National Défense
Defence nationale

Chief Review Services Chef - Service d'examen
CRS CS Ex

Revu par le CS Ex conformément à la *Loi sur l'accès à l'information* (LAI). L'article ou les articles applicables de la LAI sont cités lorsqu'il y a prélèvement de l'information.

Examen de l'infrastructure à clé publique du MDN

Mars 2005

7050-7-19 (CS Ex)

Canada

MISE EN GARDE

Le présent examen a été effectué dans le cadre du Plan de travail approuvé du CS Ex. Ses conclusions n'ont pas le poids de celles d'une vérification et elles ne doivent pas être considérées comme telles. Bien qu'elles soient suffisantes pour permettre la formulation de recommandations aux fins d'examen par la direction, les appréciations fournies et les conclusions tirées ne sont pas fondées sur l'enquête et les preuves rigoureuses exigées lors d'une vérification.

SYNOPSIS

Le présent rapport renferme les résultats d'un examen portant sur le système d'infrastructure à clé publique (ICP) du ministère de la Défense nationale (MDN). L'ICP est une importante infrastructure qui sert à appuyer l'échange protégé de données et de communications électroniques sensibles. Le MDN utilise une ICP d'entreprise depuis la fin de 2002[1], et un grand nombre de nouvelles applications d'ICP sont prévues en supposant que des services d'ICP soient disponibles et fiables. Dans le cadre de son plan de travail 2003-2004 – 2004-2005, le Chef – Service d'examen (CS Ex), en collaboration avec AEPOS Technologies Corporation (AEPOS), a effectué un examen afin d'évaluer la capacité de l'ICP du MDN à fournir des services protégés aux utilisateurs et aux applications du Ministère.

L'examen a porté sur des aspects clés des structures de gouvernance, des politiques, des processus, des ressources et de l'équipement qui appuient collectivement la gestion et le fonctionnement de l'ICP du MDN. Nous avons également examiné les futures applications d'ICP du Ministère, principalement le Système de traitement des messages militaires (STMM), qui est en voie de mise en place dans le domaine classifié[2], afin d'évaluer leur incidence sur le soutien et les processus d'infrastructure actuels de l'ICP du Ministère. L'examen ne visait pas à évaluer les aspects techniques du produit Entrust® ni sa sélection à titre de mécanisme approuvé par le Centre de la sécurité des télécommunications (CST) pour l'ICP.

Environ 60 000 cartes à puce d'ICP ont été distribuées aux employés du MDN et aux membres des Forces canadiennes (FC) dans le cadre de la mise en place du système actuel d'ICP; plus de la moitié de ces cartes ont expiré. Même si certains groupes d'utilisateurs comme la Police militaire, les Finances et les Ressources humaines l'emploient régulièrement pour protéger des messages électroniques sensibles, l'ICP n'est pas largement utilisée au sein du Ministère. Par ailleurs, de nombreux employés du MDN ne sont pas suffisamment conscients qu'il faut protéger l'information électronique sensible ou que la technologie est facilement accessible sur la plupart des postes de travail. Bon nombre des questions soulevées dans le présent examen ne sont pas particulières à l'ICP du MDN – par exemple, la nécessité de mieux définir les besoins fonctionnels complets et de renforcer les structures de gouvernance et les processus horizontaux sont des problèmes systémiques dont le CS Ex a fait état dans des rapports précédents sur d'autres systèmes/projets ministériels. La direction doit s'appliquer à résoudre ces questions avant que les utilisateurs actuels puissent faire entièrement confiance à l'ICP et avant que les nouvelles applications d'ICP puissent recevoir un soutien efficace. L'ICP est plus qu'une simple solution technologique; elle doit être gérée dans le contexte des besoins fonctionnels et opérationnels du MDN et des FC.

Les plans d'action de la direction fournis par le SMA(GI) montrent qu'une attention constructive est portée à la majorité des recommandations figurant dans le présent rapport. Par la même occasion, nous encourageons la direction à prendre certaines mesures plus tôt que prévu, particulièrement en ce qui concerne l'élaboration d'une feuille de route de l'ICP du MDN, l'éclaircissement des rôles et des responsabilités de l'ICP du MDN et la rationalisation du soutien et des processus d'infrastructure de l'ICP. À cet égard, des jalons provisoires relatifs aux plans d'action seront demandés par le biais des processus de suivi et de contrôle du CS Ex.

[1] *L'ICP actuelle fonctionne dans le domaine désigné (c.-à-d. l'intranet du MDN), qui sert à l'ensemble du trafic de données électroniques à usage général.*

[2] *Le domaine classifié est un réseau distinct du MDN qui est réservé au trafic de données électroniques classifiées. On entend par information classifiée les renseignements dont la compromission pourrait vraisemblablement porter préjudice à l'intérêt national. Elle est classée selon le degré de préjudice éventuel (c.-à-d. Confidentiel, Secret ou Très secret).*

TABLE DES MATIÈRES

SOMMAIRE DES RÉSULTATS

INTRODUCTION

L'économie d'aujourd'hui est fortement tributaire des communications et des transactions en ligne. Les particuliers et les organisations transmettent régulièrement des données sensibles et confidentielles (p. ex., transactions commerciales, données personnelles et contrats) sur des réseaux publics non protégés, en particulier Internet. De plus, les organisations recueillent et stockent une foule de renseignements électroniques sensibles qu'il faut protéger contre la modification ou l'accès non autorisé. Ce type d'environnement comporte de nombreux risques liés à la sécurité de l'information, d'où l'importance de valider et de vérifier l'identité d'une personne avant d'effectuer des communications et des transactions électroniques sensibles. Une infrastructure à clé publique (ICP)[3] est conçue pour relever ces défis et d'autres encore, en offrant des services de sécurité qui permettent d'atténuer les risques dans l'environnement numérique d'aujourd'hui.

Le ministère de la Défense nationale et les Forces canadiennes (MDN/FC) utilisent une ICP d'entreprise depuis la fin de 2002, et un grand nombre de nouvelles applications d'ICP sont prévues en supposant que des services d'ICP soient disponibles et fiables. Dans le cadre de son plan de travail de 2004, le Chef – Service d'examen (CS Ex), en collaboration avec AEPOS Technologies Corporation (AEPOS), a effectué un examen afin d'évaluer la capacité de l'ICP du MDN à fournir des services protégés et confidentiels aux utilisateurs et aux applications du Ministère. La planification de l'examen a débuté en mars 2004, l'examen a pris fin avant août 2004 et les résultats ont été communiqués en septembre/octobre 2004.

CONTEXTE

La technologie de l'ICP

Une ICP est un système regroupant du matériel, des logiciels, des politiques, des processus et des personnes qui peuvent appuyer une gamme de services de sécurité de l'information destinés à faire face aux risques que pose le traitement des communications et des transactions électroniques sensibles. Dès qu'une ICP a été mise en place dans une organisation, de nombreuses applications différentes (comme un système de courrier ou de messagerie électronique) peuvent utiliser l'infrastructure et les services de sécurité auxquels elle apporte un soutien.

[3] Une liste d'acronymes et d'abréviations figure à l'**annexe F**.

Les services de sécurité soutenus par une ICP sont les suivants :

- Authentification – qui sert à corroborer l'identité d'une personne, d'une entité ou d'un dispositif. L'authentification est souvent considérée comme l'exigence fondamentale la plus importante pour la conduite des activités dans un environnement électronique – c.-à-d. savoir à qui l'on traite.
- Confidentialité des données – qui permet de protéger l'information (en mémoire et pendant la transmission) contre toute divulgation non autorisée.
- Intégrité des données – qui permet de protéger l'information (en mémoire et pendant la transmission) contre toute modification non autorisée.
- Non-répudiation – qui empêche une personne d'affirmer faussement ne pas avoir créé, signé, envoyé ou reçu une transaction ou un document donné.

L'ICP se fonde sur les principes de la cryptographie à clé publique. Les utilisateurs se voient attribuer une paire de clés unique – une clé publique et une clé privée (secrète) – pour crypter des données ou créer des signatures numériques. L'ICP donne l'assurance que les personnes sont correctement reliées à leurs clés et que les liens sont constamment maintenus, en faisant appel à une infrastructure de confiance pour gérer les clés et la technologie connexe[4].

Cette infrastructure de confiance est réalisée grâce aux politiques, aux processus et aux personnes nécessaires pour appuyer le fonctionnement d'une ICP. Les politiques et les procédures[5] de l'ICP définissent l'ensemble des règles qui régissent l'emploi de certificats[6] ainsi que les processus à suivre pour les émettre, les gérer et les révoquer. En général, il faut procéder périodiquement à des inspections de conformité indépendantes pour s'assurer que les politiques et les procédures de l'ICP sont appliquées et observées rigoureusement. Des tierces parties de confiance, qui travaillent au sein de l'administration centrale et à l'échelle locale/au niveau de l'unité, sont également désignées pour valider l'identité des personnes[7] qui demandent l'accès au système d'ICP. Par ailleurs, une ICP doit compter sur des ressources suffisantes pour établir et maintenir les processus nécessaires de même que pour entretenir et faire fonctionner le système (c.-à-d. le matériel et les logiciels). La technologie à clé publique est relativement simple. C'est la mise en place de l'« infrastructure » (c.-à-d. les politiques, les processus et le personnel) qui représente couramment le plus grand défi. Le

[4] Une explication plus détaillée de la technologie de l'ICP et de la cryptographie à clé publique est fournie à l'**annexe A**.
[5] Les politiques et procédures de l'ICP s'appellent Politique de certification (PC) et Énoncé de pratiques de certification (EPC).
[6] Les clés publiques (c.-à-d. la clé de cryptage et la clé de vérification de signature numérique d'une personne) sont habituellement publiées sous forme de « certificats » électroniques. Ces certificats sont publiés dans un annuaire d'ICP avec l'information attestant la validité des clés. Un annuaire d'ICP ressemble à un annuaire téléphonique.
[7] Les preuves requises et le processus à suivre pour valider l'identité des personnes ou des entités dépendent de la politique de l'ICP de l'organisation.

General Accounting Office (GAO) des États-Unis (É.-U.) en est arrivé à des conclusions similaires lors de ses examens de l'implantation d'ICP au sein de départements et organismes fédéraux[8].

L'information et les communications électroniques n'ont pas toutes besoin d'être protégées par des mécanismes de sécurité comme l'ICP. La sensibilité des données ainsi que la politique de sécurité et le modèle fonctionnel d'une organisation devraient déterminer les mesures de sécurité à prendre en matière de TI.

L'ICP au gouvernement du Canada (GC)

Au cours des dernières années, le GC a annoncé un certain nombre d'objectifs en vue d'accroître l'efficacité opérationnelle et de réduire les coûts en transigeant par voie électronique. D'importantes initiatives du GC visant à appuyer les affaires et les communications électroniques ont également été présentées lors de la session de 1999 du Parlement canadien. Le gouvernement (à l'époque) a exprimé son intention de devenir « un utilisateur modèle des technologies de l'information et d'Internet »[9]. L'initiative « Gouvernement en direct » (GED) donne forme à la stratégie qui consiste à faire du Canada le pays le plus « connecté » au monde en offrant aux citoyens l'accès à l'information et aux services gouvernementaux en direct, au moment et à l'endroit qu'ils choisissent. Pour faciliter l'atteinte de son objectif, le GC a décidé que l'ICP serait l'une des principales technologies de sécurité de l'infrastructure qui sous-tend le GED, de manière à protéger la confidentialité de l'information et des transactions.

Outre le but du GC en ce qui a trait à l'amélioration des services, plusieurs lois, politiques et directives nécessitent une infrastructure électronique protégée pour assurer la conduite des opérations gouvernementales :

- La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) exige que les renseignements personnels des Canadiens soient protégés contre toute divulgation non autorisée et reconnaît l'utilisation d'une signature numérique dans les actes juridiques.
- La politique du Secrétariat du Conseil du Trésor (SCT) sur l'ICP définit comment un système d'ICP doit être mis sur pied et utilisé, en plus de préciser que l'ICP constitue le moyen privilégié d'authentification électronique de l'identité des personnes et des documents.
- La politique du SCT sur l'autorisation et l'authentification électroniques (AAE) exige que toutes les transactions électroniques soient signées numériquement à l'aide d'un mécanisme approuvé par le Centre de la sécurité des télécommunications (CST)[10].

[8] GAO-01-277 : *Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*. Février 2001. GAO-04-157 : *Status of Federal PKI Activities at Major Federal Departments and Agencies*. Décembre 2003.
[9] Discours du Trône ouvrant la deuxième session de la trente-sixième législature du Canada. 12 octobre 1999. ISBN 0-662-64508-1.
[10] Le seul mécanisme approuvé par le CST pour l'ICP et la signature numérique est celui qui est utilisé dans la suite de produits Entrust®.

L'ICP au MDN

L'ICP a été introduite au MDN dans le cadre d'un projet de recherche et de sécurité en 1994-1995. L'achat initial du produit Entrust® pour l'ICP a été effectué en 1995 au coût de 3 M$, sur la recommandation de la Direction de la sécurité de la TI (D Séc TI). L'ICP a fonctionné essentiellement dans un environnement de laboratoire du MDN jusqu'à ce que le projet du Courrier électronique commun protégé (CECP)[11] voie le jour en 2000. Le CECP a été installé sur tous les ordinateurs de bureau reliés au Réseau étendu de la Défense (RED) ou au domaine désigné[12], et tous les employés du MDN et membres des FC possédant une adresse électronique du MDN pouvaient y avoir accès. Grâce au CECP, les renseignements sensibles, y compris l'information Protégé B[13] (PB), pouvaient être envoyés ou stockés par voie électronique sur le RED. À la fin de 2002, quelque 60 000 cartes à puce[14] d'ICP avaient été distribuées au coût approximatif de 16 M$[15]. Les opérations du projet du CECP ont été prises en charge par les équipes de gestion du cycle de vie du MDN et des FC au début de 2003.

Les principales équipes de gestion du cycle de vie du MDN et des FC qui sont chargées d'appuyer l'ICP du MDN sont la Direction de la sécurité de la GI (D Sécur GI) et la Direction de l'ingénierie et de l'intégration de réseaux informatisés (DIIRI). La Dir Sécur GI assume la responsabilité globale de la politique et des opérations de l'ICP (la Dir Sécur GI 3 étant responsable du domaine désigné et la Dir Sécur GI 4, du domaine classifié[16]). La DIIRI, quant à elle, s'occupe de l'ingénierie et de la conception de l'ICP (la DIIRI 3-5 ICP étant responsable de l'autorité de certification[17] (AC) et la DIIRI 4, des services d'annuaire). Un organigramme figure à l'**annexe B**.

[11] Le CECP a été mis en place dans le cadre du projet-cadre du Système de traitement des messages de la Défense (STMD).
[12] Le domaine désigné fait référence à l'intranet du MDN et des FC, qui peut traiter en clair tous les messages à usage général, y compris l'information Protégé A.
[13] Le terme protégé ou désigné représente une classification de sécurité qui sert à identifier et à protéger l'information dont la compromission pourrait vraisemblablement porter préjudice à des intérêts privés. Cette information est classifiée selon le degré de sensibilité éventuelle (c.-à-d. Protégé A (peu sensible), Protégé B (particulièrement sensible) ou Protégé C (extrêmement sensible)).
[14] Au MDN, la preuve d'identité électronique secrète d'une personne (c.-à-d. clés de décryptage et de signature privées) se trouve sur une carte à puce d'ICP. Cette carte est nécessaire pour avoir accès aux applications d'ICP. Ce ne sont pas toutes les organisations qui utilisent des cartes à puce pour stocker les preuves d'identité électronique; il existe d'autres supports de stockage.
[15] Le coût de la mise en place du CECP, soit 16 M$, a été communiqué par l'équipe de projet du CECP.
[16] Le domaine classifié est un réseau distinct du MDN et des FC réservé au trafic de données électroniques classifiées. On entend par information classifiée les renseignements dont la compromission pourrait vraisemblablement porter préjudice à l'intérêt national. Il s'agit de renseignements gouvernementaux qui concernent la défense et le maintien de la stabilité sociale, politique et économique du Canada. Cette information est classée selon le degré de préjudice éventuel (c.-à-d. Confidentiel, Secret ou Très secret).
[17] L'AC est un élément de confiance clé d'une ICP. Elle englobe le matériel et les logiciels utilisés pour créer, émettre et gérer des certificats de clé publique.

Dans l'ensemble, le CECP et l'ICP ne sont pas largement utilisés au sein du MDN et des FC. Certains groupes d'utilisateurs comme la Police militaire, les Finances et les Ressources humaines (RH) ont beaucoup recours au CECP pour protéger les messages sensibles qui sont envoyés par courriel dans le domaine désigné, mais on ne connaît pas l'étendue réelle de l'utilisation à cause d'un manque de mesures vérifiables. Nous pouvons néanmoins confirmer que sur les 60 000 cartes à puce d'ICP distribuées à l'origine lors de la mise en place du CECP, 35 000 ont expiré (en date d'août 2004). Le coût de ces cartes expirées peut être évalué à environ 3,5 M$ (100 $ par carte à puce/lecteur fois 35 000 cartes). Or, ce montant ne tient pas compte du coût de mise en œuvre (c.-à-d. les ressources de projet nécessaires pour initialiser et distribuer les cartes ainsi que les frais de formation connexes), ni des coûts intangibles liés à la non-utilisation des cartes à puce expirées – par exemple, l'embarras dans lequel le Ministère pourrait se trouver en ne se conformant pas aux lois sur la protection de la vie privée, ou le risque que la divulgation involontaire de renseignements sensibles poserait pour la sécurité. Au sein du MDN et des FC, de l'information PB (et même classifiée) a été transmise en clair dans le domaine désigné. Plusieurs incidents ont été signalés et font l'objet d'un suivi de la part du Groupe des opérations d'information des Forces canadiennes (GOIFC), mais les rapports ne décrivent pas l'étendue véritable du problème – seulement les incidents signalés.

Un grand nombre de nouvelles applications d'ICP du MDN et des FC sont prévues et conçues en supposant qu'il existe une ICP fiable dans le domaine désigné. Ces applications comprennent l'IRPVD (Infrastructure du réseau privé virtuel de la Défense – accès à distance protégé) et le SISFC (Système d'information sur la santé des Forces canadiennes). En outre, une ICP est prévue pour le domaine classifié avec, comme principale application, le STMM (Système de traitement des messages militaires)[18]. L'**annexe C** renferme une liste des applications d'ICP du MDN. Cela signifie que le MDN aura au moins deux systèmes d'ICP distincts : l'ICP du domaine désigné qui est entrée en service avec le CECP, et l'ICP du STMM qui devrait être opérationnelle dans le domaine classifié au milieu de 2005. La mise en place de deux ICP distinctes rend leur gestion plus complexe (c.-à-d. au niveau des politiques, des processus et du personnel).

Il convient aussi de noter que le MDN et les FC mènent actuellement un projet pilote sur les postes de travail TITAN (classifiés) pour fournir une fonctionnalité similaire à l'ICP (c.-à-d. cryptage et signature numérique) au moyen d'une technologie différente. Une infrastructure à certificats (IC) assure une cryptographie de haut niveau de type 1 alors que l'ICP offre une cryptographie sûre mais de qualité commerciale. Qu'il s'agisse d'une IC ou d'une ICP, la mise en œuvre de l'infrastructure nécessaire (politiques, processus et personnel) présente les mêmes défis[19].

[18] Le STMM fait également partie du projet-cadre du STMD (dont relevait la mise en place du CECP).
[19] L'IC du MDN sera gérée par une unité distincte au sein de la Dir Sécur GI appelée l'Unité de soutien cryptographique des Forces canadiennes (USCFC).

ÉVALUATION GLOBALE

Même si certaines des exigences du MDN en matière de sécurité des communications pouvaient être remplies grâce à d'autres approches ou technologies, l'ICP offre la seule solution extensible[20] à l'heure actuelle pour répondre aux besoins de sécurité d'une collectivité très étendue dans les domaines suivants : identification et authentification rigoureuses, accès à distance protégé, confidentialité et intégrité des données électroniques, et non-répudiation.

Les besoins du MDN et des FC en matière de sécurité des communications électroniques, qui sont énumérés ci-dessous, sont manifestement valables, mais ils n'ont pas encore été formulés officiellement dans une analyse de rentabilisation du MDN ni définis à l'intérieur de son cadre global de sécurité de la TI d'un point de vue fonctionnel ou opérationnel :

- protéger l'information sensible au sein du Ministère et l'information qui appartient à des organisations externes et qui est partagée avec elles;
- progresser vers une automatisation du flux de travail et une réduction des processus papier/manuels;
- effectuer des transactions commerciales électroniques sécurisées avec des parties externes (p. ex., Travaux publics et Services gouvernementaux Canada (TPSGC) et des fournisseurs).

L'ICP du domaine désigné qui est présentement installée et l'ICP du STMM qui est prévue offrent de bonnes solutions techniques, mais il faut corriger d'importantes faiblesses touchant la gestion, les politiques, l'administration et les opérations si l'on veut que les ICP du MDN soient efficaces sur le plan opérationnel. Des questions majeures doivent être résolues avant que les utilisateurs actuels puissent faire entièrement confiance à l'ICP existante et avant que les nouvelles applications d'ICP, notamment l'IRPVD et le STMM, puissent recevoir un soutien. Ces questions sont résumées au tableau 1 ci-dessous, et chaque volet est décrit plus en détail dans la section suivante du rapport (Résultats détaillés et recommandations). L'**annexe D** indique quelles seraient les conséquences pour le MDN et les FC s'ils *n'avaient pas* d'ICP et devaient plutôt avoir recours à un fournisseur de services externe pour obtenir des certificats d'ICP.

Au cours de l'examen, il nous est apparu évident que les membres du personnel de l'ICP du MDN et des FC avaient à cœur la réussite des projets. Ils font de leur mieux sans bénéficier de processus bien établis, de ressources suffisantes et expérimentées, d'une formation appropriée et d'une participation ou de directives adéquates de la direction. Pris individuellement, chacun de ces facteurs pourrait être géré sans que cela nuise aux opérations ou au niveau de service offert aux utilisateurs. Or, collectivement, ils suscitent beaucoup d'incertitude quant à la crédibilité et à l'extensibilité du système global.

[20] Les systèmes traditionnels de cryptage à clé secrète (ou cryptage symétrique) pourraient servir à la sécurité des communications de point à point, mais ils ne sont pas en mesure d'accueillir un grand nombre d'utilisateurs répartis ni un service de signature numérique. De plus amples détails figurent à l'**annexe A**.

La carte de pointage sommaire ci-dessous présente un tableau simplifié des « bonnes pratiques communes » qu'on s'attendrait à voir en place à l'égard de tout système, en particulier une ICP. L'évaluation a été fondée sur les résultats de l'examen et le jugement professionnel de l'équipe d'examen du CS Ex[21].

Tableau 1 – Carte de pointage sommaire de l'examen de l'ICP du MDN

Critères d'évaluation		Inexistant / Non élaboré	Stade initial / ponctuel	Élaboré / en place	Amélioration continue
A. Importance et pertinence de l'ICP	Besoins fonctionnels du Ministère clairement définis		■		
	Besoins de sécurité du Ministère clairement définis		■		
	Niveau global de sensibilisation du Ministère		■		
B. Gouvernance et planification stratégique	Structure de gouvernance officielle de l'ICP	■			
	Planification de l'ICP au niveau du programme	■			
C. Politiques et procédures	Responsabilité des politiques ICP clairement attribuée		■		
	Processus officiel d'élaboration des politiques ICP		■		
	Pouvoir d'approbation clair – Politiques ICP du MDN	■			
	Politiques ICP du MDN approuvées et à jour		■		
	Politiques ICP pertinentes du GC suivies		■		
D. Rôles et responsabilités	Clairement définis et bien compris		■	■	
	Rôles clés de l'ICP déterminés et remplis		■	■	
E. Soutien et processus d'infrastructure	Processus bien définis et en place		■		
	Processus efficaces et rentables		■		
F. Mesure du rendement	Existence d'un modèle de coûts à jour pour l'ICP	■			
	Suivi des coûts réels de l'ICP par rapport au budget	■			
	Suivi des statistiques sur l'utilisation de l'ICP		■		
	Recours aux statistiques sur l'utilisation de l'ICP pour équilibrer la charge de travail	■			
	Ententes sur les niveaux de service/organisationnels en place		■		
G. Intégration de la technologie de l'ICP	Bonne interaction entre les groupes techniques et fonctionnels		■		
	Bonne interaction entre les groupes techniques et les groupes d'utilisateurs		■		

[21] L'équipe d'examen du CS Ex comptait à la fois des membres du CS Ex et d'AEPOS.

Parce que le MDN n'adopte pas une approche de gestion d'entreprise à l'égard de l'ICP, cette dernière n'est pas entièrement efficiente et efficace en tant qu'infrastructure de soutien de l'échange protégé des données et des communications. En outre, l'approche ponctuelle du Ministère rend l'ICP vulnérable aux coûts et aux risques évitables. L'ICP est plus qu'une simple solution technologique; elle doit être gérée dans le contexte des besoins fonctionnels et opérationnels du MDN et des FC.

RÉSULTATS CLÉS

- Même si le MDN a des besoins valables en matière de services de sécurité assurés par une ICP d'entreprise, les besoins fonctionnels et de sécurité n'ont pas encore été clairement définis ni formulés de manière officielle afin de communiquer l'importance et la pertinence de l'ICP à la haute direction du Ministère ou aux utilisateurs.

- Il faut mettre en place une structure de gouvernance officielle de l'ICP pour fournir des directives générales et limiter le plus possible les écarts stratégiques. L'ICP devrait être gérée comme un programme d'infrastructure commune mais, à l'heure actuelle, elle est abordée en fonction d'une série de projets indépendants.

- Les politiques et les procédures de l'ICP ne sont pas officiellement avalisées. Les politiques provisoires sont périmées et ont besoin d'être révisées.

- Les rôles et les responsabilités ayant trait aux postes clés ne sont pas clairement définis.

- Les processus d'infrastructure fondamentaux doivent être renforcés, et la coordination horizontale nécessaire n'est pas assurée.

- Il n'existe aucune mesure des coûts ou de l'utilisation de l'ICP du domaine désigné, ni aucun modèle de coûts pour l'ICP.

- Il faut une meilleure intégration de la technologie de l'ICP et des processus fonctionnels.

CAUSES POSSIBLES / AUTRES PRÉOCCUPATIONS

Bon nombre des questions soulevées au cours du présent examen ne sont pas particulières aux ICP du MDN, car elles s'appliquent également à d'autres systèmes ministériels. Des besoins fonctionnels non définis ou incomplets et un manque de gouvernance, de planification au niveau du programme et de processus horizontaux sont des problèmes systémiques qui ont déjà été cernés par rapport à différents systèmes/projets ministériels. L'une des principales causes est liée à la gouvernance de la GI, en particulier l'absence d'une approche d'entreprise pour la mise en œuvre des projets de GI.

Dans le cas des ICP du MDN, les objectifs des projets entrent parfois en conflit avec les besoins à plus long terme des gestionnaires du cycle de vie du produit (GCVP) et des groupes opérationnels. Les équipes des projets (c.-à-d. le CECP et le STMM) devaient/doivent constamment livrer les produits tout en respectant le budget et le calendrier. Certaines exigences des projets sont étroitement définies en raison de l'absence de processus de planification horizontale et d'une approche d'entreprise. Par exemple, les interdépendances avec d'autres projets (c.-à-d. le CECP, le STMM et l'IC) sont souvent négligées, car on considère qu'elles « dépassent la portée » de chaque projet. Toutefois, cela oblige les GCVP ou les groupes opérationnels à établir les processus manquants seulement après que le projet leur a été confié (c'est le cas, par exemple, de l'ICP du domaine désigné). D'autres processus des projets, comme la formation des utilisateurs, ne sont pas assez rigoureux (étant axés sur une formation ponctuelle initiale plutôt que sur une formation continue) pour répondre aux besoins des utilisateurs à plus long terme. Ces types de conflits ne seront pas et ne pourront pas être résolus à moins que le Ministère ne crée une structure de gouvernance de l'ICP pour mettre l'accent sur les objectifs au niveau du programme et commencer à gérer l'ICP comme un programme d'infrastructure commune.

Une autre préoccupation réside dans le fait que l'ICP est souvent appelée une initiative « de niveau de travail » (c.-à-d. ascendante) et qu'elle n'est pas assez visible pour la haute direction du SMA(GI). En conséquence, la direction ne comprend pas tout à fait le soutien continu qui est nécessaire à la mise en œuvre d'un système d'ICP viable et crédible. Ce manque de visibilité et de participation de la direction a sans doute contribué à la définition incomplète des besoins relatifs au CECP. Plus particulièrement, c'est une décision prise dans le cadre du projet du CECP qui a abouti à la distribution de 60 000 cartes à puce d'ICP, mais plus de la moitié de ces cartes ont expiré dans les trois années suivantes. Il convient de noter que bon nombre des questions soulevées dans le présent examen ont également été traitées dans une note de synthèse interne du MDN qui a été préparée à l'intention de la haute direction du SMA(GI) en août 2000. Aucune mesure observable n'a été prise, probablement à cause du roulement au sein des principaux groupes centraux.

Enfin, bien qu'elle déborde le cadre du présent examen, une préoccupation qu'il faudrait mettre en évidence porte sur la structure de gouvernance du projet du STMM. Le SMA(GI) est le parrain du projet et il est également chargé de sa mise en œuvre, malgré le fait que le Sous-chef d'état-major de la Défense (SCEMD) sera l'autorité opérationnelle suprême à l'égard du STMM. Pour que le STMM soit déployé avec succès, il faudra modifier les processus fonctionnels existants afin d'intégrer la technologie de la façon appropriée. Par ailleurs, il se peut que de nouvelles politiques liées à l'ICP soient nécessaires pour reconnaître la nouvelle application de la technologie et les changements apportés aux processus. La participation du SCEMD durant la phase de mise en œuvre augmenterait les chances que le STMM soit adopté par les utilisateurs et pourrait aussi éviter quelques-uns des problèmes de transition/prise en charge qui se sont posés dans le cas des projets du CECP et de l'ICP du domaine désigné.

RECOMMANDATIONS CLÉS

Il est recommandé que le SMA(GI) :

- **élabore une « feuille de route » pour l'ICP** afin de définir et de formuler clairement les besoins fonctionnels et de sécurité du MDN en ce qui a trait à une ICP d'entreprise. Cette « feuille de route » devrait préciser comment et où l'ICP s'insère dans le cadre global de sécurité de la TI, en plus de définir les besoins fonctionnels auxquels l'ICP répond pour les applications actuelles et futures;

- **gère l'ICP comme un programme d'infrastructure ministérielle commune** et établisse les structures de gouvernance et les processus de planification stratégique requis/appropriés pour fournir des directives générales, approuver officiellement les politiques de l'ICP et veiller à ce qu'il y ait le moins possible de vides et d'écarts stratégiques;

- **mette à jour et approuve officiellement les politiques nécessaires de l'ICP**. Cela comprend à tout le moins la PC et l'EPC ainsi que l'élaboration d'une politique ou directive ministérielle claire sur la nécessité et l'utilisation de clés de cryptage et de signatures numériques d'ICP. Le Ministère devrait élaborer ou réviser, au besoin, d'autres politiques liées à l'ICP, par exemple sur la gestion et l'utilisation du courrier électronique, l'application par le MDN de la politique de Bibliothèque et Archives Canada (BAC) régissant les données consignées, la gestion de l'information, etc.;

- **définisse, clarifie, attribue, documente et communique les rôles et responsabilités clés** des groupes de soutien de l'ICP, et ce, pour tous les aspects de l'ICP (notamment les politiques, le fonctionnement, l'enregistrement (à l'administration centrale et à l'échelle locale/au niveau de la base), la liaison externe, les services de dépannage, le contrôle et l'évaluation/la conformité);

- **renforce, rationalise et optimise le soutien et les processus d'infrastructure distincts de l'ICP**, en particulier l'enregistrement, la formation et les services de dépannage, pour en faire une structure de soutien qui combine les processus rationalisés des différents systèmes d'ICP et d'IC;

- **élabore un modèle de coûts pour l'ICP et mette au point des mesures du rendement opérationnel pour ensuite les rassembler, les analyser, les surveiller et en faire rapport** régulièrement afin de permettre l'évaluation du rendement, la budgétisation, l'analyse des coûts de même que la planification et l'équilibrage de la charge de travail;

- **définisse/établisse un nouveau rôle d'« analyste des activités » chargé d'assurer la liaison avec les utilisateurs et les groupes fonctionnels**, de favoriser la communication et de rassembler les besoins. Le but consiste à développer une solide

compréhension des processus fonctionnels et des besoins actuels de l'ICP pour déterminer la meilleure façon d'intégrer la technologie de l'ICP et d'obtenir les avantages souhaités (c.-à-d. accroître l'efficacité opérationnelle et réaliser des économies).

Nous avons tenu compte des pratiques et des leçons tirées d'autres organisations (voir l'**annexe E**) pour formuler les recommandations clés ci-dessus.

PLANS D'ACTION DE LA DIRECTION

Les plans d'action de la direction fournis par le SMA(GI) montrent qu'une attention constructive est portée à la majorité des recommandations figurant dans le présent rapport. Par la même occasion, nous encourageons la direction à prendre certaines mesures plus tôt que prévu, particulièrement en ce qui concerne l'élaboration d'une feuille de route de l'ICP du MDN, l'éclaircissement des rôles et des responsabilités des groupes de soutien de l'ICP du MDN et la rationalisation du soutien et des processus d'infrastructure distincts de l'ICP (réf. : points A, D et E de la matrice des plans d'action de la direction). À cet égard, des jalons provisoires relatifs aux plans d'action seront demandés par le biais des processus de suivi et de contrôle du CS Ex. Les recommandations et les plans d'action correspondants sont présentés sous forme de matrice à l'**annexe G** du rapport et résumés au tableau 1 ci-dessous.

Point	Recommandation du CS Ex	BPR/BC	Plans d'action de la direction
A.	*Élaborer une « feuille de route » pour l'ICP* afin de définir et de formuler clairement les besoins fonctionnels et de sécurité du MDN en ce qui a trait à une ICP d'entreprise.	BPR : Dir Sécur GI	D'accord. La Dir Sécur GI devrait diriger l'élaboration d'une feuille de route de l'ICP du MDN aux fins d'approbation par la haute direction. La feuille de route du MDN comportera un programme de formation et de sensibilisation.
B.	*Gérer l'ICP comme un programme d'infrastructure ministérielle commune* et établir les structures de gouvernance et les processus de planification stratégique requis/appropriés.	BPR : Dir Sécur GI	D'accord. Il est proposé que le MDN gère l'ICP comme un programme d'infrastructure commune en établissant un cadre de gouvernance et en l'intégrant au cadre existant de gestion d'infrastructure à clé.
C.	*Mettre à jour et approuver officiellement les politiques nécessaires de l'ICP.* Cela comprend la PC et l'EPC ainsi que les politiques et procédures ministérielles liées à l'ICP, par exemple sur la gestion et l'utilisation du courrier électronique, l'application par le MDN de la politique de BAC régissant les données consignées, etc.	BPR : Dir Sécur GI BC : DIIRI	D'accord. La Dir Sécur GI s'occupera du traitement de la PC du GC et de l'EPC du MDN conformément au cadre de gouvernance de l'ICP. La Dir Sécur GI et la DIIRI consulteront aussi les responsables des applications d'ICP au sujet des politiques et des procédures qui leur sont propres.

Point	Recommandation du CS Ex	BPR/BC	Plans d'action de la direction
D.	*Définir, clarifier, attribuer, documenter et communiquer les rôles et responsabilités clés* des groupes de soutien de l'ICP, et ce, pour tous les aspects de l'ICP.	BPR : DGOGI BC : D Sécur GI DIIRI/CORFC	La DGOGI établira les responsabilités des groupes de soutien de l'ICP dans le cadre du remaniement de la Division.
E.	*Renforcer, rationaliser et optimiser le soutien et les processus d'infrastructure distincts de l'ICP* pour en faire une structure de soutien qui combine les processus rationalisés des différents systèmes d'ICP.	BPR : DGOGI	La DGOGI rationalisera le soutien et les processus de l'ICP dans le cadre du remaniement de la Division. La DIIRI et la Dir Sécur GI dresseront un plan de ressources pour la stabilisation de l'ICP.
F.	*Élaborer un modèle de coûts pour l'ICP et mettre au point des mesures du rendement opérationnel* pour ensuite les rassembler, les analyser, les surveiller et en faire rapport régulièrement.	BPR : Dir Sécur GI BC : DGOGI	La DGOGI veillera à ce que les questions relatives au contrôle du rendement du système et à la planification des capacités de l'ICP soient traitées lors du remaniement de la Division. La DIIRI et la Dir Sécur GI élaboreront un modèle de coûts dans le cadre du plan de ressources pour la stabilisation de l'ICP.
G.	*Définir/établir un nouveau rôle d'« analyste des activités » chargé d'assurer la liaison avec les utilisateurs et les groupes fonctionnels* et de favoriser la communication.	BPR : Dir Sécur GI BC : CCI AGI	La Dir Sécur GI dispensera une formation initiale sur l'ICP à ses analystes et aux membres de la cellule consultative de l'ICP (CCI) relevant de l'AGI, afin de cerner les possibilités au niveau de l'entreprise et les incidences des solutions axées sur l'ICP.

Tableau 1 : Résumé des plans d'action de la direction

OBJECTIF, PORTÉE ET MÉTHODOLOGIE

OBJECTIF

Le principal objectif de l'examen était d'évaluer la capacité de l'ICP du MDN à fournir des services protégés et confidentiels aux utilisateurs et aux applications du Ministère. L'examen visait aussi à évaluer l'incidence des futurs besoins sur l'élaboration, la gestion et le fonctionnement d'une ICP ministérielle viable, crédible et extensible.

PORTÉE

L'examen a porté sur des aspects clés des structures de gouvernance, des politiques, des processus, des ressources et de l'équipement qui appuient collectivement la gestion et le fonctionnement de l'ICP du MDN. Nous avons également examiné les futures applications d'ICP du Ministère et analysé des organisations comparables. L'examen ne visait pas à évaluer les capacités techniques du produit Entrust® ni sa sélection à titre de mécanisme approuvé par le CST pour l'ICP.

MÉTHODOLOGIE

- Nous avons rassemblé et examiné l'information ministérielle sur l'ICP du MDN ainsi que les politiques pertinentes du GC.
- Nous avons élaboré un document-cadre de l'ICP et effectué une évaluation des risques de haut niveau.
- Nous avons mené des entrevues auprès :
  - des intervenants clés et de la haute direction fonctionnelle du Ministère;
  - des ingénieurs et du personnel de soutien de l'ICP du Ministère;
  - des utilisateurs du Ministère et des utilisateurs éventuels (applications prévues);
  - d'autres ministères et de certaines organisations à l'extérieur du gouvernement fédéral.
- Nous avons évalué l'incidence des nouvelles et futures applications d'ICP du Ministère.
- Nous avons examiné les approches d'autres organisations à l'égard de l'ICP.
- Nous avons examiné les besoins de cocertification [22] du MDN et leurs répercussions.

[22] La cocertification est le processus qui sert à établir un lien de confiance avec une autre ICP, de sorte que chaque ICP accepte les certificats de l'autre. Cela permet l'interfonctionnement sécurisé de domaines d'ICP distincts. Jusqu'à présent, six ministères (autres que le MDN) et une organisation provinciale ont conclu une entente de cocertification avec l'ICP du GC.

RÉSULTATS DÉTAILLÉS ET RECOMMANDATIONS

Prélèvement en vertu de l'article 20(1)(c) de la LAI – Renseignements de tiers.

A. IMPORTANCE ET PERTINENCE DE L'ICP DU MDN

……[23]

L'absence de besoins fonctionnels et de sécurité clairement définis contribue au manque de sensibilisation, de compréhension et d'utilisation de l'ICP à titre d'outil facilitant la sécurité des communications électroniques au sein du Ministère. L'ICP est souvent considérée comme une solution technique à la recherche d'un problème, plutôt qu'un moyen de répondre à un besoin fonctionnel particulier. Même si le MDN a des besoins valables pour ce qui est des services de sécurité[24] offerts par une ICP d'entreprise, il ne les a pas encore officiellement formulés dans une analyse de rentabilisation. En outre, le MDN n'a pas encore défini comment ni où l'ICP s'insère dans son cadre global de sécurité de la TI d'un point de vue fonctionnel ou opérationnel. De nombreux employés du Ministère ne sont pas suffisamment conscients qu'il faut protéger l'information électronique désignée/sensible et ne savent pas que la technologie est facilement accessible sur la plupart des postes de travail.

Besoins fonctionnels et de sécurité non définis

- La justification initiale de l'achat de l'ICP du MDN en 1995 n'était pas claire et elle n'était pas rattachée à des besoins fonctionnels précis.
- Les besoins de sécurité ministériels auxquels l'ICP est censée répondre n'ont pas été clairement définis à l'intérieur du cadre global de sécurité de la TI du Ministère (p. ex., déterminer les systèmes qui exigent une authentification robuste, en fonction d'une évaluation des risques).
- Il n'existe aucune politique ou directive ministérielle claire exigeant l'utilisation de l'ICP (p. ex., crypter l'information Protégé B (PB) ou promouvoir/favoriser le recours à des signatures numériques pour automatiser les processus).
- Le Courrier électronique commun protégé (CECP), qui était la principale application de l'ICP, n'est généralement pas considéré comme une application « indispensable » au sein du MDN, et l'on n'a pas assez insisté sur son importance pour protéger les messages sensibles pendant la transmission.

Prélèvement en vertu de l'article 20(1)(c) de la LAI – Renseignements de tiers.

[23] ……
……

[24] Les services de sécurité de l'ICP comprennent l'authentification des utilisateurs/entités, la confidentialité et l'intégrité des données et la non-répudiation.

Sensibilisation limitée du Ministère à l'utilisation et aux capacités de l'ICP

- Le Ministère est relativement peu sensibilisé à la nécessité de protéger les documents électroniques désignés/sensibles (c.-à-d. l'information PB) et au fait que l'ICP pourrait servir à combler ce besoin (comparativement au niveau de sensibilisation à l'égard de la protection des documents papier de nature sensible).
- L'importance de l'ICP comme outil de sécurité et sa capacité d'offrir de solides moyens de cryptage sont mal compris au sein du Ministère.
- Il existe un manque d'acceptation de la part du personnel du Ministère. Beaucoup d'utilisateurs ne comprennent pas la nécessité de l'ICP, tandis que la Police militaire (PM), les Ressources humaines (RH) et les Finances la trouvent très utile.
- Certains membres du personnel du MDN et des FC hésitent à accepter des cartes à puce d'ICP, et certaines unités sont peu enclines à en distribuer.
- Bien que de nombreuses cartes à puce distribuées n'aient jamais servi, on ne connaît pas l'étendue réelle de l'utilisation de l'ICP au sein du Ministère en raison de l'absence de mesures.

Exemples de la façon dont l'ICP est utilisée avec succès dans d'autres organisations

- Les organismes d'application de la loi se fient à la solide cryptographie commerciale de l'ICP pour assurer la confidentialité et la protection de l'information sensible (p. ex., les communications avec des agents d'infiltration et le registre des délinquants sexuels).
- On s'affaire à éliminer ou à réduire les processus papier en automatisant l'émission des chèques en fonction de signatures numériques (p. ex., certains programmes de remboursement de l'Agence du revenu du Canada (ARC)).
- Contrairement aux processus manuels, la transmission électronique des documents sensibles peut grandement réduire le temps de traitement, engendrer des économies et accroître l'efficacité opérationnelle. C'est le cas pour les sociétés pharmaceutiques qui ont automatisé des processus d'approbation clés, notamment en ce qui concerne les délais relatifs aux approbations de la Food and Drug Administration (FDA). Les médicaments peuvent atteindre le marché plus rapidement, ce qui procure des avantages financiers considérables aux titulaires de brevets.

RECOMMANDATIONS

Élaborer une « feuille de route » pour l'ICP afin de définir et de formuler clairement les besoins fonctionnels et de sécurité du MDN en ce qui a trait à une ICP d'entreprise. Cette « feuille de route » devrait préciser comment et où l'ICP s'insère dans le cadre global de sécurité de la TI, en plus de définir les besoins fonctionnels auxquels l'ICP répond pour les applications actuelles et futures. Il devrait s'agir d'un document évolutif qui est mis à jour périodiquement et qui sert à communiquer l'importance de l'ICP aux intervenants et aux décideurs. La « feuille de route » devrait également être fournie aux responsables des nouveaux projets qui ont des besoins en matière d'ICP afin qu'ils comprennent clairement les services de sécurité offerts (ou non) par l'ICP du MDN.

- L'ICP ne devrait être déployée que pour répondre à des besoins fonctionnels définis et à une analyse de rentabilisation financière claire (c.-à-d. une analyse coûts-avantages).
- Un effort concerté doit être fait pour accroître la sensibilisation et la compréhension du Ministère à l'égard de l'utilisation et des capacités de l'ICP. Les employés du Ministère doivent être mis au courant de la nécessité de protéger l'information électronique sensible/désignée et du fait que l'ICP est une technologie approuvée à cette fin.

BPR : SMA(GI)

B. GOUVERNANCE ET PLANIFICATION STRATÉGIQUE

Le Ministère doit se doter d'une structure officielle de gouvernance de l'ICP pour fournir des directives générales (tant interministérielles qu'intraministérielles) et veiller à limiter le plus possible les écarts au niveau stratégique. Pour que l'ICP du MDN fournisse entièrement et avec fiabilité les services de sécurité requis aux utilisateurs et aux applications du Ministère, une autorité ministérielle doit régler les questions importantes concernant la gestion, les politiques, l'administration et le fonctionnement de l'ICP[25]. Cette dernière devrait être gérée comme un programme d'infrastructure ministérielle, mais elle est actuellement abordée en fonction d'une série de projets indépendants alignés sur des applications individuelles d'ICP. L'absence de planification au niveau du programme est susceptible de nuire à l'efficacité opérationnelle et d'occasionner des dépenses inutiles parce que les deux principaux systèmes d'ICP du MDN reposent sur la conception d'un soutien et de processus d'infrastructure distincts[26]. En outre, il existe peut-être des possibilités de rationalisation avec un troisième système du MDN appelé infrastructure à certificats, ou IC, que gère actuellement l'USCFC au sein de la Dir Sécur GI.

[25] Chacun de ces sujets sera traité en détail dans les sections subséquentes du présent rapport.
[26] Les deux principaux systèmes d'ICP du MDN sont l'ICP actuelle du domaine désigné (CECP) et l'ICP du STMM qui est prévue pour le domaine classifié.

Besoin d'une structure officielle de gouvernance de l'ICP

- Il n'existe aucune structure officielle de gouvernance de l'ICP du MDN pour fournir des directives stratégiques au personnel opérationnel et technique ainsi qu'aux équipes de projet et assurer la coordination au niveau du programme, les pouvoirs décisionnels et la responsabilisation globale.
- Aucune autorité ministérielle n'a été nommée pour approuver officiellement les politiques de l'ICP du MDN.
- Le besoin d'une ICP n'a pas été communiqué clairement à la haute direction du MDN, et il ne bénéficie pas d'un appui officiel. De surcroît, la direction du SMA(GI) ne comprend qu'en partie les exigences d'investissement et de soutien continu auxquelles il faut satisfaire pour mettre en œuvre un système d'ICP viable et crédible.
- La haute direction du SMA(GI) ne comprend pas tout à fait les rôles et les responsabilités de l'ICP.

Absence d'approche coordonnée, intégrée et programmatique

- La haute direction du MDN et du SMA(GI) s'intéresse principalement à l'ICP au niveau des projets individuels (c.-à-d. le CECP, le STMM et l'IRPVD) plutôt qu'au niveau du Ministère ou de l'entreprise.
- Il faut que la planification stratégique de l'ICP au niveau du programme assure la cohérence entre les objectifs ministériels et ceux des projets, indique la voie à suivre et évite l'inefficacité opérationnelle et les dépenses inutiles.
- Plus précisément, le MDN pourrait se retrouver avec trois systèmes distincts mais similaires : l'ICP du domaine désigné, l'ICP du STMM dans le domaine classifié et l'IC de l'USCFC qui fait l'objet d'un projet pilote sur les postes de travail TITAN classifiés. Bien que trois systèmes distincts puissent être nécessaires sur le plan du *contenu*, les synergies qui pourraient résulter de la combinaison du soutien et des processus d'infrastructure (p. ex, le soutien et les processus centraux en matière d'enregistrement et de dépannage ainsi que les ressources au niveau de la base) ne sont pas suffisamment explorées, car on considère qu'elles « dépassent la portée » de chaque projet. Le fait d'avoir l'ICP et l'IC sur le même poste de travail classifié peut aussi poser des problèmes, mais on juge également que cette question « dépasse la portée » des projets individuels.
- Le Ministère ne possède aucune stratégie globale de sécurité des communications électroniques dans le cas de nouveaux dispositifs comme les assistants numériques (p. ex., Blackberry^{MC}).
- La stratégie à long terme du MDN n'est pas claire en ce qui concerne les membres de l'ICP du GC. Son ICP du domaine désigné n'est pas encore interopérable (c.-à-d. cocertifiée) avec l'ICP du GC, et il n'est pas prévu de répondre à des besoins préliminaires en matière d'inspection de conformité.

RECOMMANDATIONS

Gérer l'ICP comme un programme d'infrastructure ministérielle commune et établir les structures de gouvernance et les processus de planification stratégique requis/appropriés pour fournir des directives générales, approuver officiellement les politiques de l'ICP et veiller à ce qu'il y ait le moins possible de vides et d'écarts stratégiques. La gestion et la surveillance de l'ICP peuvent être ajoutées aux tâches d'un comité de gouvernance déjà créé au MDN, à condition que le mandat du comité soit officiellement modifié pour inclure la responsabilité de l'ICP et que la haute direction des différents commandements et secteurs fonctionnels y soit convenablement représentée.

- Des plans stratégiques liés à la gestion et à la fusion possible du soutien et des processus d'infrastructure des différents systèmes d'ICP et d'IC, ainsi que des directives sur la voie à suivre (c.-à-d. les futurs besoins de cocertification), devraient être intégrés à la « feuille de route » de l'ICP recommandée dans la section A – Importance et pertinence de l'ICP du MDN.

BPR : SMA(GI)

C. POLITIQUES ET PROCÉDURES

Les politiques de l'ICP font partie intégrante d'un système d'ICP. Elles sont indispensables pour établir la « confiance » dans un certificat de clé publique et constituent le fondement de la cocertification (qui permet une interopérabilité sécurisée) avec d'autres organisations. Les politiques de l'ICP sont décrites dans un ensemble de documents fondamentaux appelés Politique de certification (PC) et Énoncé de pratiques de certification (EPC). La PC porte généralement sur les exigences de plus haut niveau en matière de politiques (c.-à-d. qu'elle énonce les conditions dans lesquelles des certificats d'ICP peuvent être émis en fonction d'une évaluation des risques de l'entreprise), tandis que l'EPC est un document technique et procédural plus détaillé et exhaustif qui régit le fonctionnement de l'ICP (p. ex., pratiques employées pour émettre, gérer et révoquer les certificats, description des services offerts, etc.). L'exigence obligatoire du SCT qui consiste à effectuer des inspections annuelles pour vérifier la conformité aux politiques de l'ICP vise à renforcer la « confiance » dans un système d'ICP. Au MDN, aucune autorité ministérielle n'a encore avalisé ou approuvé officiellement les politiques provisoires de l'ICP, et aucune inspection de conformité officielle n'a eu lieu.

Absence de politiques et de procédures d'ICP approuvées officiellement

- L'ICP du domaine désigné du MDN est en service depuis la fin de 2002 sans qu'aucune politique d'ICP soit officiellement approuvée (p. ex., PC et EPC) ou que les procédures connexes soient en place.
- Les instructions permanentes d'opération (IPO) de l'ICP – p. ex, les IPO applicables aux postes de travail du CECP et du STMM– ne sont pas étayées par une politique. Dans certains cas, les politiques provisoires de l'ICP et les IPO sont contradictoires.
- La responsabilité relative à l'approbation des politiques de l'ICP n'est pas claire étant donné le manque de gouvernance entourant l'ICP. Cela a également nui à l'élaboration des politiques requises en matière d'ICP (p. ex., application de l'ICP à des politiques ministérielles plus générales comme la gestion de l'information et des documents électroniques).
- L'absence de politiques approuvées à l'égard de l'ICP, de directives stratégiques sur la voie à suivre et de priorités établies au niveau du programme oblige le personnel opérationnel et technique de l'ICP à fixer ses propres priorités.

Processus ponctuels pour élaborer les politiques de l'ICP

- Les processus servant à élaborer, à tenir à jour et à publier les documents sur les politiques de l'ICP sont ponctuels et mal définis. L'ICP du MDN ne peut réussir sans processus structurés pour élaborer, mettre en œuvre et tenir à jour les politiques et procédures pertinentes.
- La responsabilité des politiques de l'ICP incombe actuellement aux Dir Sécur GI 3 et 4. Or, d'après ses observations, l'équipe d'examen du CS Ex croit qu'elle devrait être réaffectée à un autre groupe pour assurer une séparation adéquate des tâches (pour de plus amples détails, voir la section D – Rôles et responsabilités).

Les politiques ministérielles n'ont pas suivi le rythme des changements technologiques et juridiques

- Les politiques ministérielles générales et les IPO liées à l'ICP n'ont pas suivi le rythme des changements technologiques et juridiques.
- Par exemple, bien que les lois sanctionnent l'acceptation des signatures numériques, les politiques ministérielles ne l'indiquent pas encore. Dans d'autres cas, les IPO exigent toujours des processus et des signatures sur papier en guise de justification, malgré l'emploi de processus électroniques et de signatures numériques.
- La directive de BAC voulant que les données soient acceptées uniquement sous leur forme originale – dans le cas de l'ICP, non cryptées et sans signature numérique – a été souvent citée comme un obstacle à l'élaboration de certaines des politiques et IPO requises en matière d'ICP. Cette difficulté ne devrait toutefois pas empêcher le MDN de prendre une décision quant à la façon d'aborder la question.

Cas de non-conformité aux politiques et autres risques

- La politique du SCT sur l'ICP exige des inspections de conformité annuelles pour tous les ministères qui exploitent leur propre AC/ICP. Contrairement à la politique du GC, l'AC du domaine désigné du MDN n'a pas encore été soumise à une inspection pour vérifier la conformité aux politiques de l'ICP (p. ex., PC et EPC).
- Il existe des cas où la certification et l'accréditation (C&A) de certains systèmes ministériels n'ont pas été effectuées de la façon appropriée. De plus, certains systèmes qui ont fait l'objet d'une autorisation provisoire d'exploitation (APE) n'en remplissent pas les conditions mais continuent de fonctionner sur le RED[27]. Cette situation s'applique à l'ICP du domaine désigné de même qu'à des systèmes autres que l'ICP et est contraire à la politique de sécurité du GC et du MDN.
- Aucune disposition explicite n'a été prévue concernant la sauvegarde des clés de décryptage privées. Si l'accès ministériel à des fichiers cryptés par l'ICP est requis, il faut utiliser un processus manuel de recouvrement de clés. Bien que le recouvrement de clés par une tierce partie soit actuellement possible pour tous les abonnés actuels et anciens abonnés de l'ICP du MDN, il n'existe aucune politique ni procédure pour garantir l'accès à long terme aux données cryptées par l'ICP.

RECOMMANDATIONS

Mettre à jour les politiques de l'ICP au besoin et les soumettre à l'approbation officielle de l'autorité ministérielle compétente. Les politiques de l'ICP devraient comprendre à tout le moins la PC et l'EPC (pour les deux principaux systèmes d'ICP du MDN), ainsi que l'élaboration d'une politique/directive ministérielle claire sur la nécessité et l'utilisation de clés de cryptage et de signatures numériques d'ICP.

- Définir clairement les processus servant à élaborer, à tenir à jour et à mettre en œuvre les politiques de l'ICP, notamment un processus efficace d'approbation et de publication.
- Réviser les IPO de l'ICP (c.-à-d. les IPO des postes de travail du CECP et du STMM) pour les harmoniser avec les politiques approuvées de l'ICP.
- Effectuer une inspection officielle pour vérifier la conformité aux politiques approuvées de l'ICP (dans l'année suivant l'approbation).

Examiner et réviser les politiques et procédures ministérielles liées à l'ICP, notamment sur la gestion et l'utilisation du courriel, l'application par le MDN de la politique de BAC régissant les données consignées (ou son approche à cet égard), la gestion de l'information, etc.

- Déterminer les politiques et procédures ministérielles sur l'ICP à réviser ou à régler.
- Le responsable des politiques ou le Comité de gouvernance de l'ICP (selon le cas) devrait approuver/avaliser la mise à jour de toute politique ministérielle concernant l'ICP. **BPR : SMA(GI)**

[27] Avant qu'un nouveau système puisse fonctionner sur le RED, il faut le soumettre au processus de C&A pour s'assurer qu'il est conçu et mis en œuvre selon les exigences de sécurité précisées. L'APE est une mesure provisoire permettant à des systèmes pilotes de fonctionner sur le RED avant de terminer tout le processus.

D. RÔLES ET RESPONSABILITÉS

Les services de sécurité assurés par l'ICP sont conçus pour atténuer les risques qu'entraîne le fait de transiger ou de communiquer sur des réseaux publics. Dans un environnement d'affaires électronique, l'un des plus grands défis consiste à garantir l'identité de la personne, de l'entité juridique ou de l'application avec laquelle on effectue une transaction (c.-à-d. l'authentification de l'utilisateur). Une ICP peut fournir cette garantie en établissant une infrastructure de confiance pour associer une identité électronique unique à la personne qui demande l'accès, et en offrant un mécanisme pour vérifier que cette association était initialement valide et qu'elle est maintenue en permanence. La tierce partie de confiance responsable de gérer et de contrôler le processus d'association est l'autorité centrale d'enregistrement (ACE). Dans une grande organisation dont les éléments sont disséminés dans plusieurs régions, des agents de confiance comme les autorités locales d'enregistrement (ALE) remplissent bon nombre des fonctions administratives de l'ACE, en particulier l'enregistrement de l'utilisateur final (c.-à-d. l'identification en personne de l'abonné). De nombreuses questions ont été soulevées en ce qui a trait aux rôles et aux responsabilités des tierces parties de confiance qui font partie des ICP du MDN.

Séparation inadéquate des tâches chez l'ACE

- La Dir Sécur GI 3 est l'ACE pour l'ICP du domaine désigné, et la Dir Sécur GI 4 deviendra l'ACE pour l'ICP du STMM, dès qu'elle sera entièrement mise en service dans le domaine classifié.
- La Dir Sécur GI 3 (et par la suite la Dir Sécur GI 4) est responsable de l'élaboration des politiques de l'ICP, de l'ingénierie, de la gestion du cycle de vie des certificats et des activités opérationnelles, en plus de l'exécution des inspections de conformité officielles décrites dans la section C – Politiques et procédures.
- La séparation des tâches est inadéquate au sein de la Dir Sécur GI 3 (et de la Dir Sécur GI 4 en fin de compte). Les groupes chargés d'établir la politique de l'ICP ne devraient pas être responsables d'exploiter le système et de remplir la fonction de conformité « indépendante ».
- Bien que la politique de l'ICP soit documentée dans le cadre des responsabilités de la Dir Sécur GI 3, certains membres clés du personnel ne reconnaissent pas leur rôle quant à l'élaboration de la politique ou n'y consacrent aucun temps. Cette situation est due en partie au manque de ressources, mais aussi aux problèmes de gouvernance et à l'absence d'une autorité ministérielle qui serait chargée d'approuver les politiques de l'ICP.

Les faiblesses des contrôles de l'ACE nuisent aux relations « de confiance »

- La Dir Sécur GI 3 n'exerce pas un contrôle efficace sur les processus de nomination, de formation, de maintien en poste et de remplacement des ALE et des coordonnateurs locaux d'enregistrement (CLE) (c.-à-d. le soutien de l'enregistrement à l'ICP au niveau de la base). Par exemple, l'ACE ne dispose d'aucune liste à jour des ALE/CLE ni d'aucun processus uniforme pour permettre aux ALE/CLE de communiquer l'information au sujet des départs ou des remplacements.

- La Dir Sécur GI 3 ne contrôle pas de manière efficace les processus de révocation des certificats. La non-révocation de certificats d'ALE présente une importante vulnérabilité de sécurité et un risque élevé pour l'intégrité de l'ICP du domaine désigné, car les ALE jouissent de privilèges liés à l'inscription d'utilisateurs et à l'émission de certificats d'ICP.
- Certains membres clés du personnel de la Dir Sécur GI 3 ne participent pas à certains processus d'enregistrement dans leur secteur de responsabilité ou ne les appuient pas.

Synergies possibles grâce à la fusion des activités d'enregistrement

- Les activités centrales d'enregistrement à l'ICP et à l'IC sont très semblables. Une *seule* ACE pourrait donc s'occuper des processus de gestion des certificats touchant les ICP (domaine désigné et STMM) et l'IC (USCFC), à condition que des procédures claires et efficaces soient élaborées et mises en place.
- Parce que l'ICP n'est pas gérée comme un programme d'infrastructure ministérielle commune, les synergies éventuelles et les possibilités de rationalisation qu'offre la fusion des processus sont négligées, et des fonctions d'ACE similaires seront répétées dans trois groupes distincts (Dir Sécur GI 3 et 4 et USCFC).
- Les rôles et responsabilités des ALE/CLE, notamment la volonté d'exécuter les tâches assignées, soulèvent plusieurs préoccupations spécifiques. À l'échelle locale/au niveau de la base, on a l'impression que des fonctions sont imposées aux ALE/CLE sans ajout de ressources. Le risque d'une résistance accrue découlant des tâches additionnelles liées à la mise en place du STMM corrobore également la nécessité de fusionner les fonctions et processus d'enregistrement à l'échelle locale/au niveau de la base.

Une coopération et une coordination accrues sont nécessaires

- Le degré de coopération et de compréhension est faible au sein des groupes de soutien centraux de l'ICP. Des différences de compréhension existent entre le GOIFC, la Dir Sécur GI 3 et la DIIRI 3-5 ICP au sujet des processus des services de dépannage ainsi que des rôles et responsabilités connexes.
- Certains projets qui ont des besoins en matière d'ICP ne semblent pas recevoir une aide adéquate au niveau de la conception de la part des groupes de soutien centraux de l'ICP, comme les groupes de l'ingénierie et des politiques. Des conflits résultent du fait que les responsables des projets doivent terminer les produits livrables et de la capacité des groupes centraux à offrir une aide opportune.

RECOMMANDATIONS

Définir, clarifier, attribuer, documenter et communiquer les rôles et responsabilités clés des groupes de soutien de l'ICP, et ce, pour tous les aspects de l'ICP (notamment les politiques, le fonctionnement, l'enregistrement (à l'échelle locale/au niveau de la base et à l'administration centrale), la liaison externe, les services de dépannage, le contrôle et l'évaluation/la conformité).

- Séparer les politiques de l'ICP et l'évaluation (fonction de conformité) de la responsabilité centrale d'enregistrement (ACE).
- Regrouper les activités centrales d'enregistrement et de gestion des certificats de l'ICP (domaine désigné et STMM) et de l'IC (USCFC) chez une *seule* ACE.
- Faire en sorte que des procédures appropriées soient élaborées et mises en place avant de déplacer des activités au sein d'un groupe.
- Renforcer le contrôle des processus des ALE/CLE et regrouper les activités locales d'enregistrement à l'égard de l'ICP et de l'IC à l'échelle locale/au niveau de la base (une fois que les processus ont été rationalisés et mis en place). **BPR : SMA(GI)**

E. SOUTIEN ET PROCESSUS D'INFRASTRUCTURE

Pour fournir les services de sécurité dont les utilisateurs et les applications ont besoin, un système d'ICP doit être doté de processus structurés, en plus d'assurer le soutien permanent des opérations et de la maintenance de son autorité de certification[28] (AC), de ses services d'annuaire[29] (SA), de ses services d'enregistrement et de ses services de dépannage. Au MDN, la prestation de services permanents de soutien et de maintenance du cycle de vie est insuffisante dans la plupart des cas et complètement absente de quelques nouvelles applications d'ICP. Par exemple, même si l'ICP du STMM fait l'objet d'un projet pilote et doit être pleinement opérationnelle d'ici le milieu de 2005, la Dir Sécur GI 4 (groupe responsable des politiques de l'ICP et des fonctions d'ACE pour l'ICP du STMM) ne dispose d'aucun poste prévu au budget pour remplir ces rôles. Les ressources de soutien centrales qui existent déjà pallient l'absence de processus en essayant de les élaborer elles-mêmes en plus d'exécuter leurs tâches habituelles. Les questions relatives à la qualité des données compliquent les processus de gestion du cycle de vie des certificats, et le personnel clé manque de fonds pour les cours de formation nécessaires.

[28] L'ACE (c.-à-d. la Dir Sécur GI 3) a recours à l'AC (équipement utilisé pour créer et assigner les certificats de clé publique) pour gérer et exploiter l'ICP.
[29] Des services d'annuaire (SA) sont requis pour gérer le dépôt de certificats d'ICP. Un annuaire d'ICP ressemble à un annuaire électronique ou à un annuaire téléphonique.

Des services adéquats de soutien du cycle de vie sont essentiels

- AC et SA – Les ressources opérationnelles et techniques de l'AC et des SA sont insuffisantes pour tenir à jour la documentation et mener les activités de liaison externe, dont la prestation de services de conseils dans le cadre de projets. Il n'existe pas de documentation à jour sur le système d'ICP du domaine désigné, par exemple un concept d'opération.
- ACE – La structure actuelle au sein de la Dir Sécur GI 3 ne pourra pas appuyer le niveau d'activité d'enregistrement nécessaire au bon fonctionnement, une fois que l'ICP du STMM et d'autres nouvelles applications d'ICP comme l'IRPVD (accès à distance protégé) seront déployées. À ce stade-ci, la Dir Sécur GI 3 n'est pas en mesure de répondre à de fortes augmentations de la demande de services d'enregistrement ou de soutien à l'égard des nouvelles applications d'ICP sans modifier les processus existants. Par ailleurs, la Dir Sécur GI 4 ne dispose d'aucun poste prévu au budget pour appuyer l'ICP du STMM.
- ALE/CLE – Parmi les préoccupations concernant les processus des ALE/CLE, mentionnons la pertinence des nominations (environ 1 500 à l'heure actuelle), l'exactitude de la liste d'ALE/CLE, la prestation d'une formation continue aux ALE, et la gestion des ententes d'abonnement sur papier.
- Enregistrement – On pourrait accroître l'efficacité du processus d'enregistrement en utilisant un système d'enregistrement libre-service automatisé ainsi qu'en concevant et en exploitant des processus similaires pour les ICP des domaines désigné et classifié (à l'administration centrale et à l'échelle locale/au niveau de la base).

Les questions relatives à la qualité des données compliquent les processus

- Les écarts et les omissions dans les dépôts de données compliquent les processus de gestion de l'identité et des certificats d'ICP, affaiblissent la fonction d'authentification des utilisateurs et pourraient, dans certains cas, compromettre les restrictions liées à la sécurité de l'accès.
- Une partie de l'information d'adressage[30] du système de gestion des RH (SGRH/PeopleSoft) n'est pas à jour.
- Les données du SGHR/PeopleSoft sur les habilitations de sécurité ne sont pas conformes à celles du Grand prévôt adjoint (Sécurité) (GPA Sécur).
- L'ICP n'est pas encore intégrée aux systèmes appropriés de gestion des documents (p. ex., RH).

[30] L'information d'adressage désigne l'information utilisée pour associer une entité à un lieu particulier (p. ex., adresses physiques et/ou électroniques). Elle est nécessaire pour créer des certificats d'ICP et les relier à la personne ou à l'unité appropriée.

La formation est indispensable au personnel et aux utilisateurs de l'ICP

- Il est extrêmement important que le personnel d'enregistrement soit bien formé en ce qui concerne la suite de produits Entrust. Or, cela ne semble pas être le cas sur le terrain (c.-à-d. chez les ALE/CLE) ni chez l'ACE (Dir Sécur GI 3) à cause de la perception d'une pénurie de fonds.
- La formation initiale des utilisateurs du CECP semble adéquate. Toutefois, la compréhension continue des caractéristiques et du potentiel de l'ICP soulève de grandes questions. La majorité des utilisateurs ne sont pas pleinement conscients des capacités de la technologie (p. ex., ils ne savent pas comment utiliser la fonction de signature numérique de Entrust).

RECOMMANDATIONS

Renforcer, rationaliser et optimiser le soutien et les processus d'infrastructure distincts de l'ICP, en particulier l'enregistrement, la formation et les services de dépannage, pour en faire une structure de soutien qui combine les processus rationalisés des différents systèmes d'ICP et d'IC.

- Automatiser le plus possible le processus d'enregistrement afin d'accroître l'efficacité globale, de réduire au minimum les processus manuels et de diminuer les travaux de maintenance.
- Dresser un plan de ressources visant à déterminer la quantité de ressources nécessaires pour appuyer le fonctionnement efficace et continu du système d'ICP en tant qu'infrastructure ministérielle commune (en se fondant sur les nouveaux processus rationalisés ainsi que les rôles et responsabilités clarifiés). Ce plan devrait comporter un facteur de croissance basé sur l'activité prévue.
- Améliorer l'exhaustivité, l'uniformité et l'exactitude globales des données nécessaires au processus de gestion des certificats en examinant leur composition et en mettant à jour les processus et les liens des divers dépôts de données du MDN.
- Revoir l'approche de la formation sur l'ICP et s'assurer que toute la formation (destinée aux utilisateurs, aux ALE/CLE et au personnel de l'ACE) est appropriée, adéquate et opportune. Il faudrait entreprendre un examen approfondi des compétences existantes à l'égard de l'ICP et des besoins de formation actuels du personnel de l'ACE et des ALE/CLE en matière d'ICP.

BPR : SMA(GI)

F. MESURE DU RENDEMENT

Il n'existe pas de mesures opérationnelles de l'ICP pour signaler avec exactitude les coûts opérationnels et le degré d'utilisation de l'ICP, ce qui rend la planification de la charge de travail pratiquement impossible, l'obtention de fonds et de ressources supplémentaires difficile et l'évaluation des options de prestation des services extrêmement complexe (p. ex., la détermination du coût d'acquisition de certificats d'ICP auprès d'un fournisseur de services d'ICP externe par rapport à la prestation du service à l'interne). Pour mesurer le rendement du programme d'ICP et affecter les fonds et ressources du Ministère efficacement, les décideurs et intervenants ministériels ont besoin de données objectives et quantifiables. De plus, l'absence d'ententes sur les niveaux opérationnels (ENO) entre les groupes opérationnels centraux de l'ICP et d'ententes sur les niveaux de service (ENS) avec les nouvelles applications donne lieu à des attentes différentes parmi les groupes et peut nuire au rendement.

Absence de mesures opérationnelles de l'ICP

- Il n'existait aucune mesure du rendement pour le système d'ICP du MDN. En général, on semble penser que le CECP est relativement peu utilisé, mais le système d'enregistrement à l'ICP n'a pu le confirmer.
- Des estimations d'ordre de grandeur peuvent être déduites du nombre de clés recouvrées et de certificats émis. D'après ces données, il y avait environ 25 000 certificats *activés* (en date d'août 2004). De ce nombre, on estimait qu'entre 13 500 et 25 000 étaient ceux d'*utilisateurs actifs* (utilisateurs actifs qui se sont connectés à Entrust au moins une fois au cours de la dernière année). Quelque 35 000 certificats émis dans le cadre de la mise en œuvre du projet du CECP ont expiré.
- Aucune information sur les coûts n'est recueillie pour suivre les dépenses imputables au système d'ICP. Il n'y a pas de budget ou de modèle de coûts de l'ICP pour assurer le suivi des coûts réels ou prévoir l'incidence du soutien de nouvelles applications d'ICP. Cette situation est due en grande partie aux problèmes de gouvernance et au fait que l'ICP n'est pas gérée comme un programme d'infrastructure ministérielle.

Besoin d'ENO et d'ENS pour évaluer les niveaux de rendement actuels

- Il n'existe aucune ENO ou ENS à jour, et la responsabilité est floue à l'égard de l'une ou l'autre.
- Le besoin d'ENO entre les groupes opérationnels centraux crée de la confusion quant aux rôles et aux responsabilités. Les tâches requises ne sont pas exécutées.
- Le fait qu'il n'y ait pas d'ENS et que les critères de rendement ne soient pas définis empêche d'évaluer avec précision le système d'ICP et peut susciter des attentes différentes en matière de service et nuire au rendement (p. ex., en raison d'augmentations imprévues de l'activité d'enregistrement ou d'un équilibrage insuffisant de la charge de travail). Cela influe sur la capacité des groupes opérationnels centraux de négocier des niveaux de service avec les nouvelles applications d'ICP, comme le STMM, puisque les niveaux de rendement actuels sont mal compris ou mal surveillés.

RECOMMANDATIONS

Élaborer, rassembler, analyser et surveiller des mesures du rendement opérationnel et en faire rapport régulièrement afin de permettre l'évaluation du rendement, la budgétisation, l'analyse des coûts de même que la planification et l'équilibrage de la charge de travail.

- Élaborer un modèle de coûts complet (ponctuel + permanent) pour l'ICP à titre de programme d'infrastructure ministérielle commune.

Élaborer, négocier et mettre en œuvre des ENO à jour entre les groupes opérationnels centraux de l'ICP **et des ENS** avec les nouvelles applications d'ICP. **BPR : SMA(GI)**

G. INTÉGRATION DE LA TECHNOLOGIE DE L'ICP

Pour que l'ICP du MDN soit considérée comme un élément essentiel de l'infrastructure commune de la technologie de l'information (TI) du Ministère, la technologie de l'ICP doit être perçue comme un outil permettant d'améliorer les processus fonctionnels. La technologie (c.-à-d. le matériel et les logiciels) n'est qu'une partie d'un système d'ICP – les politiques, les processus et le personnel sont tout aussi importants. En fait, on affirme souvent que ces derniers sont les éléments les plus essentiels à la réussite de la mise en place de tout nouveau système. Dans le cas de l'ICP du MDN, il importe non seulement que la technologie soit solide mais aussi que le produit soit bien configuré et testé, et que les processus fonctionnels soient remaniés afin d'intégrer la nouvelle technologie de façon transparente. L'ICP du MDN ne réalise pas son plein potentiel comme outil de signature numérique des documents électroniques et d'automatisation des processus fonctionnels à cause des facteurs suivants : politiques et directives contradictoires, politiques qui n'évoluent pas au même rythme que la technologie, configurations de postes de travail locaux d'ICP qui ne permettent pas une vérification conviviale des signatures numériques, et manque d'importance accordée à la façon d'intégrer harmonieusement la technologie et les processus fonctionnels.

Il faut une meilleure intégration de la technologie de l'ICP et des processus fonctionnels

- L'importance de l'ICP pourrait être grandement accrue si certaines fonctions étaient configurées, modifiées ou personnalisées afin de permettre une meilleure intégration de la technologie et des processus fonctionnels.

  Par exemple :

  - Les options actuelles de Entrust pour la configuration des postes de travail ont comme résultat de supprimer une signature numérique dès qu'un document signé numériquement est ouvert. C'est à cause des options de configuration sélectionnées et non d'une faiblesse du logiciel, et ces paramètres ne sont peut-être pas les plus optimaux ou les plus conviviaux pour les utilisateurs.

Meilleure intégration requise

Exemples (suite)

- Un utilisateur devrait être capable d'ouvrir et de lire un document signé numériquement sans avoir à utiliser sa propre carte à puce d'ICP. Or, ce n'est pas le cas à l'heure actuelle au sein du MDN.

- Pour utiliser les signatures numériques plus efficacement afin d'automatiser et de réduire les délais d'approbation des processus manuels existants, une capacité de signature numérique « multiple » devrait être offerte. Par exemple, dans une organisation interrogée, l'ICP et les signatures numériques servent à une application pour le temps supplémentaire. Une capacité de signature « multiple » était nécessaire pour que cette application soit adoptée par le responsable fonctionnel, et elle a été réalisée grâce à la personnalisation du logiciel Entrust.

- Ces types de questions ont été portés à l'attention de l'équipe du CS Ex tout au long de l'examen. Les utilisateurs ne savaient pas qui était chargé de les résoudre ou qui en était responsable.

- Il est important de noter que l'équipe d'examen du CS Ex *ne* donne *pas* à entendre que le MDN devrait personnaliser son logiciel Entrust pour répondre à chaque demande d'utilisateur. Par ces observations, elle veut plutôt faire ressortir la nécessité de collaborer avec les groupes ou responsables fonctionnels afin de définir leurs besoins pour ce qui est d'automatiser les processus fonctionnels à l'aide de la technologie et des capacités de l'ICP. Une fois ces besoins compris, les groupes des opérations et de la technologie de l'ICP doivent déterminer la meilleure *façon* d'intégrer l'ICP pour accroître l'efficacité et la rentabilité du processus. Il faudrait entreprendre une analyse de rentabilisation et une analyse des coûts avant de décider de personnaliser ou de modifier certaines fonctions.

RECOMMANDATIONS

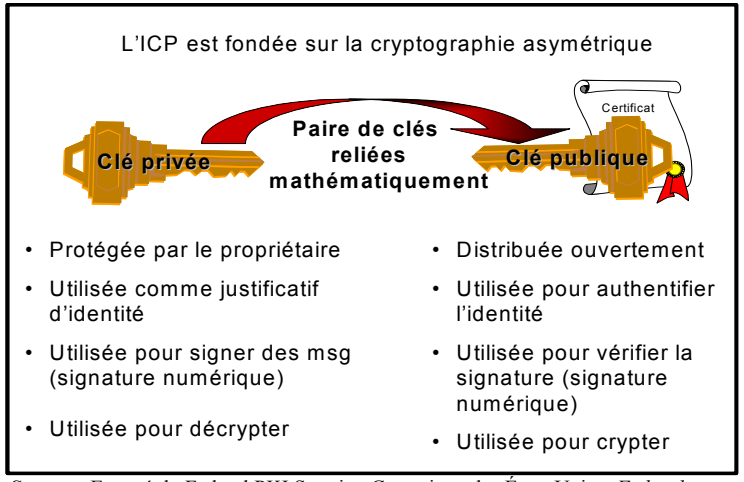
Définir/établir un nouveau rôle d'« analyste des activités » chargé d'assurer la liaison avec les utilisateurs et les groupes fonctionnels, de favoriser la communication et de rassembler les besoins. Le but consiste à développer une solide compréhension des processus fonctionnels et des besoins actuels de l'ICP pour déterminer la meilleure façon d'intégrer la technologie de l'ICP et d'obtenir les résultats souhaités (c.-à-d. gains d'efficience liés à une réduction des processus papier/manuels).

BPR : SMA(GI)

ANNEXE A – PRINCIPES DE BASE DE LA TECHNOLOGIE DE L'ICP

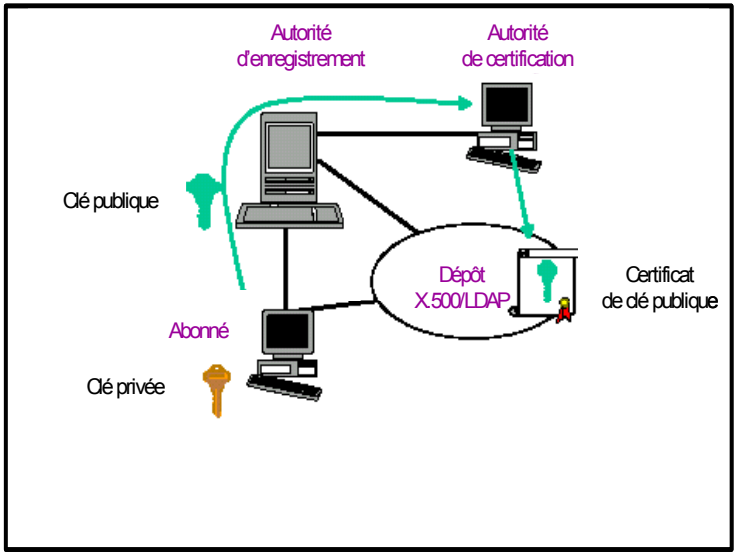
La ***cryptographie à clé publique*** permet de crypter de l'information grâce à deux clés reliées mathématiquement : l'une d'elles demeure privée et l'autre est rendue publique. La clé privée ne peut pas être déterminée à partir de la clé publique. Si une personne veut envoyer un message, elle utilise la clé publique du destinataire afin de crypter le message. Le destinataire utilise sa clé privée pour décrypter le message. L'expéditeur a donc l'assurance que seul le destinataire voulu peut lire le message.

La cryptographie à clé publique peut aussi servir à créer des ***signatures numériques*** selon les mêmes principes. Une signature numérique remplit une fonction analogue à celle d'une signature écrite et peut servir à vérifier l'origine et le contenu d'un message. Par exemple, le destinataire de données peut vérifier qui les a signées et confirmer qu'elles n'ont pas été modifiées après avoir été signées. Cela empêche l'expéditeur d'affirmer faussement ne pas avoir signé les données.



Source : Exposé du Federal PKI Steering Committee des États-Unis – *Federal Approach to Electronic Credentials* – J. Spencer

Composantes techniques de l'ICP



Une ***autorité de certification (AC)*** est une tierce partie de confiance chargée d'associer une paire de clés (c.-à-d. une clé publique et une clé privée) à une personne (ou une entité). Elle établit l'identité de la personne qui doit recevoir une paire de clés, émet les clés et les révoque quand une clé privée est perdue, volée ou autrement rendue publique, et elle diffuse des avis relatifs aux paires de clés qui ont été révoquées. L'AC signe également le certificat numérique (ICP), qui renferme la clé publique d'une personne et prouve que la personne identifiée sur le certificat détient la clé privée correspondante.

Une ***autorité d'enregistrement (AE)*** est une tierce partie de confiance chargée d'exécuter certaines des tâches administratives déléguées par l'AC. Par exemple, l'AE confirme l'identité des utilisateurs au nom de l'AC et amorce le processus de certification avec l'AC au nom des utilisateurs.

L'***annuaire de l'ICP*** (dépôt X.500/LDAP) est le dépôt où sont publiés tous les certificats de clé publique. Il ressemble à un annuaire électronique ou à un annuaire téléphonique.

ANNEXE A

L'ICP est extensible

Étant donné que la clé publique d'une personne n'a pas besoin de demeurer secrète, toutes les clés publiques émises par une AC peuvent être publiées dans un annuaire d'ICP et mises à la disposition de tous les abonnés de l'ICP. C'est ce qui fait de l'ICP une solution extensible, en ce sens qu'elle peut accueillir de nombreux utilisateurs répartis. Il s'agit là d'un des grands avantages par rapport au cryptage symétrique ou cryptage à clé secrète, selon lequel deux parties partagent une seule clé pour le cryptage et le décryptage. Le cryptage symétrique[31] suppose que les parties qui partagent une même clé peuvent compter l'une sur l'autre pour ne pas divulguer la clé et la protéger contre toute modification; elles doivent donc se faire entièrement confiance. Il devrait être évident qu'avec le cryptage symétrique, la gestion des clés peut devenir extrêmement compliquée lorsque le nombre d'utilisateurs est élevé.

Par contre, avec l'ICP, la gestion des clés peut être gérée de façon centrale de sorte qu'une personne n'a qu'à se soucier de ne pas divulguer sa clé privée. Un particulier qui veut envoyer un message crypté à quelqu'un d'autre n'a pas besoin de partager une clé secrète avec lui. Il suffit que l'expéditeur cherche la clé publique du destinataire dans l'annuaire de l'ICP, puis crypte le message qu'il désire lui envoyer. Une fois que l'infrastructure nécessaire est en place, l'ICP peut recevoir un nombre croissant d'utilisateurs.

Cocertification

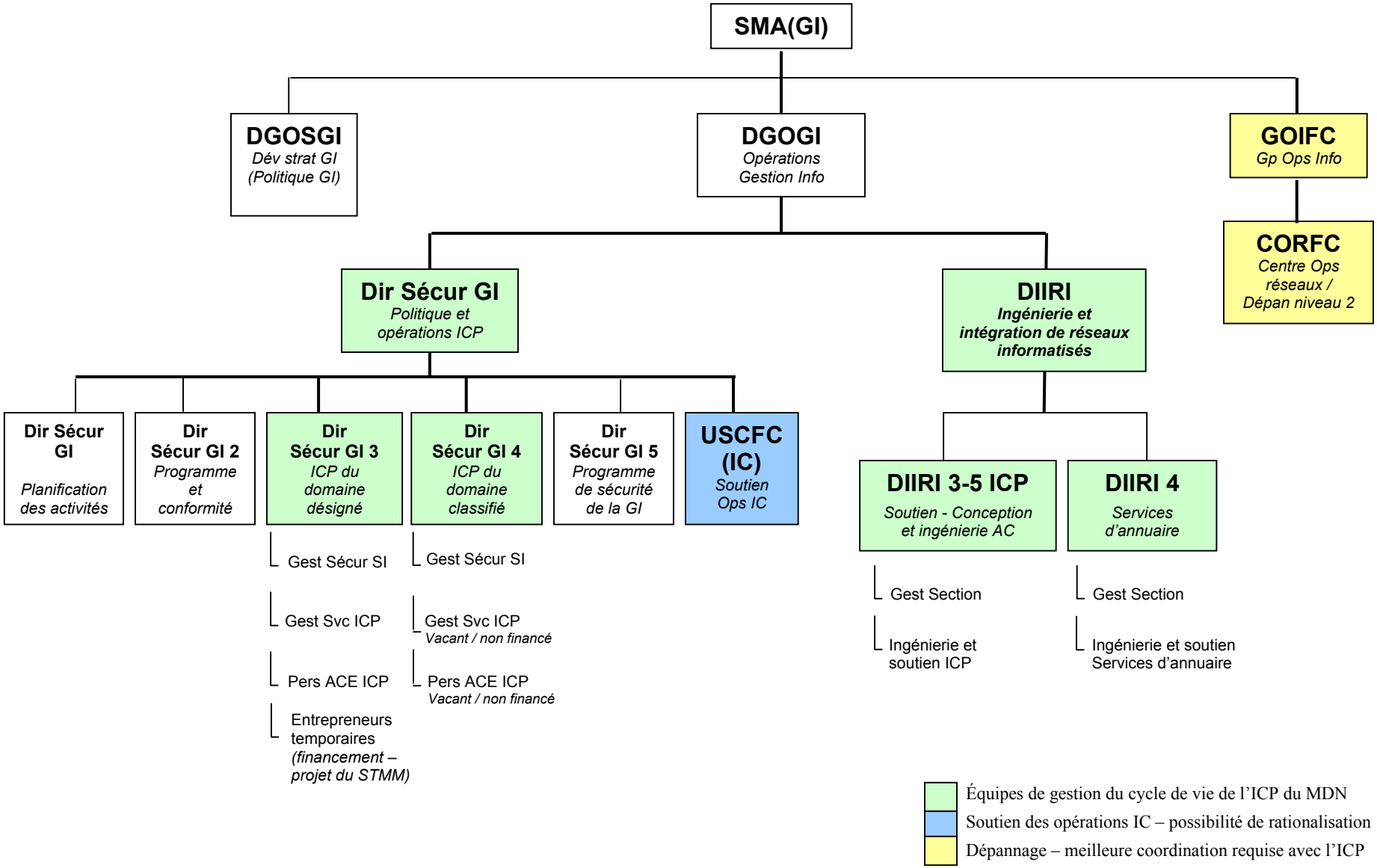
La cocertification[32] est un processus entrepris par des autorités de certification afin d'établir un lien de confiance. Les autorités de certification échangent leurs cocertificats et permettent aux utilisateurs d'un certificat émis par l'une d'elles de communiquer par des moyens électroniques sûrs avec les utilisateurs de l'autre. Quand deux autorités de certification concluent une entente de cocertification, elles acceptent de se faire mutuellement confiance et de se fier aux certificats de clé publique et aux clés de l'autre comme si elles les avaient émis elles-mêmes. Aux fins de la cocertification ou de la reconnaissance des autorités de certification, la Charnière fédérale canadienne de l'Infrastructure à clé publique constitue l'autorité de certification de charnière du gouvernement du Canada.

Renseignements supplémentaires

Pour en savoir plus long sur l'ICP, prière de consulter les sites Web ci-dessous.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg9-f.html (chapitre 19 du manuel – Cryptographie)
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/siglist_f.asp (politique régissant l'ICP du GC)
http://www.pkiforum.org/whitepapers.html (divers livres blancs et notes sur l'ICP)

[31] Manuel canadien de la sécurité des technologies de l'information du CST. Mars 1998. Section 19.1.1 – Cryptographie symétrique.
[32] Politique du SCT sur la gestion de l'ICP au gouvernement du Canada. Date d'entrée en vigueur : 26 avril 2004. Section 4 – Définitions.

ANNEXE B – ORGANIGRAMME (SIMPLIFIÉ) DE « L'ICP DU MDN »



ANNEXE C – LISTE DES APPLICATIONS D'ICP ACTUELLES ET PRÉVUES DU MDN

Applications actuelles	Domaine ICP	Nombre estimatif d'utilisateurs/de certificats*	Date cible d'entrée en service
CECP *Courrier électronique commun protégé*	Désigné	De 13 500 à 25 000 certificats actifs	En service
STMM *Système de traitement des messages militaires*	Classifié	De 5 000 à 10 000 certificats seront distribués pour 3 500 postes de travail.	Projet pilote DGE 2005
Applications à venir	**Domaine ICP**	**Nombre prévu d'utilisateurs/de certificats***	**Date cible d'entrée en service**
SISFC *Système d'information sur la santé des FC*	Désigné	3 800 (dont 800 seront des entrepreneurs, certains de l'extérieur)	Début déc. 2004
FEVS *Forfait d'entraînement au vol et de soutien*	Désigné	Maximum de 165 utilisateurs à la fois. Jusqu'à 327 stagiaires par année.	2005
SIGRHD *Système intégré de gestion des RH de la Défense*	Désigné	Certificats de dispositif pour appuyer de 7 000 à 8 000 utilisateurs	2005
IRPVD *Accès à distance protégé*	Désigné	De 5 000 à 6 000 utilisateurs actifs et plus	Début automne 2004
SISAM *Système d'information – Soutien et acquisition du matériel*	Désigné	Environ 5 000 utilisateurs	À compter de fin 2004
PHM *Programme d'hélicoptère maritime*	Désigné	Il faudra 50 utilisateurs au début. Ce nombre passera à 1 000 en quatre ans.	Début automne 2004
SISEPM *Système d'information – Sécurité et police militaire*	Désigné	1 100 utilisateurs (Police militaire) au Canada	Peut-être 2005

Source **:** *Équipes de projet – information reçue entre juin et août 2004.*

** À l'exception du STMM, le nombre estimatif de certificats d'ICP indiqué ci-dessus ne représente pas nécessairement le nombre de certificats à émettre. Dans la plupart des cas, si un utilisateur possède déjà une carte à puce d'ICP, il pourra probablement s'en servir pour avoir accès aux applications d'ICP à venir qui sont énumérées ci-dessus. Le STMM exige une carte à puce distincte d'ICP parce qu'il s'agit d'un système classifié.*

ANNEXE D – QU'ARRIVERAIT-IL SI UNE ICP MINISTÉRIELLE N'ÉTAIT PLUS DISPONIBLE?

Incidence sur les utilisateurs actuels de l'ICP (c.-à-d. les utilisateurs du CECP) :

Les utilisateurs actuels nous ont dit que, en l'absence d'une ICP, ils devraient :

- recourir de nouveau aux processus papier et aux rencontres personnelles, ce qui entraînerait une utilisation inefficace du temps et des ressources; ou
- envisager de contrevenir à la politique pour transmettre des données sensibles en clair, d'où le risque d'embarras ou de vulnérabilité possible en cas de divulgation.

Incidence sur les applications d'ICP à venir :

- Il y aurait une incidence considérable sur la mise en place des applications à venir, comme le STMM, l'IRPVD et le SISFC.
- Il faudrait trouver une solution de rechange pour assurer une identification et une authentification rigoureuses.
- La communication de données sensibles serait moins efficace, et les objectifs en matière de sécurité de la TI seraient plus difficiles à atteindre.
- Des certificats d'ICP pourraient être obtenus auprès d'un service d'AC externe, mais peut-être à un coût élevé. Il y aurait également une perte de contrôle sur l'AC et une perte possible de souveraineté (p. ex., si l'AC se trouvait à l'extérieur du Canada), ce qui serait inacceptable, notamment dans le cas de l'ICP du domaine classifié.

Incidence sur les besoins futurs en matière d'ICP :

- Certains hauts représentants du MDN ont indiqué qu'il était nécessaire de collaborer et d'échanger de l'information en toute sûreté avec le SCT et plusieurs autres ministères, dont les Finances, les Affaires étrangères, le Commerce international et la Justice. Une AC hébergée à l'externe, comme le Service d'applications protégées et de gestion des clés (SAPGC) de TPSGC, peut constituer une solution de rechange viable en ce qui concerne l'obtention de services d'ICP, mais le MDN devrait quand même maintenir certaines activités d'enregistrement et les coûts connexes.

- Tous les employés du GC (environ 260 000) utiliseront l'application Web de la rémunération du GC. Sans une ICP du MDN (qui a été cocertifiée avec l'ICP du GC), les employés devront obtenir un certificat SAPGC/TPSGC ou Web pour avoir accès à l'application de la rémunération ou à toute nouvelle application de l'ICP du GC, y compris les services du GED.

ANNEXE D

- Dans l'avenir, il se peut que le MDN ait besoin de conclure des ententes de cocertification avec des organisations externes comme l'OTAN, le département américain de la Défense (DoD) ou d'autres groupes alliés. Un fournisseur de services d'ICP externe ne serait pas en mesure de fournir les garanties de sécurité nécessaires pour pouvoir communiquer avec ces types d'organisations, car le service externe ne serait pas capable d'appuyer un niveau de sécurité supérieur à un niveau d'assurance moyen.

ANNEXE E – BONNES PRATIQUES ET LEÇONS TIRÉES D'AUTRES ORGANISATIONS

Gestion et politique

- L'ICP doit être axée sur des applications fonctionnelles – c.-à-d. qu'au sein du MDN et des FC, elle doit répondre aux besoins d'échange protégé de données électroniques.
- L'ICP est une infrastructure et doit être mise en œuvre en tant que telle – c.-à-d. comme un service commun à de multiples systèmes/applications.
- L'ICP doit recevoir l'appui de la haute direction.
- L'ICP est complexe et exige que des ressources y soient affectées en propre de manière à fonctionner comme prévu. La direction doit comprendre qu'il faut des ressources adéquates pour assurer le bon fonctionnement du système.
- Une PC et un EPC judicieux sont essentiels au succès et à la discipline.

Conception

- L'ICP et la sécurité doivent être intégrées dès la conception des applications.
- Il faut d'abord mettre en place une infrastructure d'identification bien définie.
- L'harmonisation de la technologie et de l'approche touchant de multiples ICP (systèmes désignés et classifiés) réduit les besoins de maintenance et de formation ainsi que le coût et les efforts globaux que nécessite l'exploitation du système.

Enregistrement

- Il est essentiel d'automatiser l'enregistrement.
- Les autorités locales d'enregistrement (ALE) doivent être prêtes à servir. Il faudrait envisager de confier le rôle d'ALE aux superviseurs ou étoffer une structure de soutien existante au lieu d'en établir une qui serait entièrement nouvelle.
- Il faut maintenir des rapports réguliers avec les ALE et s'assurer que les attentes sont pleinement communiquées.
- Le changement d'un justificatif d'identité (p. ex., en raison d'un changement de rôle, d'un mouvement d'employé ou de la révocation d'un certificat) entraîne de nombreuses conséquences et doit donc être bien géré.

ANNEXE E

Formation

- Les utilisateurs ne lisent pas les instructions – il faut s'attendre à ce que les services de dépannage reçoivent de nombreux appels.
  - L'interface avec l'utilisateur doit être claire afin que ce dernier comprenne ce qui se passe.
  - La formation des utilisateurs peut être assez informelle, et elle ne constitue pas une question importante après la mise en place initiale.
- Une formation officielle est indispensable dans le cas du personnel de l'ICP (ALE, agents de l'ICP, etc.).

Autre

- À l'instar du courrier électronique, il est difficile de mesurer le rendement de l'investissement en ce qui concerne l'ICP. Par conséquent, les besoins fonctionnels doivent être bien formulés, bien communiqués et bien compris par les intervenants et la haute direction.

ANNEXE F – LISTE D'ACRONYMES ET D'ABRÉVIATIONS

AC	Autorité de certification
ACE	Autorité centrale d'enregistrement
AEPOS	AEPOS Technologies Corporation
AGI	Autorité de gestion de l'infrastructure à clé publique
ALE	Autorité locale d'enregistrement
APE	Autorisation provisoire d'exploitation
ARC	Agence du revenu du Canada
BAC	Bibliothèque et Archives Canada
C&A	Certification et accréditation
CECP	Courrier électronique commun protégé (système opérationnel)
CEM SMA(GI)	Chef d'état-major du Sous-ministre adjoint (Gestion de l'information)
CLE	Coordonnateur local d'enregistrement
CORFC	Centre d'opérations de réseaux des Forces canadiennes
CRD	Chef – Recherche et développement
CS Ex	Chef – Service d'examen
CST	Centre de la sécurité des télécommunications
DGE	Déploiement à grande échelle
DGI	Directive sur la gestion de l'information
DGOGI	Directeur général – Opérations (Gestion de l'information)
DGOSGI	Directeur général – Orientation stratégique (Gestion de l'information)
DIIRI	Directeur – Ingénierie et intégration de réseaux informatisés
Dir Sécur GI	Direction de la sécurité de la GI
DoD	Département de la Défense (É.-U.)
DPSGI	Directeur – Planification stratégique (Gestion de l'information)
D Séc TI	Direction de la sécurité de la technologie de l'information
EMR	Évaluation de la menace et des risques
ENO	Entente sur les niveaux opérationnels
ENS	Entente sur les niveaux de service
EPC	Énoncé de pratiques de certification
É.-U.	États-Unis
FDA	Food and Drug Administration
F&E	Fonctionnement et entretien
FEVS	Forfait d'entraînement au vol et de soutien (projet)
GAO	Government Accounting Office (É.-U.)
GC	Gouvernement du Canada
GCVP	Gestion du cycle de vie du produit
GED	Gouvernement en direct
GOIFC	Groupe des opérations d'information des Forces canadiennes
GPA Sécur	Grand prévôt adjoint (Sécurité)
IC	Infrastructure à certificats
ICP	Infrastructure à clé publique
IPO	Instruction permanente d'opération
IRPVD	Infrastructure du réseau privé virtuel de la Défense (projet)
MDN	Ministère de la Défense nationale
MDN/FC	Ministère de la Défense nationale et Forces canadiennes
OTAN	Organisation du Traité de l'Atlantique Nord
PB	Protégé B
PC	Politique de certification
PHM	Programme d'hélicoptère maritime (projet)
PM	Police militaire
PSM	Protocole de sécurité de message
RH	Ressources humaines
RCN	Région de la capitale nationale
RED	Réseau étendu de la Défense (domaine désigné)
SA	Services d'annuaire
SAPGC	Service d'applications protégées et de gestion des clés (TPSGC)
SCT	Secrétariat du Conseil du Trésor
SGRH	Système de gestion des ressources humaines
SIGRHD	Système intégré de gestion des RH de la Défense (projet)
SISAM	Système d'information – Soutien et acquisition du matériel (projet)
SISEPM	Système d'information – Sécurité et police militaire
SISFC	Système d'information sur la santé des Forces canadiennes (projet)
SMA(GI)	Sous-ministre adjoint (Gestion de l'information)
STMD	Système de traitement des messages de la Défense (projet)
STMM	Système de traitement des messages militaires (projet)
TI	Technologie de l'information
TPSGC	Travaux publics et Services gouvernementaux Canada
USCFC	Unité de soutien cryptographique des FC (relève de la D Sécur GI)

ANNEXE G – PLANS D'ACTION DE LA DIRECTION

Point	Recommandation du CS Ex	BPR/BC	Plans d'action de la direction
A.	**Élaborer une « feuille de route » pour l'ICP** afin de définir et de formuler clairement les besoins fonctionnels et de sécurité du MDN en ce qui a trait à une ICP d'entreprise. Cette « feuille de route » devrait préciser comment et où l'ICP s'insère dans le cadre global de sécurité de la TI, en plus de définir les besoins fonctionnels auxquels l'ICP répond pour les applications actuelles et futures. ❑ L'ICP ne devrait être déployée que pour répondre à des besoins fonctionnels définis et à une analyse de rentabilisation financière (ou analyse des coûts) claire. ❑ Un effort concerté doit être fait pour accroître la sensibilisation et la compréhension du Ministère à l'égard de l'utilisation et des capacités de l'ICP.	BPR : Dir Sécur GI BPR : Dir Sécur GI BC : Contrôleur du Groupe GI	D'accord. La Dir Sécur GI devrait diriger l'élaboration d'une feuille de route de l'ICP du MDN aux fins d'approbation par la haute direction. Cela pose problème à l'heure actuelle, car les ressources sont limitées. À ce jour, le MDN a déterminé que la feuille de route de l'ICP du DoD américain pouvait être un modèle à suivre. La feuille de route du MDN comportera un programme de formation et de sensibilisation. La Dir Sécur GI établira les besoins en matière d'ICP en consultant les intervenants du Ministère. Or, le manque de personnel nuira à cette activité. De plus, étant donné que les ICP à grande échelle sont relativement peu au point, il est prématuré de procéder à une analyse de rentabilisation financière claire tant qu'on n'aura pas acquis une meilleure compréhension des avantages et des coûts.
B.	**Gérer l'ICP comme un programme d'infrastructure ministérielle commune** et établir les structures de gouvernance et les processus de planification stratégique requis/appropriés pour fournir des directives générales, approuver officiellement les politiques de l'ICP et veiller à ce qu'il y ait le moins possible de vides et d'écarts stratégiques.	BPR : Dir Sécur GI	D'accord. Il est proposé que le MDN gère l'ICP comme un programme d'infrastructure commune en établissant un cadre de gouvernance et en l'intégrant au cadre existant de gestion d'infrastructure à clé. Un cadre de gouvernance de l'ICP du MDN est proposé dans une ébauche de DGI – la DGI 118 sur la gouvernance de l'ICP – qui est en cours de préparation aux fins d'approbation par le SMA(GI). La DPSGI a déjà accepté d'accélérer le traitement de toute proposition de politique sur l'ICP dès qu'elle sera reçue.

* **Nota** : Le CS Ex assurera uniquement le suivi des recommandations clés (alphanumériques) au nom du Comité de vérification et d'évaluation. Les sous-recommandations (points vignettes) visent à fournir d'autres directives sur la mise en œuvre des recommandations clés.

ANNEXE G

Point	Recommandation du CS Ex	BPR/BC	Plans d'action de la direction
	❑ Des plans stratégiques liés à la fusion du soutien et des processus d'infrastructure des différents systèmes d'ICP et d'IC, ainsi que des directives sur la voie à suivre devraient être intégrés à la « feuille de route » de l'ICP.	BPR : Dir Sécur GI	La Dir Sécur GI 3 et l'USCFC étudieront les activités et ressources communes exigées par l'infrastructure actuelle de l'IC et de l'ICP (étude de l'IC/ICP), ainsi que les points communs avec les activités existantes de sécurité cryptographique et de gestion des clés, pour fournir des processus plus rationalisés qui tirent parti des ressources existantes. Les résultats figureront dans la feuille de route de l'ICP du MDN.
C1.	**Mettre à jour les politiques de l'ICP et les soumettre à l'approbation officielle** de l'autorité ministérielle compétente. Les politiques de l'ICP devraient à tout le moins comprendre la PC et l'EPC ainsi qu'une politique ou directive claire sur la nécessité et l'utilisation de clés de cryptage et de signatures numériques d'ICP.	BPR : Dir Sécur GI BC : DIIRI	D'accord. La Dir Sécur GI s'occupera du traitement de la PC du GC et de l'EPC du MDN aux fins d'approbation par le SMA(GI), conformément au cadre de gouvernance de l'ICP.
	❑ Définir clairement les processus servant à élaborer, à tenir à jour, à mettre en œuvre, à approuver et à publier les politiques de l'ICP.	BPR : Dir Sécur GI BC : DPSGI	L'élaboration, la mise en œuvre et la publication des politiques de l'ICP seront conformes à la DOAD 6000-0 et coordonnées par la DPSGI. L'approbation sera donnée par l'entremise de l'autorité de gestion de l'ICP (AGI), conformément au cadre de gouvernance de l'ICP. La DPSGI a déjà accepté d'accélérer le traitement de toute proposition de politique sur l'ICP.
	❑ Réviser les IPO de l'ICP (c.-à-d. les IPO des postes de travail du CECP et du STMM) pour les harmoniser avec les politiques approuvées de l'ICP.		Il est proposé d'inclure l'élaboration et la tenue à jour des IPO de l'ICP dans le cadre existant de gestion des documents COMSEC.

ANNEXE G

Point	Recommandation du CS Ex	BPR/BC	Plans d'action de la direction
	❑ Effectuer une inspection officielle pour vérifier la conformité aux politiques approuvées de l'ICP (dans l'année suivant l'approbation).	BPR : Dir Sécur GI	Les inspections de conformité seront considérées dans le cadre de l'étude de l'IC/ICP, et l'on envisagera de les inclure dans le processus de certification et d'accréditation ou dans le processus de vérification COMSEC.
C2.	**Examiner et réviser les politiques et procédures ministérielles liées à l'ICP**, notamment sur la gestion et l'utilisation du courriel, l'application par le MDN de la politique de BAC régissant les données consignées, la gestion de l'information, etc.	BPR : Dir Sécur GI BC : DIIRI	La Dir Sécur GI et la DIIRI consulteront les responsables des applications d'ICP au sujet des politiques et des procédures qui leur sont propres.
	❑ Déterminer les politiques et procédures ministérielles sur l'ICP à réviser.	BPR : Dir Sécur GI	L'AGI sera chargée de cautionner les questions relatives à la politique de gestion de l'ICP.
	❑ Le responsable des politiques ou le Comité de gouvernance de l'ICP devrait approuver la mise à jour de toute politique ministérielle concernant l'ICP.	BPR : Dir Sécur GI	Le Comité de surveillance de la GI sera chargé d'avaliser les directives sur l'utilisation de l'ICP dans les processus fonctionnels du Ministère.
D.	**Définir, clarifier, attribuer, documenter et communiquer les rôles et responsabilités clés** des groupes de soutien de l'ICP, et ce, pour tous les aspects de l'ICP.	BPR : DGOGI BC : Dir Sécur GI DIIRI CORFC	La DGOGI établira les responsabilités des groupes de soutien de l'ICP dans le cadre du remaniement de la Division.
	❑ Séparer les politiques de l'ICP et l'évaluation de la responsabilité de l'ACE.	BPR : Dir Sécur GI	La Dir Sécur GI remaniera les rôles internes de la Dir Sécur GI 3 et de l'USCFC une fois que l'étude de l'IC/ICP sera terminée.

ANNEXE G

Point	Recommandation du CS Ex	BPR/BC	Plans d'action de la direction
	❑ Regrouper les activités centrales d'enregistrement et de gestion des certificats de l'ICP et de l'IC (USCFC) chez une *seule* ACE.		
	❑ Faire en sorte que des procédures appropriées soient élaborées et mises en place avant de déplacer des activités au sein d'un groupe.	BPR : Dir Sécur GI BC : Membres de l'AGI	Les processus des ALE/CLE seront décrits dans les politiques et procédures à publier par l'AGI.
	❑ Renforcer le contrôle des processus des ALE/CLE et regrouper les activités locales d'enregistrement à l'égard de l'ICP et de l'IC à l'échelle locale/au niveau de la base (une fois les processus rationalisés et mis en place).	BPR : Dir Sécur GI	Les rôles et responsabilités figureront dans la feuille de route de l'ICP du MDN.
E.	**Renforcer, rationaliser et optimiser le soutien et les processus d'infrastructure distincts de l'ICP,** en particulier l'enregistrement, la formation et les services de dépannage, pour en faire une structure de soutien qui combine les processus rationalisés des différents systèmes d'ICP et d'IC.	BPR : DGOGI	La DGOGI rationalisera le soutien et les processus de l'ICP dans le cadre du remaniement de la Division.
	❑ Automatiser le plus possible le processus d'enregistrement afin d'accroître l'efficacité globale.	BPR : Dir Sécur GI BC : DIIRI	La DIIRI et la Dir Sécur GI dresseront un plan de ressources pour la stabilisation de l'ICP des réseaux désigné et classifié.
	❑ Dresser un plan de ressources visant à déterminer la quantité de ressources		

ANNEXE G

Point	Recommandation du CS Ex	BPR/BC	Plans d'action de la direction
	nécessaires pour appuyer le fonctionnement efficace et continu du système d'ICP en tant qu'infrastructure ministérielle commune.		
	❑ Améliorer l'exhaustivité, l'uniformité et l'exactitude globales des données nécessaires au processus de gestion des certificats en examinant leur composition et en mettant à jour les processus et les liens des divers dépôts de données du MDN.	BPR : Dir Sécur GI	Les questions liées à l'intégrité des données sur la gestion de l'identité seront traitées dans la directive qui sera acheminée à l'AGI, ce qui comprend les ENO avec les organisations compétentes en matière de RH et d'habilitations de sécurité. Il convient de noter que les lacunes des processus de gestion de l'identité au MDN ont une incidence considérable sur l'ICP, mais elles en dépassent la portée.
	❑ Revoir l'approche de la formation sur l'ICP et s'assurer que toute la formation (destinée aux utilisateurs, aux ALE/CLE et au personnel de l'ACE) est appropriée, adéquate et opportune.	BPR : Dir Sécur GI	Il est proposé que l'infrastructure de soutien de l'ICP englobe le personnel de l'officier du développement de l'instruction (ODI), afin d'évaluer la formation actuelle et de déterminer les futurs besoins de formation.
F1.	**Élaborer, rassembler, analyser et surveiller des mesures du rendement opérationnel et en faire rapport** régulièrement afin de permettre l'évaluation du rendement, la budgétisation, l'analyse des coûts de même que la planification et l'équilibrage de la charge de travail.	BPR : Dir Sécur GI BC : DGOGI	La DGOGI veillera à ce que les questions relatives au contrôle du rendement du système et à la planification des capacités de l'ICP soient traitées lors du remaniement de la Division. L'organisation chargée de gérer l'ICP rassemblera les statistiques (manuelles) sur les processus et en fera rapport.
	❑ Élaborer un modèle de coûts complet pour l'ICP à titre de programme d'infrastructure commune.	BPR : Dir Sécur GI BC : DIIRI	La DIIRI et la Dir Sécur GI élaboreront un modèle de coûts dans le cadre du plan de ressources pour la stabilisation de l'ICP. Or, étant donné que les ICP à grande échelle sont relativement peu au point, il est

ANNEXE G

Point	Recommandation du CS Ex	BPR/BC	Plans d'action de la direction
			prématuré d'élaborer un modèle des coûts d'utilisation tant qu'on n'aura pas acquis une meilleure compréhension des coûts globaux.
F2.	**Élaborer, négocier et mettre en œuvre des ENO à jour** entre les groupes opérationnels centraux de l'ICP **et des ENS** avec les nouvelles applications d'ICP.	BPR : DGOGI BC : AGI	La cellule de la DGOGI responsable des ENO et des ENS veillera à ce que des ENO et des ENS liées à l'ICP soient rédigées et acheminées à l'AGI.
G.	**Définir/établir un nouveau rôle d'« analyste des activités » chargé d'assurer la liaison avec les utilisateurs et les groupes fonctionnels** et de favoriser la communication. Le but consiste à développer une solide compréhension des processus fonctionnels et des besoins actuels de l'ICP pour déterminer la meilleure façon d'intégrer la technologie de l'ICP et d'obtenir les résultats souhaités (c.-à-d. accroître l'efficacité opérationnelle et réaliser des économies).	BPR : Dir Sécur GI BC : CCI AGI	La Dir Sécur GI dispensera une formation initiale sur l'ICP à ses analystes et aux membres de la cellule consultative de l'ICP (CCI) relevant de l'AGI, afin de cerner les possibilités au niveau de l'entreprise et les incidences de solutions possibles ou proposées axées sur l'ICP.

Comme nous l'avons indiqué précédemment dans la section **Sommaire des résultats** du rapport, le CS Ex encourage la direction à prendre certaines mesures plus tôt que prévu, particulièrement en ce qui concerne :

- l'élaboration d'une feuille de route de l'ICP du MDN (point A);
- l'éclaircissement des rôles et des responsabilités des groupes de soutien de l'ICP du MDN (point D);
- la rationalisation du soutien et des processus d'infrastructure distincts de l'ICP (point E).