l'industrie;
   vii. fournir des recommandations et de brèves justifications concernant les parties des capacités de GIJIA qui nécessiteront de la formation offerte par l'industrie;
   viii. préciser leur approche en matière d'innovation, en vue de maintenir la pertinence des capacités tout au long du cycle de vie, et décrire comment la solution proposée permet d'atteindre la capacité souhaitée indiquée à l'annexe B;
   ix. indiquer le degré de modularité déployable de leur solution et de ses composants;
   x. indiquer l'évolutivité de leurs solutions pour répondre aux plus grands besoins opérationnels de tout au plus 50 000 utilisateurs, avec un potentiel de croissance annuelle des données de trente pour cent (30 %) par an;
   xi. fournir des détails sur le déploiement de la solution, y compris les approches progressives, l'élaboration, les mises à l'essai, la mise en œuvre, la formation et les mises à niveau;
   xii. préciser, au moyen d'informations historiques, la fiabilité et la disponibilité des produits, des sous-systèmes et des systèmes;
   xiii. indiquer les risques d'ordre technique et liés à la gestion, à la formation, à la sécurité, au soutien et au calendrier cernés. Préciser les mesures d'atténuation. (Remarque : Si un risque peut être atténué en modifiant les politiques existantes, les CONOPS ou l'architecture, le fournisseur doit se sentir libre de recommander une telle stratégie d'atténuation);
   xiv. fournir des fiches techniques pertinentes pour les solutions et les produits et solutions proposées, si elles existent et n'ont pas déjà été fournies.

2. Plan détaillé de haut niveau et séquence d'événements – Un plan et un calendrier indicatifs du projet (mesuré en mois après l'attribution du contrat) pour la livraison de tout produit ou de tous les produits livrables définis à l'annexe C que le répondant a l'intention de fournir.

3. Les coûts estimés pour chaque livrable – Une estimation de coût indicative, avec une description par unité, s'il y a lieu, pour tout produit ou tous les produits livrables définis à l'annexe C que le répondant a l'intention de fournir. L'objectif est d'estimer en toute confiance le coût total de possession sur la durée de vie de la capacité. Pour ce faire, le fournisseur doit présenter un aperçu afin que les coûts de développement, de mise à l'essai, de déploiement, de soutien et de mise à niveau, y compris les coûts récurrents et non récurrents, soient clairement identifiés et répartis pour l'ensemble du cycle de vie. En complétant le modèle

de données sur les coûts fourni à l'annexe C, les répondants sont invités à indiquer clairement comment chaque produit livrable est fourni avec ses coûts annuels estimés de soutien en service. Les coûts de soutien en service devraient comprendre des informations détaillées telles que le nombre d'employés nécessaires à l'implantation de la solution. Par exemple, si la livraison d'une capacité nécessite des unités matérielles et logicielles discrètes, du personnel de soutien ou du personnel du centre d'opérations, les fournisseurs doivent clairement l'indiquer dans la base de coûts unitaires, le prix par unité ou le nombre d'unités requis. À tout le moins, la réponse doit indiquer que le coût de la solution se calcule facilement à l'aide du modèle simple suivant : *Coût = prix / unité x nombre d'unités.* Il en va de même pour les tâches telles que les solutions d'ingénierie, pour lesquelles la réponse doit indiquer le coût en fonction du modèle suivant : *Coût = niveau d'effort (jours) x prix/personne (par jour) x nombre de personnes requises*.

Section 4 – Commentaires et conseils généraux.

Les répondants sont invités à fournir des commentaires, des remarques et des conseils concernant ce qui suit :

1) Les objectifs de rendement, les exigences opérationnelles ou les composants fonctionnels théoriques décrits à l'annexe A.
2) Les capacités actuelles décrites à l'annexe B, y compris les structures organisationnelles des unités opérationnelles.
3) L'amélioration des descriptions de projets, des objectifs, de la gestion et des approches d'approvisionnement pour rehausser l'efficacité globale de la mise en œuvre.
4) Solutions proposées :
    i. La ou les solutions proposées répondent-elles à toutes les exigences pertinentes?
    ii. Énumérez les composants libres ou les composants de tiers (fournisseurs), disponibles sur le marché, qui doivent être intégrés à la solution proposée pour la rendre complète.
    iii. Comment la ou les solutions proposées, y compris certains composants libres ou de tiers, disponibles sur le marché, s'intègrent-elles et interopèrent-elles dans un environnement technologique diversifié? La solution proposée prévoit-elle de réutiliser et d'intégrer les composants existants du MDN ou des FAC?
    iv. Les composants de la solution proposée seront-ils rendus inefficaces dans un environnement à bande passante déconnectée, intermittente et faible, et dans quelle mesure les interruptions peuvent-elles être récupérées? Que propose-t-on comme solutions de rechange pouvant apporter du soutien dans un environnement à bande passante déconnectée, intermittente et à faible, et quels sont les coûts associés?
    v. S'il y a lieu, le MDN ou les FAC pourraient-ils obtenir des licences de démonstration des composants des solutions proposées pour son environnement d'essai et d'évaluation?
5) Sécurité et intégrité de la chaîne d'approvisionnement
    i. Références :
        a. https://www.cse-cst.gc.ca/fr/page/conseils-chaine-dapprovisionnement-technologies
        b. https://www.cse-cst.gc.ca/fr/node/300/html/25733
        c. https://www.cse-cst.gc.ca/fr/node/299/html/25729
    ii. Le Centre de la sécurité des télécommunications Canada offre au gouvernement du Canada des conseils et des directives en matière de sécurité des TI sur les menaces et les vulnérabilités de la chaîne d'approvisionnement, ainsi que des conseils sur la prévention et l'atténuation des risques.
    iii. Les Clauses contractuelles visant l'équipement et les services de télécommunications (TSCG-01\L) contiennent des clauses de sécurité qui peuvent être incluses dans les contrats de SPAC dans le but de prévenir ou d'atténuer les risques de la chaîne d'approvisionnement pour les réseaux de communications et l'infrastructure de TI du gouvernement du Canada, ce qu'on appelle souvent l'intégrité de la chaîne d'approvisionnement.
    iv. Les clauses sont fondées sur un scénario de services de télécommunications gérés dans lequel un entrepreneur est chargé de choisir, de mettre en œuvre, d'exploiter et d'entretenir l'infrastructure et les services de télécommunications pour les clients du gouvernement du Canada. Certaines de ces clauses s'appliquent également à l'acquisition de solutions informatiques ou de matériel/équipement. Les lignes directrices définissent un processus de sélection et d'adaptation de clauses (coût, calendrier et exigences, par exemple).
    v. Le dépliant Clauses contractuelles visant l'équipement et les services de télécommunications (TSCG-01\L) décrit le but des clauses regroupées et en fait une brève description.

vi. Question : Comment ces clauses contractuelles pourraient-elles influer sur le coût, le calendrier et la conception de la solution proposée? De quelles informations supplémentaires votre entreprise aurait-elle besoin pour mieux gérer les risques de coût, de calendrier et de conception imposés par les restrictions à l'intégrité de la chaîne d'approvisionnement?

6) Tout autre sujet de préoccupation ou conseil qui aiderait à fournir une recommandation d'amélioration pour la définition des projets et leur mise en œuvre.

Appendice 1 de la DDR

CABA	Contrôle d'accès basé sur les attributs
CA	Contrôle de l'accès
LCA	Listes de contrôle d'accès
SCA	Système de contrôle d'accès
SMA(GI)	Sous-ministre adjoint (Gestion de l'information)
API	Interface de programmation d'applications
NMPO	Notation de modélisation des processus opérationnels
AE	Approche globale
FAC	Forces armées canadiennes
DSIC	Direction de la sécurité industrielle canadienne
CIV	Civil
CONOPS	Concept d'opération
PRODUIT COMMERCIAL	Produit du commerce
CSTC	Centre de la sécurité des télécommunications
IRSC	Infrastructure des réseaux secrets consolidés
CSV	Valeurs séparées par des virgules
DIIGI	Directeur –Ingénierie et intégration (Gestion de l'information)
DMN	Modèle de décision et notation
MDN	Ministère de la Défense nationale
RED-ICP	RED – Infrastructure à clés privées
RED	Réseau étendu de la Défense
RED-ICP	Infrastructure à clés publiques du RED
SGAE	Service de gouvernance de l'accès d'entreprise
SAFE	Service d'authentification fédérée d'entreprise
SAGE	Service d'accès de gouvernance d'entreprise
SDIE	Service de données d'identité d'entreprise
ACS+	Analyse comparative entre les sexes plus
GC	Gouvernement du Canada
GOTS	Gouvernemental standard
SGRH	Système de gestion des ressources humaines
HTTP	Protocole de transfert hypertexte

GJIIA	Gestion de l’identité, des justificatifs d’identité et de l’accès
ID	Identité
SGI	Système de gestion de l’identité
DSII	Direction de la sécurité industrielle internationale
SES	Soutien en service
TI	Technologie de l’information
RIT	Retombées industrielles et technologiques
BDITI	Bibliothèque de données sur l’infrastructure des technologies de l’information
GSTI	Gestion des services en technologie de l’information
RL ou LAN	Réseau local
LDAP	Protocole allégé d’accès annuaire
NA	Niveau d’assurance
LI	Lettre d’intérêt
MOTS	Militaire standard
MS	Microsoft
OTAN	Organisation du Traité de l’Atlantique Nord
ESN	Exception au titre de la sécurité nationale
NTLM	Protocole NTLM (NT LAN Manager)
AUTHO	Authentification ouverte
AMOG	Autres ministères et organismes gouvernementaux
OIDC	Protocole de couche d’identification OpenID Connect
EOE	Essai opérationnel et évaluation
SCAP	Système de contrôle de l’accès physique
PDF	Format de document portable
PDP	Point de décision politique
PAP	Point d’application de politique
PII	Informations personnelles identifiables
NIP	Numéro d’identification personnel
PIP	Point d’information de politique
ICP	Infrastructure à clés publiques
SPAC	Services publics et Approvisionnement Canada
CABR	Contrôle d’accès basé sur les rôles
SGBDR	Système de gestion de bases de données relationnelles

TER	Transfert d'état représentationnel
DP	Demande de proposition
DDR	Demande de renseignements
ÉSA	Évaluation de la sécurité et autorisation
GEAS	Guide sur l'évaluation et l'autorisation de sécurité
SAML	Langage de balisage des assertions de sécurité
SCIM	Système de gestion des identités interdomaines
CCS	Caractéristiques de conception d'un système
PS	Plan de la systémique
EIS	Exigences d'interface du système
RT	Répartition des tâches
ICP-S	Infrastructure à clés publiques – Secret
PEU	Procédures d'exploitation uniformisées
SQL	Langage d'interrogation structuré
DES	Document sur les exigences du système
STANAG	Accord de normalisation OTAN
EMR	Évaluation des menaces et des risques
USB	Bus série universel (Universal Serial Bus)
PV	Proposition de valeur
RPV	Réseau privé virtuel
V et V	Vérification et validation
WS-Fed	Fédération des services Web
XACML	Langage de balisage de contrôle d'accès extensible

ANNEXE A

ÉNONCÉ PRÉLIMINAIRE DES BESOINS OPÉRATIONNELS

Contexte sur la capacité en gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)

Le projet de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) du ministère de la Défense nationale (MDN), qui se déroulera entre 2018 et 2027, vise à concevoir et à fournir des capacités interopérables et fédérées de GIJIA en vue de gérer, de surveiller et de contrôler de façon centralisée les identités, les comptes utilisateurs et les justificatifs. Ces capacités de GIJIA amélioreront la productivité et la sécurité des ressources ministérielles et permettront au Ministère de respecter les politiques gouvernementales en matière de protection des renseignements personnels.

Le maintien de l'approche actuelle de la GIJIA, qui est disséminée, déconnectée et peu automatisée, limiterait la protection des biens, ralentirait la capacité des utilisateurs à accéder aux ressources, entraverait la prise de décisions concernant l'octroi et la révocation des droits d'accès et augmenterait le risque de perte, de dommage ou de compromission des biens du Ministère.

Le MDN a établi qu'il doit moderniser et améliorer l'interopérabilité, l'exactitude et la confidentialité de ses données d'identité et de ses justificatifs, de même que de ses contrôles d'accès aux installations physiques, à l'information et aux systèmes d'information. À l'heure actuelle, le MDN traite avec de multiples sources d'information non coordonnées sur l'identité et les justificatifs, qui sont reproduites de nombreuses fois.

Le projet de GIJIA permettra aux propriétaires de biens de générer rapidement et en toute sécurité des justificatifs d'identité pour les utilisateurs et de résoudre les questions liées aux décisions d'accès au moyen d'une identité numérique unique, fournie par un service d'identité géré de manière centralisée. Des processus de GIJIA simplifiés seront conçus pour améliorer la productivité des utilisateurs, la sûreté des actifs, la transparence des décisions et la vérifiabilité des actions. De plus, la GIJIA permettra de faire ce qui suit.

- Atténuer les cybermenaces.
- Appuyer la tenue rapide d'enquêtes judiciaires sur les violations d'accès à l'information.
- Donner aux gens un droit de regard sur leur information d'identité personnelle.
- Permettre aux gens d'accéder à leur propre profil et de le mettre à jour.
- Permettre d'employer l'analyse comparative entre les sexes plus (ACS+) dans la conception des systèmes d'identité, de justificatifs et d'accès.

En juillet 2019, le MDN mettait en place un cadre de gouvernance afin de coordonner les activités de GIJIA dans l'ensemble du Ministère. Parallèlement, la phase d'analyse des options du projet était en cours; pendant cette phase, l'équipe du projet a produit 15 cas d'utilisation de la GIJIA décrivant les fonctions requises de la capacité. Ces cas figurent dans la section sur les exigences d'exploitabilité ci-dessous.

Opérations du système

Mission et scénarios. Le ministère de la Défense nationale (MDN) fournira une capacité de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) pour centraliser les services ministériels relatifs à l'identité, aux justificatifs d'identité et à l'accès.

Actuellement, au MDN, les mesures de contrôle de l'identité, des justificatifs d'identité et de l'accès sont cloisonnées et la centralisation de la gestion, de la surveillance et du contrôle demeure une lacune. Les menaces externes découlant de l'exposition des réseaux non classifiés du MDN à Internet public compliquent les choses. La situation actuelle est complexe et non viable, et elle expose les opérations ministérielles à des risques pour la sécurité de l'information.

Une fois qu'elle sera fournie, la capacité de GIJIA sera fondée sur le principe selon lequel chaque entité du ministère, qu'il s'agisse d'une personne ou non, aura une identité numérique unique. De 2018 à 2027, les responsables du projet de GIJIA du MDN élaboreront et fourniront des capacités de GIJIA interopérables et fédérées permettant de

gérer, de surveiller et de contrôler, de façon centralisée, les identités, les comptes d'utilisateurs et les justificatifs d'identité. Ces capacités de GIJIA amélioreront la productivité et la sécurité des ressources ministérielles et elles permettront au Ministère de se conformer aux politiques gouvernementales en matière de confidentialité.

L'approche actuelle en matière de GIJIA, laquelle est distribuée, déconnectée et non automatisée, limite la protection des actifs, ralentit l'accès des utilisateurs aux ressources, nuit à la prise de décisions en lien avec l'attribution et la révocation de droits d'accès et augmente les risques de perte, de dommage ou de compromission des actifs ministériels.

Le projet de GIJIA permettra aux propriétaires d'actifs de générer rapidement et en toute sécurité des justificatifs d'identité et de prendre les décisions relatives à l'accès au moyen de l'identité numérique unique fournie par un service d'identité géré de manière centralisée. Des processus de GIJIA rationalisés seront créés pour rendre les utilisateurs plus productifs, les actifs plus sécurisés, les décisions plus transparentes et les actions plus vérifiables. De plus, la GIJIA :

- permettra aux personnes de voir leurs renseignements d'identification personnels;
- permettra aux personnes de créer et de mettre à jour leur profil;
- permettra l'analyse comparative entre les sexes plus (ACS+) dans le cadre de la conception des systèmes d'identité, de justificatifs d'identité et d'accès;
- atténuera les cybermenaces;
- appuiera la tenue rapide d'enquêtes judiciaires sur les accès non autorisés.

La Figure 1 ci-dessous offre un aperçu des processus opérationnels de GIJIA et montre la navigation pour les cas d'utilisation de la GIJIA de haut niveau. La Figure 1 divise la GIJIA en deux types de processus principaux – ceux dont l'information est conservée au MDN, notamment pour ses employés et fournisseurs, et ceux dont l'information est gérée à l'externe et transmise par le truchement d'un processus fédéré. Les utilisateurs gérés par le MDN et les utilisateurs fédérés font partie des trois catégories suivantes :

- Entités fédérales – Toute personne qui est un employé ou un fournisseur du gouvernement fédéral. Ces entités peuvent être gérées par le MDN ou fédérées, selon l'utilisateur et le système.
- Partenaires opérationnels – Les personnes appartenant à des administrations nationales ou locales ou à des organisations commerciales sont habituellement fédérées, toutefois, elles peuvent être gérées par le MDN dans certains cas.
- Clients – Les personnes qui sont des clients du MDN. Ils sont habituellement fédérés, mais ils peuvent être gérés par le MDN dans certains cas.

Bien que chaque cas d'utilisation décrive un processus opérationnel particulier de la GIJIA, tous les cas sont étroitement reliés. Les lignes pointillées du schéma illustrent des relations entre les différents cas d'utilisation.

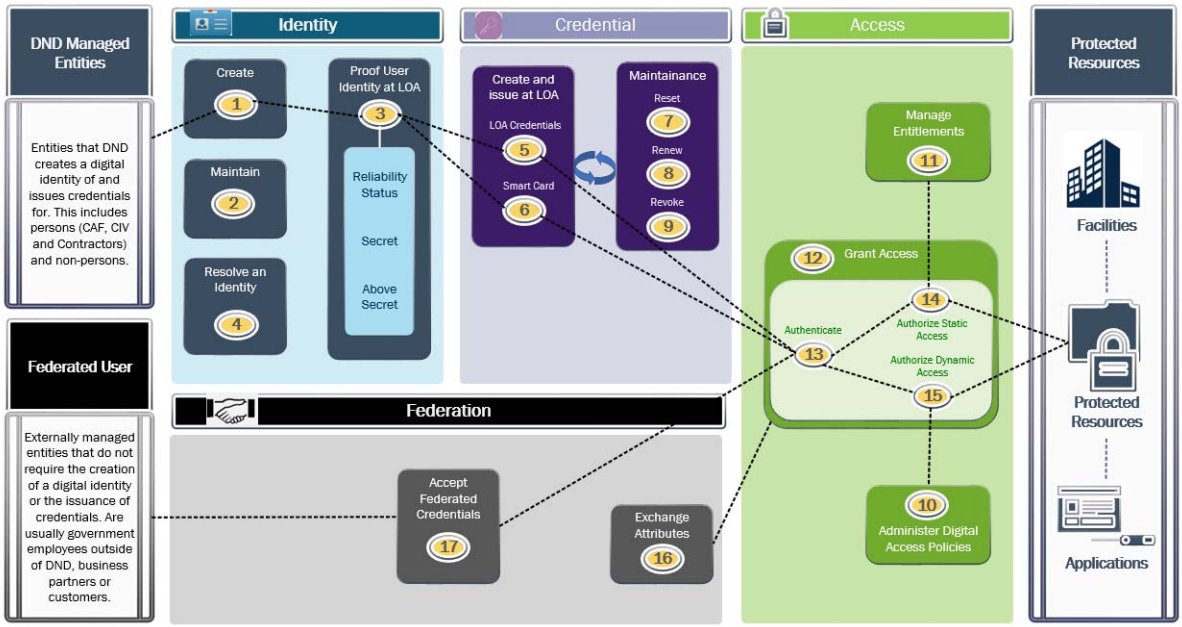

Figure 1 : Affichage opérationnel de la GIJIA. Les chiffres 1 à 17 renvoient aux tâches de GIJIA présentées à la section 0.

EN	**FR**
DND managed entities	Entités gérées par le MDN
Entities that DND creates a digital identity of and issues credentials for. This includes persons (CAF, CIV and Contractors) and non-persons.	Entités pour lesquelles le MDN crée une identité numérique et des justificatifs d'identité. Cela comprend des personnes (membres des FAC, membres civils et fournisseurs) et des entités autres que des personnes.
Identity	Identité
Create	Créer
Maintain	Tenir à jour
Resolve an Identity	Résoudre une question d'identité
Proof user identity at LOA	Vérification de l'identité de l'utilisateur au niveau d'assurance
Reliability status	Cote de fiabilité
Secret	Secret
Above secret	Supérieur à secret
Credential	Justificatif d'identité
Create and issue at LOA	Créer et émettre au niveau d'assurance
LOA credentials	Justificatifs d'identité au niveau d'assurance
Smart card	Carte à puce
Maintainance	Gestion
Reset	Réinitialiser
Renew	Renouveler
Revoke	Révoquer
Access	Accès
Manage entitlements	Gestion des droits
Grant access	Autoriser l'accès
Authenticate	Authentifier
Authorize static access	Autoriser l'accès statique
Authorize dynamic access	Autoriser l'accès dynamique
Administer digital access policies	Administrer les politiques d'accès numérique
Federated user	Utilisateur fédéré

Externally managed entities that do not require the creation of a digital identity or the issuance of credentials. Are usually government employees outside of DND, business partners or customers.	Entités gérées à l'externe qui ne nécessitent pas la création d'une entité numérique ou l'octroi de justificatifs d'identité. Habituellement des employés du gouvernement externes au MDN, des partenaires d'affaires ou des clients.
Federation	Fédération
Accept federate credentials	Accepter les justificatifs d'identité des entités fédérées
Exchange attributes	Échange d'attributs
Protected resources	Ressources protégées
Facilities	Installations
Protected resources	Ressources protégées
Applications	Applications

Environnement opérationnel. La capacité de GIJIA s'appliquera aux environnements des Forces armées canadiennes (FAC) et du MDN à tous les niveaux de sécurité : Non classifié, Secret et supérieur à Secret. Cette capacité constituera l'autorité centrale pour l'identification numérique à l'appui des niveaux les plus élevés d'assurance de l'identité et des justificatifs afin d'appuyer les exigences des différents environnements et niveaux de sécurité.

Par la normalisation, la gouvernance et la prestation d'un service commun, la GIJIA pourra intégrer des points de contrôle d'accès logiques et physiques sur les plans stratégique et tactique.

Le responsable opérationnel des ressources logiques (réseaux, applications, etc.) pourra adopter la capacité de GIJIA pour appuyer ses propres exigences en matière d'information sur l'identité, d'authentification, d'accès et de justificatifs d'identité.

De la même manière, le responsable opérationnel des installations et des bases pourra adopter la capacité de GIJIA pour appuyer ses propres exigences en matière d'information sur l'identité, d'authentification, d'accès et de justificatifs d'identité.

Bien que le projet lui-même visera une intégration avec un sous-ensemble de ressources logiques et physiques, l'objectif est d'offrir un service moderne avec des interfaces normalisées, une assurance de haut niveau pour l'identité et les justificatifs d'identité ainsi qu'une gouvernance pour appuyer l'intégration possible de tous les systèmes et services à une capacité de GIJIA unique.

L'environnement opérationnel de la capacité doit tenir compte des exigences actuelles et potentielles des systèmes qui ont besoin d'un contrôle de l'accès dans l'ensemble des FAC et du MDN.

Contexte de menace. Auparavant, le Ministère protégeait les ressources d'information contre les menaces en les conservant dans des espaces physiquement contrôlés. À l'ère de l'information, les technologies émergentes permettent un accès élargi et facile à l'information. Associées aux menaces criminelles et militaires ainsi qu'aux menaces relatives au renseignement qui sont de plus en plus persistantes et sophistiquées, ces nouvelles technologies ont augmenté le risque d'accès non autorisé aux renseignements électroniques et aux systèmes de contrôle du MDN. La situation actuelle n'est pas le résultat d'une défaillance d'un élément du cadre organisationnel ou d'un changement soudain et imprévu dans l'environnement. Elle a plutôt évolué lentement par la prolifération des ordinateurs et des services en réseau dans le cadre de toutes les opérations et pratiques ministérielles.

De plus, la menace envers les ressources d'information augmentera de façon exponentielle tandis que le MDN continue de mettre en œuvre l'approche exhaustive pour les opérations, puisque cette approche requiert un accroissement de l'accessibilité et de l'échange d'information internes, interministériels et multinationaux. Outre la prévision selon laquelle l'accessibilité et l'échange d'information augmenteront, la haute direction du MDN s'attend à ce que la protection de l'information augmente aussi pour satisfaire aux exigences en matière de protection des renseignements personnels et assurer la confidentialité des ressources d'information.

Évaluation des menaces et des risques. Les systèmes de GIJIA se trouveront dans des domaines non classifiés ou classifiés Secret ou à un niveau supérieur à Secret. Les exigences en matière d'évaluation des menaces et des risques varieront en fonction du domaine.

Concept des opérations

La capacité de GIJIA créera une identité numérique unique pour chaque personne et entité autre qu'une personne au sein du Ministère. Une fonction centrale de gestion de l'identité sera utilisée par les gestionnaires des actifs physiques et logiques, notamment les bases, les stations, les autres installations, les réseaux, les applications et les

autres services de TI, afin de créer et de gérer les justificatifs d'identité requis pour authentifier une personne ou une entité autre qu'une personne et l'autoriser à accéder à un actif.

Le service d'identité central agira à titre de courtier entre les organisations qui ont besoin de produire ou d'utiliser de l'information sur l'identité. Le courtier permettra aux gestionnaires d'actifs d'utiliser de l'information fondée sur le rôle ainsi que de l'information fondée sur les attributs pour prendre des décisions concernant l'accès.

La GIJIA ne sera pas intégrée aux systèmes de gestion de l'accès actuels ou nouveaux; elle sera plutôt offerte en tant que service auquel les responsables opérationnels des réseaux, des applications et des systèmes d'accès physique s'abonneront. Un ensemble de processus et de protocoles normalisés sera mis en place pour régir l'échange de renseignements sur l'identité et sur les justificatifs d'identité.

Le MDN et les FAC entretiennent de nombreuses relations avec les organisations externes, notamment les autres ministères et organismes fédéraux, des armées alliées et des partenaires du secteur privé. Ces relations exigeront que le MDN fournisse des capacités de GIJIA fédérées qui permettent l'échange de renseignements sur l'identité et les justificatifs d'identité avec ces organisations externes. Voici certains exemples d'utilisations fédérées de la GIJIA :

- autorisation automatique de l'échange d'un élément d'information avec un partenaire externe;
- autorisation automatique de l'accès d'une personne externe à un espace physique du MDN;
- échange automatique d'information sur l'identité à un partenaire externe pour permettre l'accès, par une entité du MDN, aux actifs physiques ou logiques d'une organisation externe.

La GIJIA comprend une fonction de gouvernance qui coordonnera la mise en œuvre des capacités de GIJIA dans les organisations de niveau 1 du Ministère. Cela permettra de prendre des décisions au sujet de l'adoption de normes, d'optimiser un programme d'initiatives et de projets pour maximiser les avantages nets des investissements dans la GIJIA et de tenir à jour les vues de l'architecture de la GIJIA à mesure que celle-ci est mise en œuvre et se développe.

Rôles clés. Les rôles clés sont décrits au Tableau 1.

Tableau 1 : Rôles clés de la GIJIA

Rôles et acteurs	Définition
Administrateur de données	Un administrateur de données est une personne qui travaille en étroite collaboration avec l'organisme administratif afin d'administrer et de mettre en œuvre les ajouts et ajustements aux politiques sur l'accès numérique.
Administrateur du personnel	Administrateur des ressources humaines ayant la responsabilité d'entrer les renseignements sur un nouvel employé ou un fournisseur dans la source de données faisant autorité appropriée.
Application	Une application est un logiciel conçu pour exécuter un ensemble de fonctions, tâches ou activités coordonnées pour l'utilisateur.
Autorité approbatrice	L'autorité approbatrice désignée est le responsable ayant le pouvoir d'assumer officiellement la responsabilité relative à l'utilisation d'un système ou d'une fonction opérationnelle à un niveau de risque acceptable.
Clients	Personnes qui sont des clients du MDN. Ces personnes sont habituellement fédérées, mais elles peuvent être gérées par le MDN dans certains cas.
Demandeur	Le demandeur est une personne ou un système qui présente une demande.
Dépôt de données	Le dépôt lui-même est une infrastructure de bases de données servant à recueillir, gérer et entreposer divers ensembles de données.

Rôles et acteurs	Définition
Employé	Un terme générique qui désigne les employés civils et les membres militaires du MDN.
Entités fédérées	Toute personne qui est un employé ou un fournisseur du MDN. Elle peut être gérée par le MDN ou fédérée selon l'utilisateur et le système.
Entrepreneur	L'entrepreneur est la personne, l'entité ou les entités nommées dans le contrat qui doivent fournir au MDN des biens, des services ou les deux.
Fournisseur de justificatifs d'identité	Un fournisseur de justificatifs d'identité est une entité de confiance qui émet des jetons de sécurité ou des justificatifs électroniques aux abonnés et qui consiste en un service commercial, un service offert par un organisme ou un service partagé.
Gestionnaire de l'identité	Le gestionnaire de l'identité relève les sources de données concernant la personne et rassemble les données sur l'identité pour créer un profil d'identité complet.
Gestionnaire des droits	Le gestionnaire des droits supervise et ajuste les privilèges d'accès accordés aux personnes, aux rôles et aux groupes d'une organisation.
Gestionnaire des justificatifs d'identité	Le gestionnaire des justificatifs d'identité est une personne ou un système qui accorde, réinitialise, renouvelle ou révoque des justificatifs d'identité.
Organisme d'administration des politiques sur le numérique	Organisme d'administration des politiques qui crée et met à jour les règles qui régissent l'accès logique et physique d'une organisation et qui établit les politiques sur le numérique qui gouvernent les décisions en matière d'accès d'après ces règles. Les organismes d'élaboration de politiques se fondent souvent sur les règlements fédéraux, les décrets, les lois, les règles propres à une organisation et les précédents pour établir ou mettre à jour une politique sur l'accès numérique.
Parrain	Le parrain est un représentant qui peut vérifier qu'une personne a vraiment besoin de certains éléments, notamment des justificatifs d'identité. Par exemple, un parrain pourrait demander des justificatifs de niveau LoA3 pour une personne.
Partenaires opérationnels	Personnes faisant partie d'autres ministères ou organismes fédéraux ou organisations du secteur privé.
Ressource protégée	Toutes les ressources du MDN auxquelles seuls les utilisateurs ou systèmes autorisés peuvent accéder.
Source de données	L'emplacement principal d'où proviennent les données faisant autorité.
Source faisant autorité	Une source de production de données reconnue ou officielle qui publie des données fiables et exactes qui seront utilisées ultérieurement par les clients. Une source faisant autorité peut être la combinaison fonctionnelle de multiples sources de données distinctes.
Système à distance	Un système pour lequel un utilisateur n'a pas d'accès physique, mais auquel il peut accéder, ou qu'il peut utiliser, au moyen d'un réseau informatique.

Rôles et acteurs	Définition
Système de contrôle de l'accès	Dans les domaines de la sécurité physique et de la sécurité de l'information, le contrôle de l'accès désigne la restriction sélective de l'accès à un lieu ou à une autre ressource. L'accès peut désigner la consommation, l'entrée ou l'utilisation. On appelle « autorisation » la permission d'accéder à une ressource. Les systèmes de contrôle de l'accès assurent l'authentification de l'identification ainsi que l'autorisation des utilisateurs et des entités en évaluant les justificatifs d'ouverture de session, qui peuvent comprendre des mots de passe, des numéros d'identification personnels (NIP), des identificateurs biométriques, des jetons de sécurité ou d'autres facteurs d'authentification. L'authentification à plusieurs facteurs, qui nécessite deux facteurs d'authentification ou plus, est souvent un élément important d'une défense à couches multiples visant à protéger les systèmes de contrôle de l'accès.

Tâches clés. Les tâches clés sont décrites au Tableau 2.

Tableau 2 : Tâches clés de la GIJIA

Nº	Tâche
1	Création (intégration) de l'identité numérique d'une entité
2	Tenue à jour de l'identité numérique d'une entité
3	Vérification de l'identité au niveau d'assurance requis, p. ex. au MDN, la vérification de l'identité s'effectue actuellement aux niveaux suivants : 1) Cote de fiabilité 2) Secret 3) Supérieur à Secret
4	Résolution d'une question relative à une identité interne au MDN
5	Création et délivrance d'un justificatif d'identité au niveau d'assurance
6	Création et délivrance d'une carte à puce
7	Réinitialisation des justificatifs d'identité d'une entité
8	Renouvellement des justificatifs d'identité d'une entité
9	Révocation des justificatifs d'identité d'une entité
10	Administration des politiques sur l'accès numérique
11	Gestion des droits en supervisant et en ajustant les privilèges d'accès accordés à une entité
12	Autorisation d'accès aux ressources protégées
13	Authentification d'une entité
14	Autorisation d'accès au moyen d'une méthodologie statique
15	Autorisation d'accès au moyen d'une méthodologie dynamique

Nº	Tâche
16	Échange des attributs dans une fédération
17	Acceptation des justificatifs d'identité dans une fédération

Concept de soutien

Le soutien de la capacité de GIJIA sera conforme aux pratiques exemplaires de l'industrie. Celles-ci sont actuellement décrites dans le cadre intitulé Bibliothèque de l'infrastructure des technologies de l'information (ITIL), qui met l'accent sur l'harmonisation des services de TI avec les besoins opérationnels. Les pratiques d'ITIL seront adaptées à l'environnement et la structure organisationnelle uniques du MDN et des FAC.

Puisque la capacité de GIJIA deviendra un service clé offert dans l'ensemble du MDN et des FAC, un soutien de haut niveau pour le service sera assuré par le sous-ministre adjoint (Gestion de l'information – SMA[GI]), plus particulièrement par le directeur, Ingénierie et intégration (Gestion de l'information – DIIGI). Son rôle consistera à tenir à jour l'architecture de référence de la GIJIA pour le Ministère et d'assurer la supervision de l'ingénierie et de l'intégration des ressources à la capacité de GIJIA.

L'établissement d'un organisme de gouvernance permanent pour la GIJIA au sein du MDN est essentiel à la réussite de cette capacité. L'organisme de gouvernance comportera de multiples niveaux, y compris un comité directeur exécutif et des groupes de travail qui peuvent appuyer l'intégration, le soutien, la gestion et l'évolution continus du service de GIJIA.

Dans les différents domaines, la capacité de GIJIA sera intégrée aux systèmes de soutien existants.

Lignes de soutien. Le Concept de soutien décrira, dans le futur, comment les cinq composants d'ITIL énumérés ci-dessus seront améliorés et mis en œuvre par le SMA(GI) à l'appui des capacités fournies par le projet. Le Concept de soutien détaillé sera élaboré pendant la phase de définition du projet, alors que la conception du système, les mesures de rendement principales et les spécifications fonctionnelles seront définies.

Niveaux de soutien. Les systèmes de GIJIA et les mesures de soutien de l'infrastructure seront harmonisés avec l'approche en trois niveaux actuellement utilisée par le MDN et les FAC, soit :

- Soutien de premier niveau – porte sur la consignation et le classement des incidents reçus et sur l'intervention immédiate menée dans le but de tenter de rétablir dès que possible un service en panne. Si une solution immédiate ne peut être obtenue, le soutien de premier niveau transmettra le problème au soutien de deuxième niveau. Le soutien de premier niveau traite aussi les demandes de service et tient les utilisateurs au courant de l'état de résolution des problèmes.
- Soutien de deuxième niveau – se charge des incidents qui ne peuvent pas être résolus immédiatement par le soutien de premier niveau. Le soutien de deuxième niveau assurera la coordination avec les fournisseurs de services, suivant les besoins, afin de résoudre les incidents. Les problèmes qui ne peuvent pas être résolus à ce niveau sont transmis au soutien de troisième niveau.
- Soutien de troisième niveau – est assuré par les services techniques. Ceux-ci assureront la liaison avec les fabricants et des tiers fournisseurs, suivant les besoins, afin de résoudre les incidents. De manière typique, les incidents qui sont transmis au troisième niveau de soutien exigent, pour que ceux-ci soient résolus, qu'une demande de changement soit faite afin de faire modifier le système.

En ce qui concerne les systèmes et l'infrastructure de GIJIA, les niveaux de soutien seront déterminés pour chaque technologie et système fourni. Les organisations de soutien auront pour tâche de fournir des niveaux de soutien précis selon leurs connaissances et compétences ainsi que d'après les données techniques, les outils spéciaux, l'équipement d'essai ou le temps requis.

Applications. La capacité de GIJIA sera intégrée au Réseau étendu de la Défense (RED) ainsi qu'à l'Infrastructure du réseau secret consolidé (IRSC) en tant que service de base. Les applications majeures (p. ex. services d'annuaire, infrastructure à clés publiques [ICP], Système de gestion des ressources humaines [SGRH]) se trouvant sur ces réseaux seront intégrées pour permettre la gestion et le contrôle par l'intermédiaire du nouveau service. Des systèmes à accès physique seront connectés au service. L'intégration d'applications, de réseaux et de services supplémentaires sera envisagée au cas par cas pendant les phases de définition et de mise en œuvre du projet de GIJIA.

Lignes directrices pour la conception

Voici les lignes directrices relatives à la conception de la GIJIA :

- Au centre de la conception de la GIJIA se trouve le concept d'une identité numérique unique pour chaque personne et chaque entité autre qu'une personne.
- La conception du système de GIJIA doit être fondée sur le principe selon lequel les renseignements sur l'identité et les justificatifs d'identité font autorité et sont créés et contrôlés par des sources faisant autorité.
- L'automatisation est un concept central de la conception de la capacité de GIJIA.
- Les services de GIJIA doivent être modulaires dans toute la mesure possible.
- L'interopérabilité entre les organisations et l'interopérabilité entre le MDN et les partenaires externes sont essentielles pour une conception réussie de la GIJIA.
- La confidentialité de l'information, en particulier la protection des renseignements personnels, est au cœur de la conception de la capacité de la GIJIA.
- Les protocoles, formats et échanges d'information de la GIJIA sont, lorsque c'est possible, fondés sur les normes communes et acceptées de l'industrie ou du gouvernement. La conception de la capacité de GIJIA doit maximiser l'utilisation de composants commerciaux, gouvernementaux ou militaires sur étagère et minimiser la conception personnalisée des systèmes.
- La capacité de GIJIA doit permettre la réutilisation maximale des systèmes, composants, structures et processus organisationnels existants, elle doit être conçue en vue d'être extensible et faciliter les mises à niveau avec les technologies émergentes.
- La conception de la capacité de GIJIA doit minimiser le recours à de nouvelles infrastructures.
- La conception de la capacité de GIJIA doit maximiser l'utilisation des TI disponibles à la fine pointe (cette ligne directrice n'élimine pas l'exigence relative à la réutilisation [sous-paragraphe ☐]).
- La conception de la capacité de GIJIA doit pouvoir prendre en charge une croissance annuelle des données allant jusqu'à 30 %. Cela doit être pris en considération pour la conception de l'infrastructure et le soutien en service.

Les services de GIJIA suivants font partie de la portée du projet :

- Service de données d'identité d'entreprise – décrit à l'annexe B de la présente demande d'information
- Service d'authentification fédérée d'entreprise – décrit à l'annexe B de la présente demande d'information
- Service de gouvernance de l'accès d'entreprise – décrit à l'annexe B de la présente demande d'information
- Passerelle d'échange d'information interdomaines pour la GIJIA

Le service de données d'identité d'entreprise et le service d'authentification fédérée d'entreprise peuvent être élaborés par le MDN avant la phase de mise en œuvre de la GIJIA. Ces services devront ensuite être intégrés à la solution de GIJIA.

La création des services suivants ne fait pas partie de la portée du projet :

- Infrastructure à clé publique du RED
- Infrastructure à clé publique de niveau Secret

Évaluation de la sécurité et autorisation (ESA). Une ESA complète sera menée conformément au Guide d'évaluation de la sécurité et autorisation (GESA), ce qui donnera lieu à la promulgation d'une directive appropriée relativement à la mise en place du matériel et des logiciels, au recours au personnel et à la mise en œuvre des procédures afin de satisfaire aux exigences en matière de sécurité propres aux capacités.

Exigences en matière d'efficacité du système

Critères relatifs aux niveaux en matière d'exigences et de rendement. Toutes les exigences relatives à la GIJIA sont obligatoires. Les exigences seront classées en ordre de priorité en fonction de la valeur, de la négociation, de la répartition du temps et du niveau d'effort.

Exigences générales. L'établissement et le maintien d'une structure de gouvernance permanente qui :

- établit l'orientation politique pour la GIJIA;
- optimise le programme de GIJIA par rapport aux objectifs stratégiques du MDN;
- applique et gère les normes sur les données relatives à l'identité et aux justificatifs d'identité;
- crée et maintient l'architecture d'entreprise de la GIJIA.

La capacité de créer une identité faisant autorité ainsi que des justificatifs d'identité connexes pouvant être utilisés pour régir l'accès au sein du MDN et des FAC ainsi qu'à l'externe, entre le MDN et les FAC ainsi qu'avec d'autres ministères et organismes et des partenaires multinationaux.

La capacité de mettre à niveau, de consigner et de supprimer en toute sécurité les identités uniques et les justificatifs connexes des membres des FAC, des employés du MDN, des partenaires étrangers, des entrepreneurs internationaux, des visiteurs et des entités qui ne sont pas des personnes.

La capacité de contrôler en temps quasi réel, c'est-à-dire de minutes à heures, les droits d'accès à un bâtiment, un emplacement ou un espace comportant un point de contrôle de l'accès qui le protège contre l'accès non autorisé.

La capacité de contrôler les droits d'accès à l'information électronique, aux réseaux, aux services de technologie de l'information, aux applications et aux systèmes à l'appui de la protection contre l'accès non autorisé.

La capacité d'accorder aux personnes et aux entités autres que des personnes l'accès aux ressources d'information physiques et électroniques et de leur retirer cet accès en quelques minutes ou quelques heures tout en minimisant les erreurs humaines au moyen de l'automatisation de l'échange de renseignements sur l'identité entre les systèmes, réseaux et organisations.

La capacité d'isoler des segments endommagés ou déstabilisés de la GIJIA et de maintenir les fonctions relatives à l'identité, aux justificatifs d'identité et à la gestion de l'accès dans les segments non touchés de l'entreprise.

Les exigences en matière d'opérabilité sont décrites au Tableau 3.

Tableau 3 : Exigences en matière d'opérabilité de la GIJIA

Identifiant	Titre	Description Entité = 1) personne et 2) entité autre qu'une personne
1	Création d'une identité	Lorsqu'une entité est intégrée à une unité du MDN, de l'information est recueillie et conservée pour servir de référence numérique dans les systèmes de TI. Cette information est stockée dans un dossier d'identité, qui est ensuite modifié ou supprimé au besoin. Une fois qu'un dossier d'identité numérique est établi, il est transmis à d'autres systèmes à partir d'une source faisant autorité, et des droits d'accès y sont associés (voir l'exigence « Gestion des droits »). **Remarque :** La marche à suivre est différente pour les personnes (membres, employés, fournisseurs ou visiteurs temporaires) et les entités autres que les personnes.
2	Tenue à jour d'une identité	Une fois que l'identité d'une entité a été créée au MDN, les données sur l'identité peuvent être mises à jour seulement dans la source faisant autorité, ce qui permet de s'assurer de l'exactitude des données. Le système de GIJIA transmet l'identité mise à jour avec les ressources qui ont accès aux données sur l'identité de cette entité.

Identifiant	Titre	Description Entité = 1) personne et 2) entité autre qu'une personne
3	Validation d'une identité au niveau d'assurance Cote de fiabilité Secret Supérieur à Secret	Avant l'intégration d'une personne, un processus de validation est exécuté. Ce processus permet de vérifier son identité, et une fois le processus terminé, la personne reçoit des justificatifs d'identité à un niveau d'assurance approprié. Le niveau d'assurance requis pour une personne dépend de son rôle, et ce niveau peut être Cote de fiabilité, Secret ou supérieur à Secret. La validation offre un niveau d'assurance plus détaillé et permet à une personne de recevoir des justificatifs d'identité. **Cote de fiabilité** : La personne doit soumettre des documents de base pour prouver l'identité revendiquée. **Secret** : Nécessite un processus de vérification rigoureux et la présentation de davantage de documents que pour le niveau Cote de fiabilité. **Supérieur à Secret :** Nécessite le processus de vérification de l'identité revendiquée le plus rigoureux.
4	Détermination d'une identité interne au MDN	Le MDN compte de nombreux systèmes sources qui contiennent des données concernant l'identité d'une entité. Une demande de données sur l'identité sera soumise par le gestionnaire de l'identité. Le gestionnaire de l'identité doit pouvoir relever les sources de données pertinentes pour obtenir les attributs relatifs à l'identité depuis les systèmes sources faisant autorité et les rassembler pour créer un enregistrement unique à des fins de présentation ou d'évaluation.
5	Création et attribution de justificatifs d'identité au niveau d'assurance approprié	Lorsqu'une demande de justificatifs d'identité au niveau d'assurance approprié est présentée, un fournisseur de services de justificatifs doit pouvoir valider la demande et assigner des justificatifs d'identité au demandeur. Un jeton de justificatif respecte le niveau d'assurance requis lorsqu'il utilise un ou plusieurs facteurs d'authentification (voir le cas d'utilisation sur l'authentification), exige l'utilisation d'un NIP ou d'un mot de passe fort et protège les renseignements sur les justificatifs au moyen d'un mode de transmission chiffré.
6	Création et délivrance d'une carte à puce	Lorsqu'une personne est intégrée, il faut créer une carte à puce et la lui remettre. La carte à puce contiendra les données dont le détenteur aura besoin pour accéder aux installations et aux systèmes d'information du MDN et elle assurera des niveaux de sécurité appropriés pour toutes les applications pertinentes du MDN. Une carte à puce doit être sécuritaire et fiable.
7	Tenue à jour des justificatifs d'identité – réinitialisation	Lorsqu'une personne oublie le secret partagé qui est associé à ses justificatifs d'identité, habituellement un mot de passe ou un NIP, elle peut demander une réinitialisation. Cela lui évite de demander de nouveaux justificatifs.
8	Tenue à jour des justificatifs d'identité – renouvellement	Lorsque les justificatifs d'identité d'une entité expirent et qu'elle dispose des approbations nécessaires, elle entité doit avoir l'option de renouveler automatiquement les justificatifs d'identité plutôt que de recommencer le processus de demande.
9	Tenue à jour des justificatifs d'identité – révocation	Lorsqu'une entité se dissocie du MDN ou qu'elle ne satisfait plus aux critères d'admissibilité de ses justificatifs d'identité, ces derniers doivent être révoqués. Lorsque le gestionnaire des justificatifs d'identité reçoit la demande de révocation, il invalide les justificatifs et désactive les droits d'accès.
10	Administration des politiques sur l'accès numérique	L'administration des politiques décrit le processus de création et de mise à jour des règles qui régissent l'accès logique et physique d'une organisation et qui établit les politiques sur le numérique qui gouvernent les décisions en matière d'accès d'après ces règles. La création et la mise en œuvre des processus stratégiques se produiront pendant la période de conception, avant que les

Identifiant	Titre	Description Entité = 1) personne et 2) entité autre qu'une personne
		personnes et les entités autres que des personnes tentent d'accéder aux ressources protégées. Une fois qu'une politique est créée, elle doit être prise en considération pendant l'exécution pour prendre des décisions sur l'accès de façon dynamique, au moment où une tentative d'accès est effectuée, en fonction des rôles et des attributs d'une entité. Les organes responsables des politiques se fonderont sur les règlements fédéraux, les décrets, les lois, les règles propres à une organisation et les précédents pour établir ou mettre à jour une politique sur l'accès numérique.
11	Gestion des droits	La gestion des droits est le processus de supervision et d'ajustement des privilèges d'accès accordés à une entité dans une organisation. Ce processus s'appelle « approvisionnement » et s'applique à la gestion statique de l'accès. La gestion des droits est effectuée à l'étape de la conception, avant qu'une entité tente d'accéder aux ressources protégées, et les droits d'accès seront accordés à l'entité avant que celle-ci accède aux ressources protégées. La demande de création de droits pour une entité sera soumise et examinée et, si le changement demandé respecte la politique et que l'entité a besoin de cet accès pour exercer ses fonctions, la demande sera approuvée. L'entité recevra des droits d'accès à jour. Ces droits sont mis à jour chaque fois que les rôles de l'entité changent.
12	Octroi d'un accès à une ressource protégée	Seule une entité admissible peut obtenir un accès aux ressources protégées. Dans le cadre de ce processus, l'entité est authentifiée, puis on lui accorde ou refuse un accès d'utilisateur aux ressources logiques et physiques protégées, notamment les systèmes, les fichiers et les installations physiques. Une personne peut consulter l'information sur son identité et en autoriser l'échange avec les responsables de ressources.
13	Authentification d'une entité	Certaines étapes de ce processus permettent d'authentifier une entité qui a demandé un accès à une ressource protégée. Pendant le processus d'authentification, un système vérifie l'identité revendiquée par l'entité d'après un certain niveau d'assurance. Il y a trois types de facteurs d'authentification : quelque chose que l'on sait (comme un mot de passe ou un NIP), quelque chose que l'on possède (comme une carte à puce) et quelque chose que l'on est (comme des empreintes digitales). Le système demande ensuite à l'entité de fournir une authentification; l'entité fournit une authentification à un ou plusieurs facteurs (selon le niveau d'assurance). Le système de contrôle de l'accès compare ensuite les données saisies par l'entité aux renseignements dont il dispose concernant l'identité revendiquée par l'entité. Si les facteurs sont vérifiés, l'authentification est réussie.
14	Autorisation d'accès – statique	L'accès peut être autorisé au moyen d'une méthode statique d'autorisation de l'accès à une ressource protégée. Selon le modèle statique, le MDN fournit aux entités un ensemble de droits d'accès. Lorsque les entités tentent d'accéder à une ressource protégée, le système de contrôle de l'accès vérifie leurs autorisations d'après les règles d'accès de la ressource. Ce modèle est commun pour les listes de contrôle d'accès et les systèmes de contrôle de l'accès fondé sur le rôle.
15	Autorisation d'accès – dynamique	L'accès peut être autorisé au moyen d'une méthode dynamique d'autorisation de l'accès à une ressource protégée. Selon le modèle dynamique, le MDN établit un ensemble de politiques d'accès. Lorsque les entités tentent d'accéder à une ressource

Identifiant	Titre	Description Entité = 1) personne et 2) entité autre qu'une personne
		protégée, le système de contrôle de l'accès évalue leurs attributs par rapport à ces politiques. Lorsque les attributs d'une entité changent, leurs droits d'accès changent de manière dynamique. Ce modèle est commun pour les systèmes de contrôle de l'accès en fonction des attributs.

Exigences en matière d'interopérabilité. Pour assurer l'interopérabilité, la capacité de GIJIA doit permettre le respect des normes en matière d'interopérabilité suivantes :

- Normes relatives au service de données d'identité d'entreprise :
    - Frontal : norme System for Cross-domain Identity Management (SCIM), protocole Lightweight Directory Access Protocol (LDAP).
    - Dorsal : protocole LDAP, système de gestion de base de données relationnelle (SGBDR), flux CSV (valeurs séparées par des virgules), format LDAP Data Interchange Format (LDIF), architecture Custom Representational State Transfer (REST).
- Normes relatives au service d'authentification fédérée d'entreprise :
    - Soutien relatif aux authentifiants : certificat d'authentification client, mot de passe, authentification fondée sur un mot de passe à usage unique (hors bande et dispositif).
    - Fédération : langage Security Assertion Markup Language (SAML), couche d'authentification OpenID Connect (OIDC), protocole OAuth, spécification WS-Fed.
    - Authentification unique : protocole Kerberos, protocole NT LAN Manager (NTLM), en-tête HTTP, jeton de fédération.
- Normes relatives au service de gouvernance de l'accès d'entreprise :
    - Frontal : service de gouvernance de l'accès d'entreprise protégé (application fondée sur un navigateur Web, application mobile).
    - Dorsal (gestion de l'approvisionnement et de l'accès) : norme SCIM, protocole LDAP, SGBDR, flux CSV, architecture REST, programme de sécurité Resource Access Control Facility (RACF) ou Top-Secret, PowerShell, protocole SSH, MS Exchange, SharePoint, CRM Dynamics.
    - Flux de travail : outils de modélisation Business Process Model and Notation (BPMN) et Decision Model and Notation (DMN), scripts d'activité et d'automatisation personnalisés.
    - Modélisation de l'accès : contrôle de l'accès fondé sur les rôles (RBAC) et contrôle de l'accès fondé sur les attributs (ABAC).
    - Notifications : courriel, alertes sur appareils mobiles.

L'infrastructure doit offrir une capacité d'échange d'attributs au sein d'une fédération. Le terme « fédération » désigne un environnement au sein duquel une organisation a mis en place les outils et les politiques permettant d'accepter les renseignements d'identité et les justificatifs d'identité d'entités provenant d'une autre organisation, élargissant ainsi l'accès sécurisé aux entités externes à l'organisation. Lorsqu'une entité d'une organisation partenaire demande l'accès à une ressource du MDN, le MDN utilise les attributs de l'entité pour prendre une décision en ce qui concerne l'accès. Plutôt que de créer un nouvel enregistrement d'identité, le MDN fait une requête auprès d'un service de métadonnées pour déterminer si un enregistrement des attributs de cette entité existe déjà. Ce processus est également utilisé à l'appui de l'établissement des délais de maintenance de l'identité. Il s'agit à la fois d'une approche d'obtention d'attributs avec intermédiaire et sans intermédiaire. Le processus s'applique également aux situations lors desquelles des attributs sont demandés auprès d'une autre division au sein du MDN.

L'infrastructure doit permettre d'accepter les justificatifs d'identité au sein d'une fédération. Le MDN établira une fédération avec des organisations externes (gouvernementales et privées) afin de mener les opérations, d'élargir les services, de réduire les coûts et d'améliorer l'efficacité générale.

Pérennité. La capacité de GIJIA, en tant que service essentiel fourni au MDN et aux FAC, doit être exploitée au sein de l'environnement cible (p. ex. niveau de classification faible – RED, niveau de classification élevé – IRSC) dans l'infrastructure ayant le plus au niveau de pérennité possible. À l'état final, la capacité de GIJIA permettra la prise en

charge de multiples exigences de GIJIA relatives au domaine de sécurité. L'interface avec le service de données d'identité d'entreprise fournira les sources d'attributs d'identité faisant autorité. Une fois ces sources consolidées (au sein de l'environnement de niveau de classification faible), elles seront transférées vers les domaines de sécurité de niveau plus élevé. La GIJIA mettra à profit les solutions interdomaines actuelles et futures afin de transférer les instances vers les domaines de sécurité de niveau plus élevé. La pérennité doit être intégrée à chaque domaine de sécurité selon le degré nécessaire pour permettre le soutien des opérations.

Disponibilité. La disponibilité est une mesure du pourcentage de temps selon lequel le matériel informatique ou les logiciels de GIJIA sont en état de fonctionnement. Le niveau de disponibilité attendu pour la GIJIA est de 99,99 %. Ce niveau pourrait être révisé dans toute demande de propositions qui pourrait être émise.

La disponibilité peut également être prise en considération selon les systèmes de GIJIA utilisés et être conçue, configurée et déployée de manière pertinente en fonction de l'utilisation prévue. Par exemple, la disponibilité du système pour l'émission de nouveaux justificatifs d'identité pourrait être inférieure à la disponibilité de la fonction de vérification pendant le processus d'authentification. L'état final est une solution de GIJIA hautement disponible étant en mesure d'appuyer les exigences opérationnelles du MDN.

Fiabilité. La fiabilité désigne la capacité du matériel informatique ou des logiciels de fonctionner de manière constante conformément aux spécifications. Le niveau de fiabilité attendu pour la GIJIA est de 99,99 %. Ce niveau pourrait être révisé dans toute demande de propositions qui pourrait être émise.

La capacité de GIJIA, en tant que service essentiel fourni au MDN et aux FAC, doit être exploitée au sein de l'environnement cible (p. ex. niveau de classification faible – RED, niveau de classification élevé – IRSC) dans l'infrastructure ayant le plus au niveau de fiabilité.

Soutenabilité. La GIJIA doit respecter les exigences en matière de soutenabilité suivantes :

- Capacité d'être livrée avec toutes les ressources de soutien en service requises pour assurer l'exécution et le soutien de la GIJIA.
- Capacité d'offrir des opérations centralisées et une fonction de gestion du service pour la GIJIA au sein de l'environnement de niveau de classification faible (RED) et au sein de l'environnement de niveau de classification élevé (IRSC).
- Capacité de surveiller l'état des services, de détecter le mauvais fonctionnement d'un service et de générer automatiquement des notifications d'événement à l'intention du centre d'exploitation de réseau pertinent.
- Capacité d'ajuster et de réajuster les services rapidement sans incidence sur le reste de la capacité à l'aide d'outils automatisés, dans la mesure du possible.
- Capacité d'assurer le suivi, la consignation et la gestion des détails, des dépendances et des interfaces pour tous les services en cause à l'aide d'outils automatisés, dans la mesure du possible.
- Capacité de fournir un portail libre--service pour les utilisateurs.
- Capacité de surveiller et de générer des rapports automatisés sur les mesures relatives aux services.
- Capacité de gérer les identités des utilisateurs et des entités à l'aide d'outils automatisés, dans la mesure du possible.
- Capacité de gérer les justificatifs d'identité des utilisateurs et des entités à l'aide d'outils automatisés, dans la mesure du possible.
- Capacité d'accorder l'accès à l'infrastructure à l'aide d'outils automatisés, dans la mesure du possible.
- Capacité d'appuyer l'attribution des privilèges administratifs.

Sécurité et confidentialité. Les exigences en matière de sécurité et de confidentialité relatives à la GIJIA sont les suivantes :

- Capacité d'activer des contrôles d'accès à l'aide d'un processus d'authentification à facteurs multiples et de les appliquer dans certains cas.
- Capacité de contrôler les justificatifs des utilisateurs dans l'ensemble des systèmes associés à la GIJIA.
- Capacité de mettre fin immédiatement à l'accès d'une entité à un ou à tous les systèmes associés à la GIJIA.

- Capacité de limiter les utilisateurs privilégiés aux fonctions d'administration et à l'information de la GIJIA.
- Capacité d'utiliser des étiquettes de métadonnées relatives aux marques de sécurité conformément à STANAG 4774 – Confidentiality Metadata Label Syntax.
- Capacité de liaison des métadonnées relatives aux marques de sécurité conformément à STANAG 4778 – Metadata Binding Mechanism de l'OTAN et à la Politique du MDN et des FAC.
- Capacité d'appuyer les décisions relatives à l'accès fondées sur le ou les rôles de l'entité.
- Capacité d'appuyer les décisions relatives à l'accès fondées sur les attributs de l'entité.
- Capacité de vérifier les flux de travail de la GIJIA, y compris en ce qui concerne :
    - l'inscription;
    - la désinscription;
    - la confirmation de l'identité;
    - l'émission de justificatifs;
    - la révocation de justificatifs;
    - l'authentification;
    - l'autorisation de l'accès.
- Capacité de vérifier les décisions relatives à l'accès, y compris :
    - les décisions manuelles;
    - les décisions automatisées;
    - les décisions d'accès autorisé;
    - les décisions d'accès non autorisé.
- Capacité d'appuyer les enquêtes criminalistiques relatives aux atteintes à la sécurité.
- Capacité de garantir et de protéger la confidentialité de l'information pour les informations personnelles identifiables (PII).
- Capacité d'assurer le suivi de la provenance de toutes les données d'identité traitées par la GIJIA, de la création à la destruction.
- Capacité de réaliser des vérifications inviolables pour toutes les décisions relatives aux politiques et à l'accès traitées par la GIJIA.

Durabilité écologique. La capacité de GIJIA doit respecter la Politique d'achats écologiques du gouvernement du Canada.

Santé et sécurité. Les exigences en matière de santé et de sécurité relatives à la GIJIA sont les suivantes :

- Capacité de respecter les politiques en matière de santé et de sécurité du gouvernement du Canada, du MDN et des FAC.
- Évolution continue.
- Capacité de prendre en charge l'ajout de nouvelles capacités sans incidence pour les autres sous--systèmes.
- Capacité de mettre à niveau et de remplacer de façon continue les services de GIJIA au sein de l'architecture de GIJIA.

Exigences relatives à la livraison. Les exigences relatives à la livraison pour la GIJIA seront diffusées au cours de la phase de définition du projet.

Exigences relatives à l'efficacité des sous--systèmes

Service d'authentification fédérée d'entreprise. La capacité de GIJIA doit pouvoir fédérer les identités au sein des réseaux existants (MDN et FAC, Groupe des cinq, autres ministères, OTAN, autres). Nota : un service d'authentification fédérée d'entreprise (projet mineur) est en cours d'élaboration parallèlement au projet majeur de solution GIJIA et que celui--ci est fondé sur les protocoles et les interfaces standard de l'industrie. La solution découlant du projet majeur de GIJIA devra être intégrée au service d'authentification fédérée d'entreprise au moyen d'interfaces de communication standard.

Service de gouvernance de l'accès d'entreprise. Les exigences en matière de service de gouvernance de l'accès d'entreprise relatives à la GIJIA sont les suivantes :

- Capacité de stocker et de gérer les politiques d'entreprise.
- Capacité de gérer l'accès logique aux réseaux.
- Capacité de gérer les systèmes de contrôle de l'accès physique et d'assurer l'intégration avec ceux--ci.
- Capacité de prendre en charge les demandes d'accès présentées à l'aide des fonctions de libre--service.
- Capacité de gérer la conformité aux politiques et aux normes et de produire des rapports connexes.
- Capacité de fournir des connecteurs aux bases de données, aux répertoires et aux interfaces de programmation d'applications (API) du service.
- Capacité d'assurer l'intégration avec le système de gestion des services de technologie de l'information dans les environnements cibles.
- Capacité de stocker et de gérer les droits pour les environnements cibles.
- Capacité de fournir des flux de travail et d'assurer l'automatisation des demandes de création, de mise à jour et de suppression des accès.
- Capacité de vérifier toutes les transactions effectuées par le système du service de gouvernance de l'accès d'entreprise au sein d'un dépôt inviolable.
- Capacité d'assurer le suivi et la vérification de la provenance des données d'identité, de leur création à leur suppression.
- Capacité d'assurer la confidentialité des données d'identité.

Service de données d'identité d'entreprise. Le service de données d'identité d'entreprise est élaboré par le MDN en tant que projet mineur. Ce service permettra d'appuyer le service d'authentification fédérée d'entreprise et la capacité de GIJIA au moyen de la collecte d'attributs d'identité qui seront utilisés par les solutions d'authentification fédérée et d'accès. Les exigences en matière de service de données d'identité d'entreprise relatives à la GIJIA sont les suivantes :

- Capacité de gérer l'accès aux données d'identité selon les politiques.
- Capacité d'assurer l'intégrité des données d'identité.
- Capacité d'assurer la protection des données d'identité.
- Services de transfert de données interdomaines la GIJIA.
- Capacité de transférer toute l'information d'identité requise du niveau de classification faible (RED) au niveau de classification élevé (IRSC) conformément aux normes prescrites et au modèle de données d'identité du MDN et des FAC.

Exigences relatives à l'accès physique pour la solution de GIJIA. La solution de GIJIA du MDN sera intégrée aux systèmes d'accès physique des bases et des garnisons du MDN. Les normes et les protocoles qui seront utilisés doivent respecter les normes de l'industrie afin de maximiser l'adoption de la GIJIA à l'appui des exigences en matière d'accès physique.

Exigences relatives à la formation. De la formation initiale et sur la transition sera offerte par l'équipe du projet de GIJIA aux membres du personnel qui assureront l'exécution, l'administration, la maintenance et le soutien des services de GIJIA. De la formation sur l'état stable du système de GIJIA sera élaborée dans le cadre du projet

de GIJIA et sera offerte aux nouveaux administrateurs du système de GIJIA. La fréquence à laquelle la formation sera offerte sera fondée sur le rythme de rotation des administrateurs du système de GIJIA.

ANNEXE B

DESCRIPTION DE L'ARCHITECTURE ET DU SYSTÈME DE GESTION DE L'IDENTITÉ, DES JUSTIFICATIFS D'IDENTITÉ ET DE L'ACCÈS

Architecture actuelle de la gestion de l'identité, des justificatifs d'identité et de l'accès

L'architecture actuelle de la gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) du ministère de la Défense nationale (MDN) est illustrée à la Figure 1. Cette représentation opérationnelle montre l'approche cloisonnée utilisée pour la GIJIA selon laquelle les identités, les justificatifs d'identité et les contrôles d'accès ne sont pas reliés entre les différentes enclaves et les divers domaines du MDN. Certaines percées ont été réalisées pour réduire ces cloisonnements et le projet de GIJIA mettra à profit les technologies et les normes actuelles pour fournir une identité numérique unique et un service d'identité connexe que pourront utiliser les applications des réseaux et des systèmes de contrôle de l'accès physique du MDN.

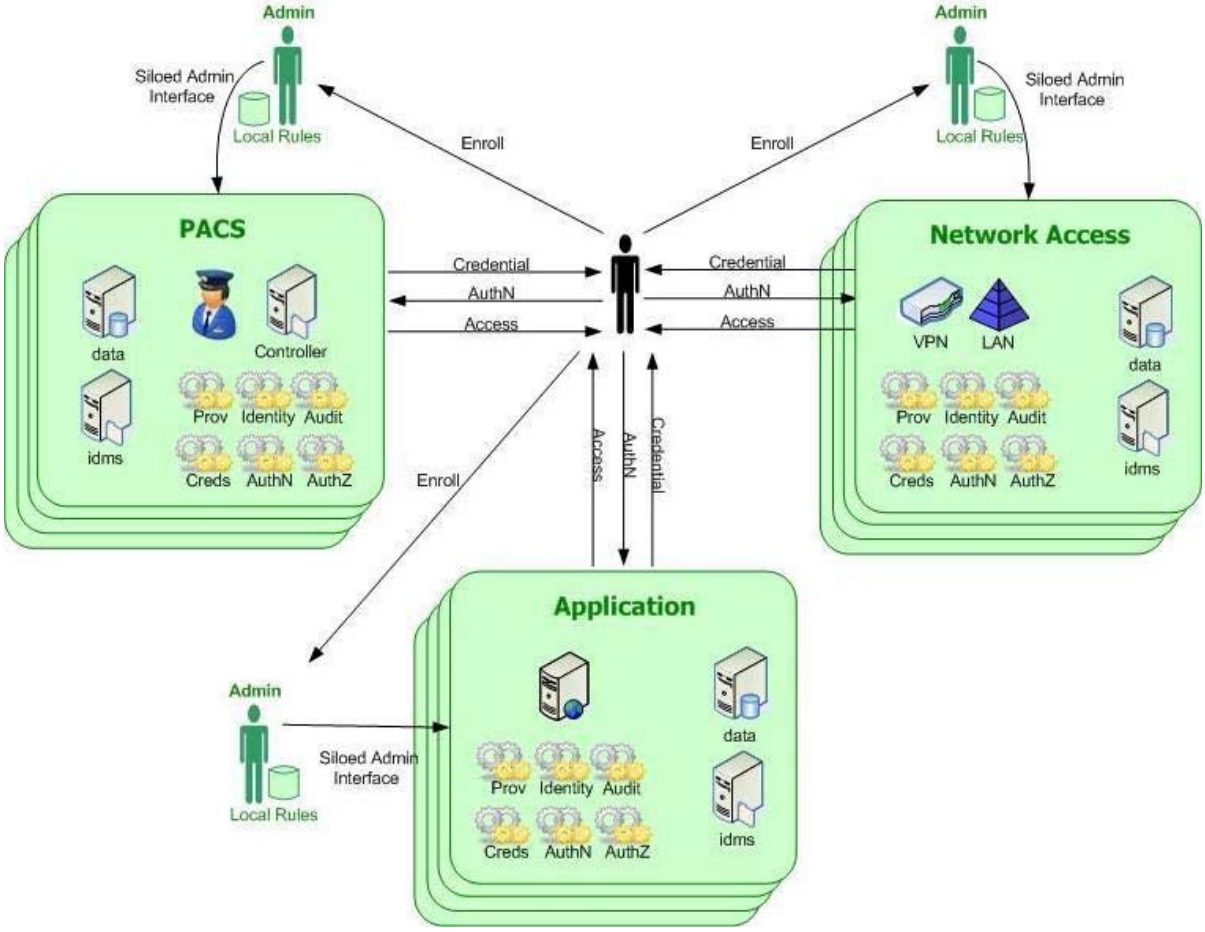

Figure 1 : Représentation opérationnelle de l'architecture de la GIJIA en place au MDN

Architecture future de la gestion de l'identité, des justificatifs d'identité et de l'accès

Dans l'architecture future de la GIJIA (Figure 2), chaque entité du Ministère (que ce soit une personne ou autre) aura sa propre identité numérique. La capacité de GIJIA sera centrée sur un service d'identité qui utilise l'identité numérique unique pour les décisions d'authentification et d'autorisation dans l'ensemble du Ministère et pour les partenaires externes. Cette architecture opérationnelle montre que les services de la GIJIA prennent en charge les applications dans le domaine désigné tandis que le même service prend en charge les applications au--delà de la limite du domaine désigné au sein d'environnements classifiés et fédérés dans des réseaux et applications partenaires.

Figure 2 représente les services suivants :

- ICP-S (ICP-Secret) et ICP-D (ICP RED)
- Service d'authentification fédérée d'entreprise
- Service de données d'identité d'entreprise
- Service de gouvernance de l'accès d'entreprise

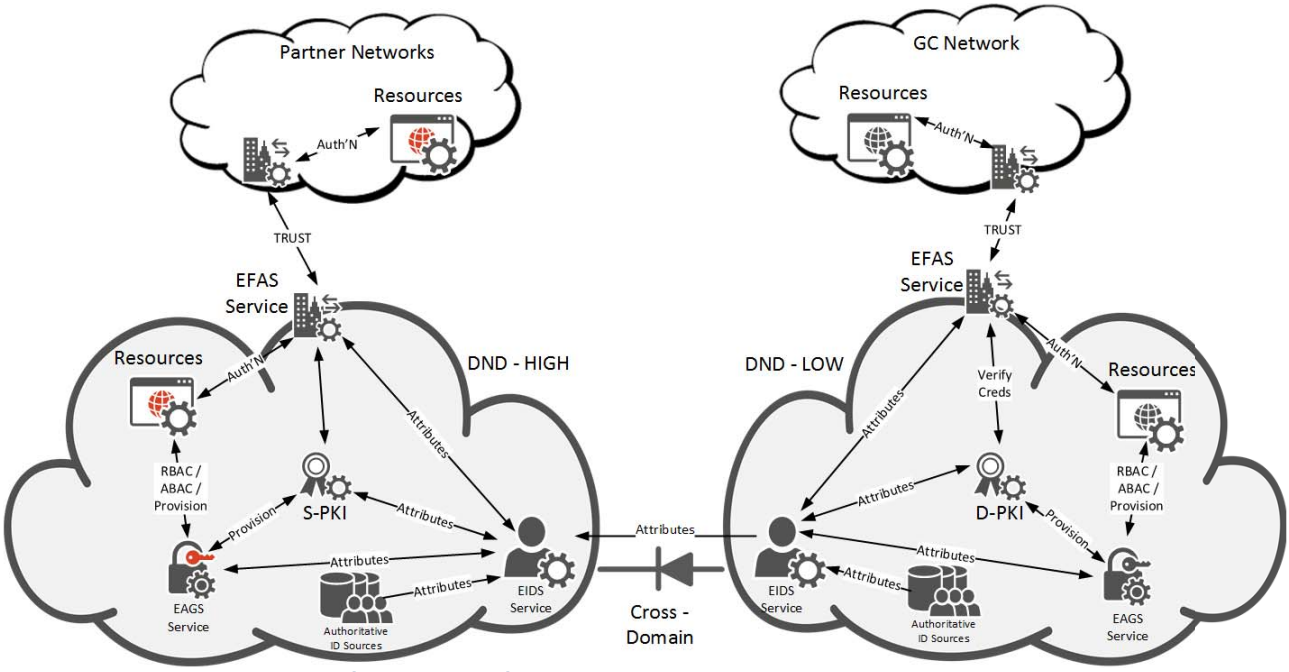

Figure 2: Représentation opérationnelle de l'architecture de la GIJIA future

L'ICP-S et l'ICP-D sont des services en place que le projet de GIJIA mettra à profit; il n'a pas pour but de les remplacer. Les autres services représentés dans la Figure 2 relèvent de la portée du projet de GIJIA.

EN	**FR**
Partner networks	Réseaux de partenaires
Resources	Ressources
Auth'N	Authentification
Trust	Confiance
EFAS service	Service d'authentification fédérée d'entreprise
Auth'N	Authentification
Resources	Ressources
RBAC/ABAC	RBAC/ABAC
Provision	Approvisionnement

EAGS service	Service de gouvernance de l’accès d’entreprise
Provision	Approvisionnement
S-PKI	ICP-S
Attributes	Attributs
EIDS service	Service de données d’identité d’entreprise
Attributes	Attributs
Attributes	Attributs
Authorative ID sources	Sources d’identité faisant autorité
DND – high	Environnement de niveau de classification élevé du MDN
Attributes	Attributs
Cross-domain	Interdomaines
DND – low	Environnement de niveau de classification faible du MDN
EIDS service	Service de données d’identité d’entreprise
Attributes	Attributs
Attributes	Attributs
Attributes	Attributs
Attributes	Attributs
Authorative services	Services d’autorisation
EAGS service	Service de gouvernance de l’accès d’entreprise
Provision	Approvisionnement
D-PKI	ICP-D
RBAC/ABAC	RBAC/ABAC
Provision	Approvisionnement
Verify creds	Vérification des justificatifs d’identité
Resources	Ressources
Auth’N	Authentification
EFAS service	Service d’authentification fédérée d’entreprise
Trust	Confiance
Auth’N	Authentification
Resources	Ressources
GC network	Réseau du GC

Service de données d'identité d'entreprise

Le service de données d'identité d'entreprise est représenté à la Figure 3.

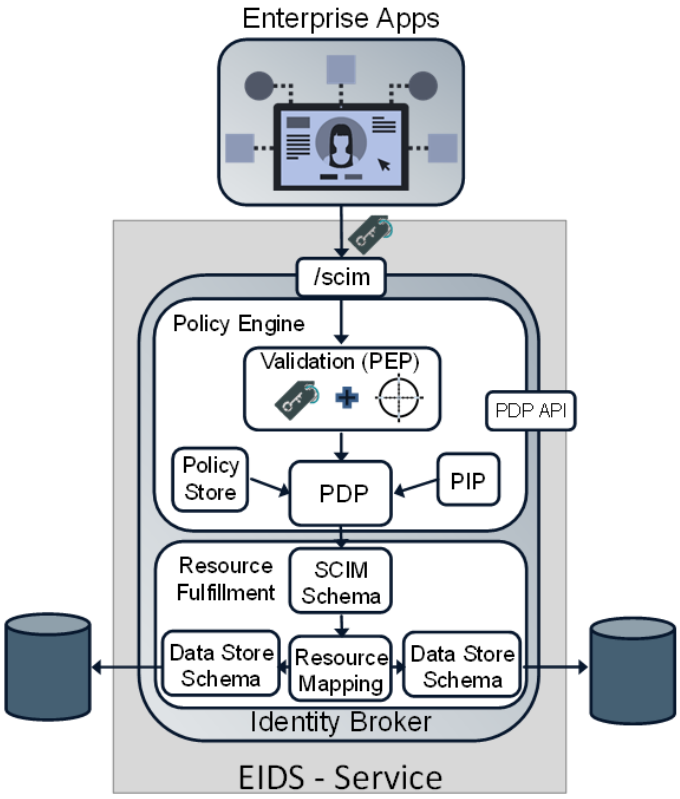

Figure 3: Architecture future de la GIJIA – Service de données d'identité d'entreprise

EN	**FR**
Enterprise apps	Applications d'entreprise
/scim	/scim
Policy engine	Moteur de politiques
Validation (PEP)	Validation (PEP)
Policy store	Dépôt de politiques
PDP	PDP
PIP	PIP
PDP API	API du PDP
Resource fulfillment	Exécution des ressources
SCIM schema	Schéma SCIM
Data store schema	Schéma du dépôt de données
Resource mapping	Mappage des ressources
Data store schema	Schéma du dépôt de données
Identity broker	Courtier des services d'identité
EIDS - service	Service de donnée d'identité d'entreprise

Le service de données d'identité d'entreprise est le point d'application de la politique (Policy Enforcement Point [PEP])[1] qui se rattache aux données d'identité faisant autorité. Les éléments suivants seront essentiels à la mise en œuvre réussie du service de données d'identité d'entreprise :

- Création d'un modèle de données d'identité normalisé pour le MDN qui comprend :
    - o des attributs d'entreprise;
    - o des attributs pour les communautés d'intérêts;
    - o des attributs locaux.
- Désignation des sources faisant autorité pour les attributs d'identité.
- Application de la norme SCIM (System for Cross Domain Identity Management) à l'appui de l'interopérabilité des identités.
- Élaboration de politiques pour permettre l'échange de données d'identité.
- Mise en place d'une gouvernance pour assurer l'application des politiques établies.

Service d'authentification fédérée d'entreprise

Le service d'authentification fédérée d'entreprise est représenté à la Figure 4.

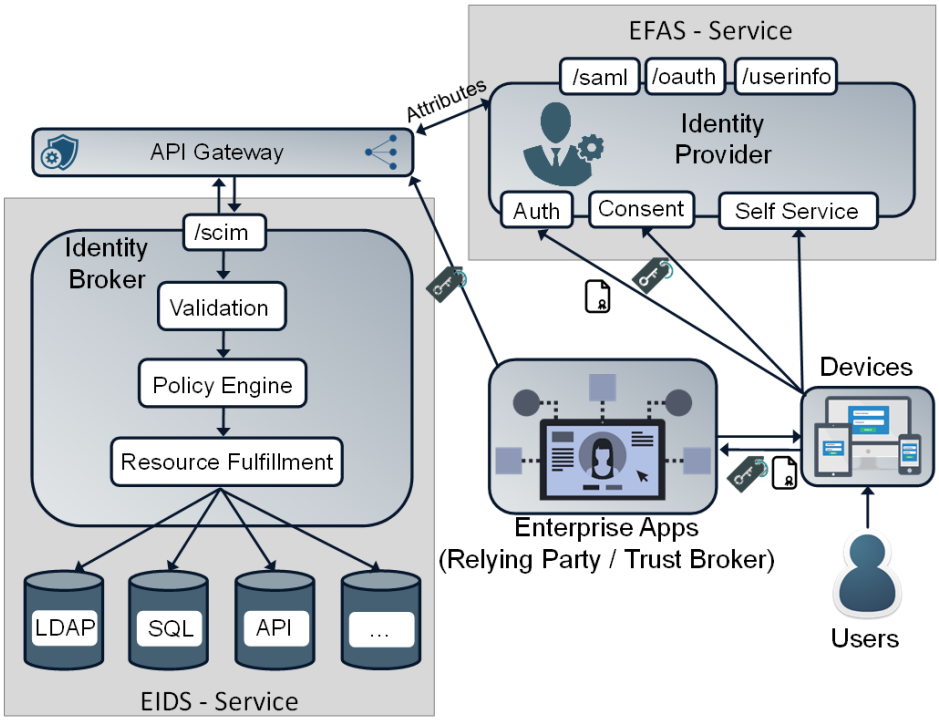

Figure 4 : Architecture future de la GIJIA – Service d'authentification fédérée d'entreprise

EN	FR
API gateway	Passerelle API
/scim	/scim
Identity broker	Courtier des services d'identité
Validation	Validation

[1] Les définitions de « Policy Enforcement Point » (PEP), « Policy Decision Point » (PDP) et « Policy Information Point » (PIP) se trouvent dans la norme ouverte XACML disponible auprès d'OASIS.

Policy engine	Moteur de politiques
Resource fulfillment	Exécution des ressources
LDAP	LDAP
SQL	SQL
APO	API
EIDS – service	Service de données d'identité d'entreprise
EFAS – service	Service d'authentification fédérée d'entreprise
Attributes	Attributs
/saml	/saml
/oauth	/oauth
/userinfo	/userinfo
Identity provider	Fournisseur d'identité
Auth	Authentification
Consent	Consentement
Self service	Libre-service
Devices	Appareils
Users	Utilisateurs
Enterprise apps (relying party/trust broker)	Applications d'entreprise (partie utilisatrice /courtier des services d'identité)

Le service d'authentification fédérée d'entreprise agit en tant que fournisseur d'identité. Le service d'authentification fédérée d'entreprise permet l'utilisation des normes ouvertes actuelles comme SAML (Security Assertion Mark-up Language), OIDC (OpenID Connect), OAuth et WS-Federation. Le service d'authentification fédérée d'entreprise pourra être adapté afin de suivre l'évolution des normes. Le service d'authentification fédérée d'entreprise est le courtier de confiance qui relie le MDN, les autres ministères et organismes fédéraux ainsi que les autres partenaires externes.

Service de gouvernance de l’accès d’entreprise

Le service de gouvernance de l’accès d’entreprise est représenté à la Figure 5.

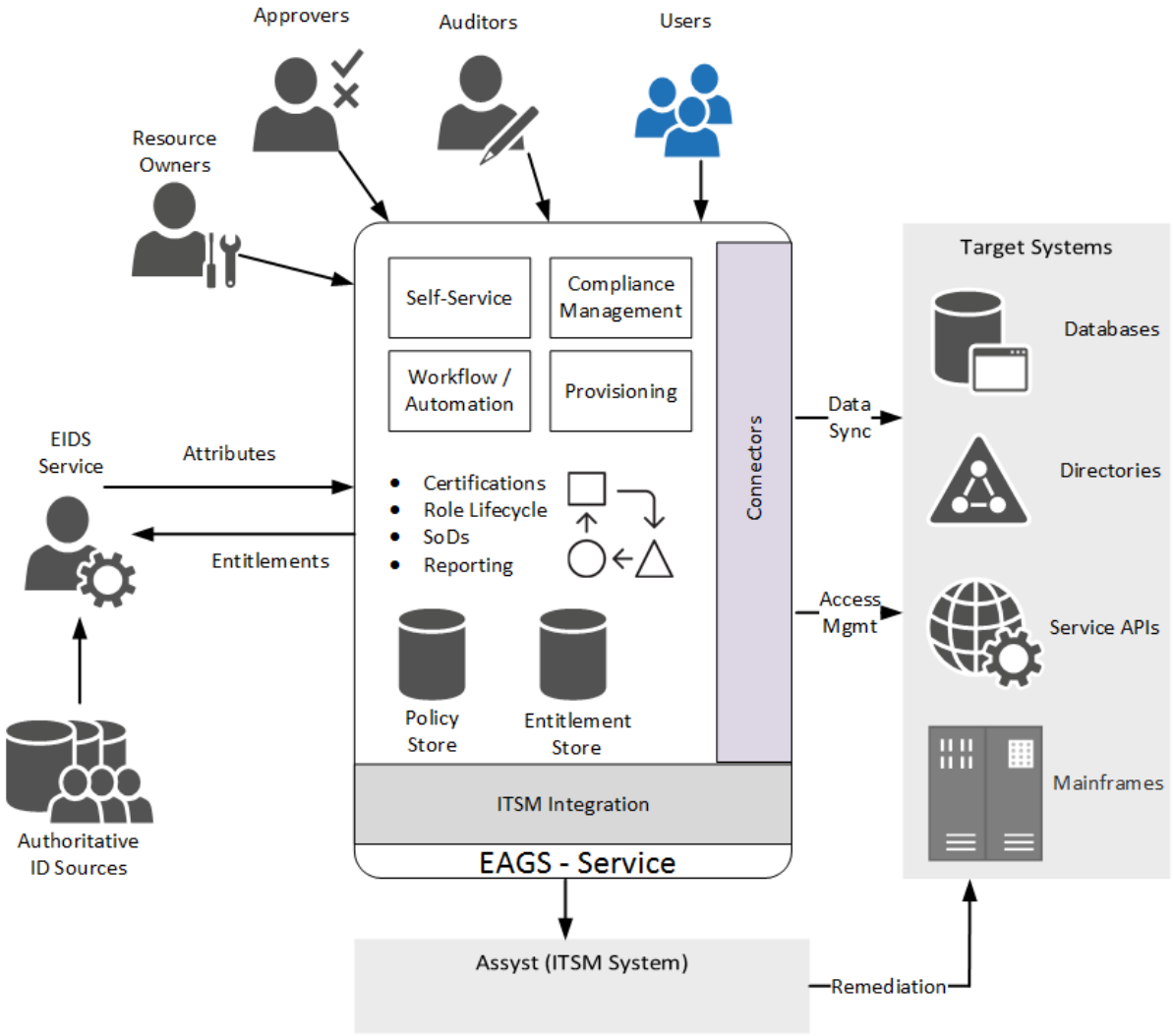

Figure 5 : Architecture future de la GIJIA – Service de gouvernance de l’accès d’entreprise

EN	FR
Users	Utilisateurs
Auditors	Vérificateurs
Approvers	Approbateurs
Resource owners	Responsables des ressources
EIDS service	Service de données d’identité d’entreprise
Authorative ID sources	Sources d’identité faisant autorité
Attributes	Attributs
Entitlements	Droits
Self-service	Libre-service
Compliance management	Gestion de la conformité
Workflow/automation	Flux de travail/automatisation
Provisioning	Approvisionnement
Certifications	Certifications

Role lifecycle	Cycle de vie du rôle
SoDs	Séparation des tâches
Reporting	Rapports
Policy store	Dépôt de politiques
Entitlement store	Dépôt des droits
ITSM intergration	Intégration de la GSTI
EAGS service	Service de gouvernance de l'accès d'entreprise
Connectors	Connecteurs
Assist (ITSM system)	Assyst (système de GSTI)
Remediation	Correctifs
Data sync	Synchronisation des données
Access mgmt	Gestion de l'accès
Target systems	Systèmes cibles
Databases	Bases de données
Directories	Répertoires
Service APIs	API du service
Mainframes	Ordinateurs centraux

Le service de gouvernance de l'accès d'entreprise sera le principal système de gestion de l'accès pour le MDN. Dans le cadre de la capacité de GIJIA, le service de gouvernance de l'accès d'entreprise s'intégrera aux bases de données, aux répertoires et aux services nécessitant une authentification et une autorisation.

ANNEXE C

Offres et évaluation des prix des produits

1 Renseignements complémentaires

Les participants à la demande de renseignements (DDR) sont invités à fournir des estimations de coûts confidentielles non contraignantes pour les produits livrables des projets énumérés dans la présente annexe qui les intéressent et pour lesquels ils ont de l'expérience. Les réponses partielles sont les bienvenues.

Comme indiqué à l'annexe A, la stratégie d'approvisionnement n'est pas encore arrivée à maturité. Le niveau de détail fourni par les intervenants de l'industrie aidera l'équipe responsable du projet à finaliser son analyse de rentabilisation.

2 Information détaillée des tableaux d'établissement des prix

Les tableaux de la présente annexe doivent être utilisés par les répondants à la DDR afin de fournir des prix pour les livrables du projet, par ailleurs, on encourage les participants de la DDR à inclure des renseignements supplémentaires sur des pages distinctes. Aux fins du projet, deux produits logiciels ont été désignés (voir la Figure 1).

Exigences relatives aux produits logiciels de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)

- Produit logiciel nº 1. Courtier des services d'identité comprenant ce qui suit :
    - Service de données d'identité d'entreprise. Un service de gestion d'identité normalisé fondé sur des politiques permettant de gérer l'échange de données d'identité entre les services de fournisseurs de renseignements sur l'identité et les services de gestion de l'accès et des justificatifs d'identité qui ont besoin de renseignements sur l'identité.
    - Service de gouvernance de l'accès d'entreprise. Un service de gouvernance normalisé pour la gestion des droits d'accès, des politiques et des flux de travail, tel que décrit à l'annexe B.
- Produit logiciel nº 2. Service d'authentification fédérée d'entreprise. Un service d'identité fédérée normalisé pour étendre les identités des Forces armées canadiennes (FAC) et du ministère de la Défense nationale (MDN) aux réseaux du gouvernement du Canada et de ses partenaires. Ce service est décrit plus en détail à l'annexe B.

Exigences relatives à l'intégration

- Intégration du courtier des services d'identité (service de données d'identité d'entreprise et service de gouvernance des accès d'entreprise) et le service d'authentification fédérée d'entreprise l'un à l'autre ainsi qu'aux réseaux, aux répertoires d'identité, aux systèmes de justificatifs d'identité et aux systèmes de contrôle de l'accès physique du MDN existants. L'établissement des coûts relatifs à l'intégration doit être décomposé en un certain nombre de scénarios.
- Intégration de sources de données faisant autorité au service de données d'identité d'entreprise.
- Intégration de ressources physiques au service de gouvernance de l'accès d'entreprise et au service d'authentification fédérée d'entreprise – authentification gérée par la capacité de GIJIA et autorisation gérée selon la ressource.
- Intégration de ressources physiques au service de gouvernance de l'accès d'entreprise et au service d'authentification fédérée d'entreprise – authentification et autorisation gérées par la capacité de GIJIA.
- Intégration des ressources logiques au service de gouvernance de l'accès d'entreprise et au service d'authentification fédérée d'entreprise – authentification gérée par la capacité de GIJIA et autorisation gérée selon la ressource.
- Intégration des ressources logiques au service de gouvernance de l'accès d'entreprise et au service d'authentification fédérée d'entreprise – authentification et autorisation gérées par la capacité de GIJIA.

- Intégration de la capacité de GIJIA au Réseau étendu de la Défense (RED) [la capacité de GIJIA doit être modulable et évolutive pour permettre l'intégration aux systèmes d'entreprise du RED qui ont leur propre capacité supplémentaire de gestion de l'accès].
- Intégration de la capacité de GIJIA à l'Infrastructure de réseau secret consolidé (IRSC) [la capacité de GIJIA doit être modulable et évolutive pour permettre l'intégration aux systèmes d'entreprise de l'IRSC qui ont leur propre capacité supplémentaire de gestion de l'accès].
- Intégration de la capacité de GIJIA au système de gestion de l'accès de l'édifice de la région de la capitale nationale (la capacité de GIJIA doit être modulable et évolutive pour permettre l'intégration aux autres systèmes de contrôle de l'accès physique, p. ex., aux autres bases, escadres et stations).

La Figure 1 montre l'interaction entre les différents composants de GIJIA. Le service de données d'identité d'entreprise fournit des attributs d'identité, qui proviennent de sources de données d'identité faisant autorité, aux autres services de GIJIA aux fins d'émission de justificatifs d'identité, de contrôle de l'accès aux ressources locales ainsi que de contrôle de l'accès aux sources externes par l'intermédiaire de la fédération. La Figure 1 montre que les services de GIJIA doivent fonctionner de manière synchronisée dans les environnements de niveau de classification faible ainsi que dans les environnements de niveau de classification élevé du MDN.

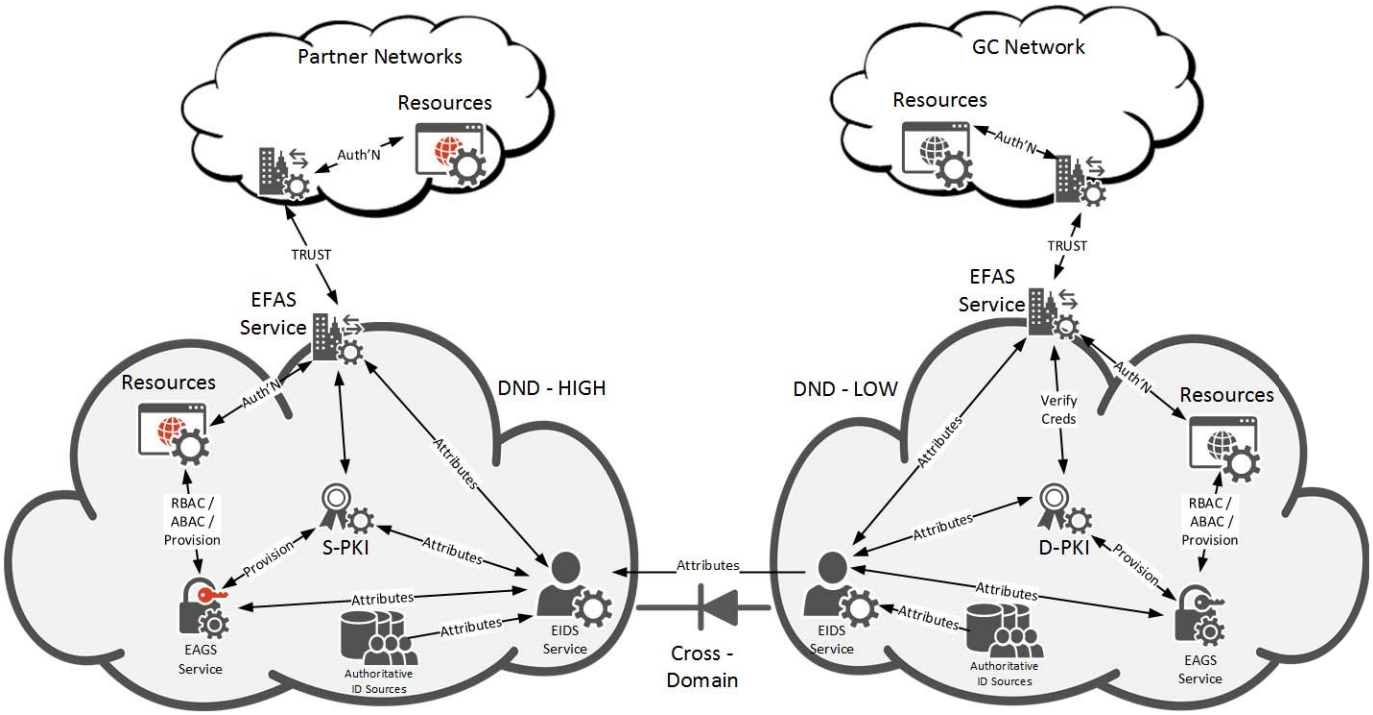

Figure 1 : Représentation des composants livrables de la GIJIA dans une architecture de haut niveau

EN	FR
Partner networks	Réseaux de partenaires
Resources	Ressources
Auth'N	Authentification
Trust	Confiance
EFAS service	Service d'authentification fédérée d'entreprise
Auth'N	Authentification
Resources	Ressources
RBAC/ABAC	RBAC/ABAC
Provision	Approvisionnement
EAGS service	Service de gouvernance de l'accès d'entreprise
Provision	Approvisionnement
S-PKI	ICP-S

Attributes	Attributs
EIDS service	Service de données d'identité d'entreprise
Attributes	Attributs
Attributes	Attributs
Authorative ID sources	Sources d'identité faisant autorité
DND – high	Environnement de niveau de classification élevé du MDN
Attributes	Attributs
Cross-domain	Interdomaines
DND – low	Environnement de niveau de classification faible du MDN
EIDS service	Service de données d'identité d'entreprise
Attributes	Attributs
Attributes	Attributs
Attributes	Attributs
Attributes	Attributs
Authorative services	Services d'autorisation
EAGS service	Service de gouvernance de l'accès d'entreprise
Provision	Approvisionnement
D-PKI	ICP-D
RBAC/ABAC	RBAC/ABAC
Provision	Approvisionnement
Verify creds	Vérification des justificatifs d'identité
Resources	Ressources
Auth'N	Authentification
EFAS service	Service d'authentification fédérée d'entreprise
Trust	Confiance
Auth'N	Authentification
Resources	Ressources
GC network	Réseau du GC

Aux fins de l'établissement des coûts, le MDN a cerné les produits livrables supplémentaires et connexes suivants qui, à son avis, seront nécessaires. Les prix des produits livrables et des sous--éléments connexes doivent tenir compte de ce qui suit :

- Matériel informatique. Matériel informatique nécessaire pour exécuter le logiciel de GIJIA.
- Amélioration des processus. Documentation des nouveaux processus opérationnels qui seront nécessaires pour permettre l'exécution des services de GIJIA, y compris les règles et les procédures opérationnelles ainsi que les postes créés ou modifiés au sein de l'organisation.
- Gestion de projet. Exigences que doit respecter l'équipe de gestion de projet tout au long du cycle de vie du projet.
- Conception technique. Conception technique de la capacité de GIJIA.
- Essais opérationnels et évaluation. Essais d'acceptation sur place visant à s'assurer que les objectifs en matière de GIJIA sont atteints dans l'environnement opérationnel.
- Installation. Installation et configuration des systèmes aux emplacements du MDN.
- Production des documents suivants :
    - structure de répartition du travail (SRT) du projet et dictionnaire de la SRT;
    - calendrier du projet;
    - plan d'assurance de la qualité du projet;
    - plan de gestion des risques du projet;
    - document des exigences du système;
    - plan d'ingénierie du système;
    - concept des opérations;
    - exigences d'interface de service;
    - spécification de conception du système;

- plan de vérification et de validation;
- plan de mise en œuvre du système;
- plan de soutien du cycle de vie du système;
- documents liés à la conception et à la configuration;
- rapports d'essai;
- documents de dépannage pour le soutien en service (p. ex., directives, instructions permanentes d'opérations).

- Formation. Formations suivantes visant à répondre aux besoins des utilisateurs et aux exigences en matière de soutien du MDN et des FAC en ce qui concerne la capacité de GIJIA :
  - Utilisateur général. Formation commune des utilisateurs à l'intention du personnel du MDN et des FAC qui utilisera les nouvelles capacités.
  - Utilisateur avancé. Formation à l'intention des utilisateurs avancés pour les grands utilisateurs du système (p. ex., ceux qui assurent le soutien local aux communautés d'utilisateurs généraux et de la direction dans les situations qui ne nécessitent pas le recours au soutien d'un centre d'aide).
  - Utilisateur technique. Formation technique à l'intention du personnel qui assurera l'exploitation, l'administration, la maintenance et le soutien du système.
- Soutien en service. Estimation du prix par an pour prendre en charge la GIJIA après le déploiement, y compris la formation du nouveau personnel affecté à des rôles d'utilisateurs du système.

2 Information détaillée des tableaux d'établissement des prix

Lorsque vous remplissez les tableaux d'établissement des prix, la colonne « Description » doit être utilisée pour inclure les détails concernant le sous--élément livrable, le cas échéant.

La colonne « Prix total » doit indiquer les coûts associés au sous--élément livrable.

Tous les prix doivent être précisés dans leur devise d'origine, qui doit être indiquée dans la colonne « Devise ».

Ajoutez toute information supplémentaire pertinente dans la section « Remarques » pour aider l'équipe de projet à mieux comprendre le prix total estimé.

Tableau 1 – Courtier des services d'identité (y compris le service de données d'identité d'entreprise et le service de gouvernance de l'accès d'entreprise)

Sous-éléments livrables	Description	Prix total ($)	Devise	Remarques
Matériel				
Logiciels				

Tableau 2 – Service d'authentification fédérée d'entreprise

Sous-éléments livrables	Description	Prix total ($)	Devise	Remarques
Matériel				
Logiciels				

Tableau 3 – Intégration

Sous-éléments livrables	Description	Prix total ($)	Devise	Remarques
Matériel				
Logiciels				

Tableau 4 – Livrables connexes

Sous-éléments livrables	Description	Prix total ($)	Devise	Remarques
Gestion de projet				
Amélioration des processus				
Conception technique				
Intégration des systèmes				
Essais opérationnels et évaluation				
Installation				
Documents				

Sous-éléments livrables	Description	Prix total ($)	Devise	Remarques
Formation générale et formation des utilisateurs avancés				
Formation technique des utilisateurs				
Soutien annuel				

ANNEXE D

RÈGLES DE CONSULTATION

Introduction

Ces règles de consultation s'appliquent à l'ensemble du processus de consultation et en particulier aux rencontres individuelles.

Règles et principes généraux

1. Un des principes fondamentaux de la consultation précoce des entreprises est que celle-ci doit être réalisée avec le plus haut degré de justice et d'équité entre toutes les parties. Nulle personne ou organisation ne doit recevoir ni sembler avoir reçu un quelconque avantage inhabituel ou injuste par rapport aux autres.
2. Les présentes règles de consultation précoce entreront en vigueur à la publication du document de demande de renseignements (DDR), et prendront fin au moment de la publication de la demande de propositions (DP).
3. Le processus de consultation comprendra la DDR, des rencontres individuelles et une éventuelle ébauche d'une ou de plusieurs DP et tout autre processus jugé nécessaire par le responsable des achats.
4. Afin de maximiser les avantages du processus de consultation, le Canada peut s'efforcer de solliciter les commentaires des participants sur diverses questions soulevées.
5. Toutes les solutions, idées ou questions traitées au cours des rencontres individuelles feront l'objet d'un examen plus poussé par le Canada.
6. Une version provisoire de la ou des DP, qui fera l'objet d'un dernier examen avant la publication de la ou des DP officielles, peut être mise à la disposition des participants qui satisfont aux exigences de sécurité.
7. Le Canada ne divulguera pas de renseignements exclusifs ou délicats sur le plan commercial concernant un participant à d'autres participants ou à des tiers, sauf dans la mesure où la loi l'exige.
8. Les répondants éventuels sont informés que tout renseignement soumis au Canada dans le processus de consultation peut être utilisé par le Canada dans l'élaboration d'une DP concurrentielle.

Modalités

Les modalités qui suivent s'appliquent au processus de consultation. Afin de favoriser le dialogue ouvert, les participants conviennent de ce qui suit :

1. Les participants doivent exposer leurs points de vue quant à l'approvisionnement et fournir des solutions positives aux questions soulevées.

2. Aucun enregistrement audio ou visuel ne sera autorisé pendant les rencontres individuelles.

3. Les participants doivent prévenir le Canada s'ils prévoient être accompagnés d'un avocat au moment de la rencontre individuelle. Le Canada se réserve le droit de refuser toute réunion en présence d'un avocat.

4. **Les participants doivent présenter leurs demandes ou leurs commentaires seulement à l'autorité contractante de TPSGC ou aux représentants autorisés du Canada,** conformément aux avis provenant de l'autorité contractante. Toute communication avec des représentants non autorisés du Canada peut faire l'objet d'une divulgation complète par le Canada sur le site Achats et ventes.

5. L'inscription est requise pour participer à la Journée de l'industrie, et seuls les fournisseurs potentiels peuvent s'inscrire. Les Journées de l'industrie ne sont pas ouvertes au public.

6. Le Canada n'est pas tenu de publier de DP ou de négocier de contrat pour les projets.
7. Si le Canada publie une ou plusieurs DP, les modalités en seront définies à l'entière discrétion du Canada.

8. Le Canada ne remboursera pas les frais engagés par une personne ou une entité pour participer à ce processus de consultation des entreprises.

9. La participation n'est pas obligatoire. La non-participation à ce processus de consultation de la DDR n'empêche pas un soumissionnaire de présenter une proposition en réponse à une DP définitive.

10. La documentation préliminaire (DP, plan d'évaluation, énoncé des travaux) sera envoyée aux participants qui satisfont aux exigences de sécurité en vue de solliciter leurs commentaires.

11. Dans le cadre de discussions officieuses et négociations de bonne foi, TPSGC et le participant doivent faire tous les efforts raisonnables pour régler les différends et les réclamations ou pour mettre fin à des controverses découlant de ce processus de consultation, ou qui sont liés d'une quelconque façon à celui-ci.

ANNEXE E

DÉTAILS SUR LA JOURNÉE DE L'INDUSTRIE ET LES RENCONTRES INDIVIDUELLES ET INSCRIPTION

Journée de l'industrie

Tous les répondants de l'industrie intéressés sont invités à assister à une présentation de groupe non classifiée à l'intention de l'industrie qui aura lieu à Ottawa, en Ontario. Cette journée de l'industrie permettra au personnel de projet du ministère de la Défense nationale (MDN) de présenter un aperçu du projet, d'obtenir les commentaires des membres de l'industrie tout en leur permettant de poser des questions à Services publics et Approvisionnement Canada (SPAC), à la Direction de la sécurité industrielle canadienne (DSIC), au MDN et à Innovation, Sciences et Développement économique Canada (ISDE). La Journée de l'industrie sera non classifiée. Les fournisseurs qui ne participent pas à la Journée de l'industrie sont tout de même invités à soumettre une réponse à cette DDR.

Détails sur la Journée de l'industrie :

Date : Le lundi 22 juillet 2019

Heure : De 9 h 30 à midi

Lieu : Salle Palladium, Mess des caporaux et soldats du Canal Rideau
3e étage, 4, promenade Queen Elizabeth, Ottawa (Ontario)

Date limite d'inscription : Le 15 juillet 2019. Les fournisseurs doivent s'inscrire avant la date limite d'inscription.

Veuillez arriver trente minutes avant le début de la Journée de l'industrie afin de vous inscrire au registre. Les participants sont responsables de leur transport, de leur hébergement, de leurs repas, de leur stationnement et de toute autre dépense.

WebEx : Cet événement sera également disponible via WebEx à la date et à l'heure indiquées ci-dessus. Les fournisseurs souhaitant s'inscrire via WebEx sont invités à envoyer un courrier électronique à l'adresse suivante: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca.

Rencontres individuelles

L'intention des rencontres individuelles est de tenir des discussions avec les membres de l'industrie.

Les fournisseurs sont avisés que même si les discussions lors des rencontres individuelles fourniront plus de précisions sur les exigences du MDN, ils ne sont pas tenus de fournir une réponse complète à la DDR. Les fournisseurs ne sont pas tenus d'assister à une rencontre individuelle. Les fournisseurs qui ne participent pas sont tout de même invités à soumettre une réponse à cette DDR.

Détails sur les rencontres individuelles :

Format : Créneaux d'une heure par fournisseur

Période : Du 22 au 24 juillet 2019

Plages disponibles :

- Le 22 juillet 2019, de 13 h à 16 h 30
- Le 23 juillet 2019, de 8 h à 16 h
- Le 24 juillet 2019, de 8 h à 16 h

Lieu : Salle Athena, Mess des caporaux et des soldats du Canal Rideau,
3e étage, 4, promenade Queen Elizabeth, Ottawa (Ontario)

Date limite d'inscription : Le 15 juillet 2019. Les fournisseurs doivent s'inscrire avant la date limite d'inscription. La tenue d'une réunion n'est pas garantie avec les fournisseurs qui ne s'inscrivent pas avant la date limite. L'inscription aux rencontres individuelles se déroulera selon le principe du premier arrivé, premier servi; toutefois, la disponibilité du MDN et du fournisseur influera sur le calendrier des réunions.

Les fournisseurs sont priés d'arriver quinze minutes avant leur rencontre afin de s'inscrire au registre. Le transport, l'hébergement, les repas, le stationnement et toutes les autres dépenses sont aux frais des participants.

Processus d'inscription à la rencontre individuelle et à la journée de l'industrie

Pour s'inscrire, les fournisseurs **doivent soumettre** à l'autorité contractante de TPSGC indiquée ci-dessous les renseignements suivants :

- le nombre de personnes qui participeront à la journée de l'industrie ou à la rencontre individuelle;
- l'adresse courriel et le numéro de téléphone de la personne-ressource;
- la langue de préférence pour les rencontres individuelles : français ou anglais.

Veuillez prendre note de ce qui suit :

- En raison du nombre limité de places, chaque fournisseur peut inscrire **un maximum de quatre (4) représentants** qui assisteront à la Journée de l'industrie et à la rencontre individuelle.
- Les noms de tous les participants peuvent être publiés.

Autorité contractante pour la Journée de l'industrie et les rencontres individuelles

À l'attention de : Chantale Norris ou Patrick Scott
Travaux publics et Services gouvernementaux Canada
Place du Portage, Phase III, bureau 8C2
11, rue Laurier, Gatineau (Québec) K1A 0S5

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Il est préférable de communiquer par courriel.

Présentation de renseignements avant la Journée de l'industrie et les rencontres individuelles

Les fournisseurs peuvent soumettre des commentaires ou des questions par écrit dans l'une ou l'autre des deux langues officielles à l'autorité contractante susmentionnée.

En prenant part à la Journée de l'industrie et à une rencontre individuelle, les participants acceptent les règles de consultation détaillées à l'annexe D.

Communication avec les entreprises

Le Canada mettra par écrit les préoccupations, les questions et les suggestions formulées lors de la Journée de l'industrie, avec les réponses. Pendant le processus de consultation, l'autorité contractante de TPSGC peut choisir de communiquer avec les participants inscrits par courriel plutôt que d'afficher d'autres avis sur le Service électronique d'appels d'offres du gouvernement (SEAOG). Pour assurer l'équité, la transparence et l'intégrité du processus, TPSGC partagera avec l'industrie les renseignements découlant du processus (à l'exclusion des renseignements désignés exclusifs ou confidentiels).

L’exposé présenté par le Canada, les réponses aux questions soulevées au cours de la Journée de l’industrie et la liste des participants seront publiés sur le SEAOG après l’activité.

Langue

Tous les documents seront accessibles dans les deux langues officielles.

ANNEXE F

DEMANDE DE PARRAINAGE DE SÉCURITÉ

INTRODUCTION

Comme la version provisoire et définitive de la ou des DDR ainsi que le contrat subséquent pourraient contenir de l'information classifiée, l'un des principaux objectifs de la présente DDR est d'encadrer les fournisseurs intéressés qui ne satisfont actuellement pas aux exigences de sécurité pour qu'ils obtiennent les attestations de sécurité requises.

DEMANDE DE PARRAINAGE POUR UNE ATTESTATION DE SÉCURITÉ

Les fournisseurs dont l'organisation aura besoin d'attestations de sécurité valides délivrées par la Direction de la sécurité industrielle canadienne (DSIC) sont invités à amorcer le processus d'autorisation de sécurité dès que les clauses de sécurité seront achevées par une modification à la DDR publiée sur le site Achats et ventes. Les demandes de parrainage peuvent être envoyées par courriel à l'autorité contractante de TPSGC indiquée ci-dessous.

Autorité contractante principale pour le parrainage de sécurité :

Chantale Norris ou Patrick Scott
Services publics et Approvisionnement Canada (SPAC)
Place du Portage, Phase III, bureau 8C2
11, rue Laurier, Gatineau (Québec) K1A 0S5

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Il est préférable de communiquer par courriel.

Il incombe au fournisseur de veiller à ce que l'information requise concernant l'attestation de sécurité soit communiquée à temps à l'autorité requérante ou à la DSIC. La demande doit comprendre les renseignements suivants :

a. la dénomination sociale de l'entreprise;
b. la dénomination commerciale, si elle est différente de la dénomination sociale;
c. l'adresse postale;
d. l'adresse municipale, si elle est différente de l'adresse postale;
e. le numéro de téléphone de l'entreprise;
f. le prénom et le nom de famille de la personne-ressource (représentant au Canada);
g. le titre de la personne-ressource;
h. le numéro de téléphone de la personne-ressource;
i. l'adresse courriel de la personne-ressource;
j. la langue de préférence (anglais ou français).

À la réception de la demande de parrainage, la DSIC communiquera avec le fournisseur pour achever la collecte des renseignements requis.

Pour obtenir des renseignements sur les exigences de sécurité, le fournisseur doit communiquer avec la DSIC au 866-368-4646, ou au 613-948-4176 dans la région de la capitale nationale. Site Web de la Direction de la sécurité industrielle canadienne : https://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html.

Aucun coût direct n'est exigé aux fournisseurs qui souhaitent obtenir une attestation de sécurité d'installation. Il est toutefois possible qu'ils aient à assumer des coûts indirects découlant de l'obligation qui leur est faite de respecter les normes minimales, comme les frais liés à l'installation de mécanismes pour la protection des documents, s'il y a lieu.