DIRECTION DES GRANDS PROJETS

EDT — ANNEXE A de l'appendice A

ARCHITECTURE ACTUELLE — ITR / SAID / SSV

RENOUVELLEMENT DU SAID

Dernière modification :	2015-02-17
Statut :	Version préliminaire
SRT :	REB-11
No de la version :	0.1
No de document SGDDI :	À déterminer
Classification :	Protégé « A »

REGISTRE DES MODIFICATIONS

TABLE DES MATIÈRES

FIGURES

TABLEAUX

1. INTRODUCTION

1.1 OBJET

1. Le présent document vise à décrire l'architecture de GRC/SPC dans laquelle fonctionne le système d'ITR. Malgré son renouvellement, le SAID et tous ses sous-systèmes doivent fonctionner efficacement dans cette architecture et respecter toutes les exigences du présent EDT.
2. Voici donc une courte description générale de l'architecture de GRC/SPC, suivie d'une description plus détaillée des éléments de cette architecture liés aux composants du SAID.

1.2 GÉNÉRALITÉS

1. Le GRC joue un rôle crucial dans la collecte, le stockage et la gestion les renseignements liés au travail des policiers. C'est par le réseau des Services nationaux de police (SNPNet) que les organismes canadiens d'application de la loi ont accès à ces renseignements centralisés. SNPNet prend aussi en charge des applications propres à la GRC; c'est un inter-réseau national spécialisé et privé qu'utilisent la GRC et ses partenaires affinitaires. Il rend possible la transmission de données électroniques à l'appui des services administratifs et opérationnels qu'utilisent les organisations clientes. Le réseau SNPNet dessert 60 000 utilisateurs environ dans grosso modo 1200 emplacements au Canada et dans les régions arctiques.
2. Le réseau SNPNet permet aussi aux agences policières nationales et étrangères, aux organismes fédéraux, provinciaux et municipaux canadiens ainsi qu'aux agences privées d'avoir accès aux fonction d'ITR. Ces communications sont assurées Posture de sécurité du réseau (PSR), un RPV privé sécurisé contrôlé et géré par Services partagés Canada, par l'établissement d'un RPV dans le Réseau de la Voie de communication protégée (VCP) du GC ou par l'établissement d'un RPV sécurisé dans Internet. Toutes les communications d'ITR sont effectuées par l'une de ces méthodes; elles sont décrites plus en détail dans le présent document.

1.3 ORGANISATION DU DOCUMENT

1. Le présent document donne une courte description générale de l'architecture de la GRC. Après cet aperçu, il décrit l'architecture actuelle du SAID et du SSV.
2. L'architecture du SAID et du SSV est décrite en général; cette description est suivie de diagrammes et descriptions détaillés des connexions entre divers éléments du SAID et du SSV, notamment des interfaces avec les composantes de l'ITR et de l'architecture de GRC/SPC.

2. APERÇU DE L'ARCHITECTURE DE LA GRCC ET DE SPC

2.1 APERÇU CONCEPTUEL — ARCHITECTURE DE SÉCURITÉ DE GRC/SPC

1. Le diagramme conceptuel suivant illustre l'architecture de sécurité de la GRC et de SSC dans laquelle l'ITR fonctionne. On pourra approfondir tout détail de cette architecture de sécurité touchant l'ITR à la journée de l'industrie associée au présent EDT sur le renouvellement du SAID.
2. Le diagramme montre le réseau spécialisé privé de la GRC (SNPNet) ainsi que la PSR et les connexions VCP/Internet par RPV destinées aux agences externes.

   N.B. : Certains sites passent d'une connexion RPV à une connexion MLPS (*Multi-Layer Protocol Switching*, protocole de commutation multicouche), mais cela n'a aucune incidence sur l'ITR ou le SAID; c'est tout bonnement une autre façon d'établir une connexion sécurisée et chiffrée.
3. Le diagramme indique aussi les dispositifs d'ITR utilisées dans les divers types de connexions.
4. Il montre aussi l'emplacement conceptuel du SNS et du SAID dans l'architecture de GRC/SPC.

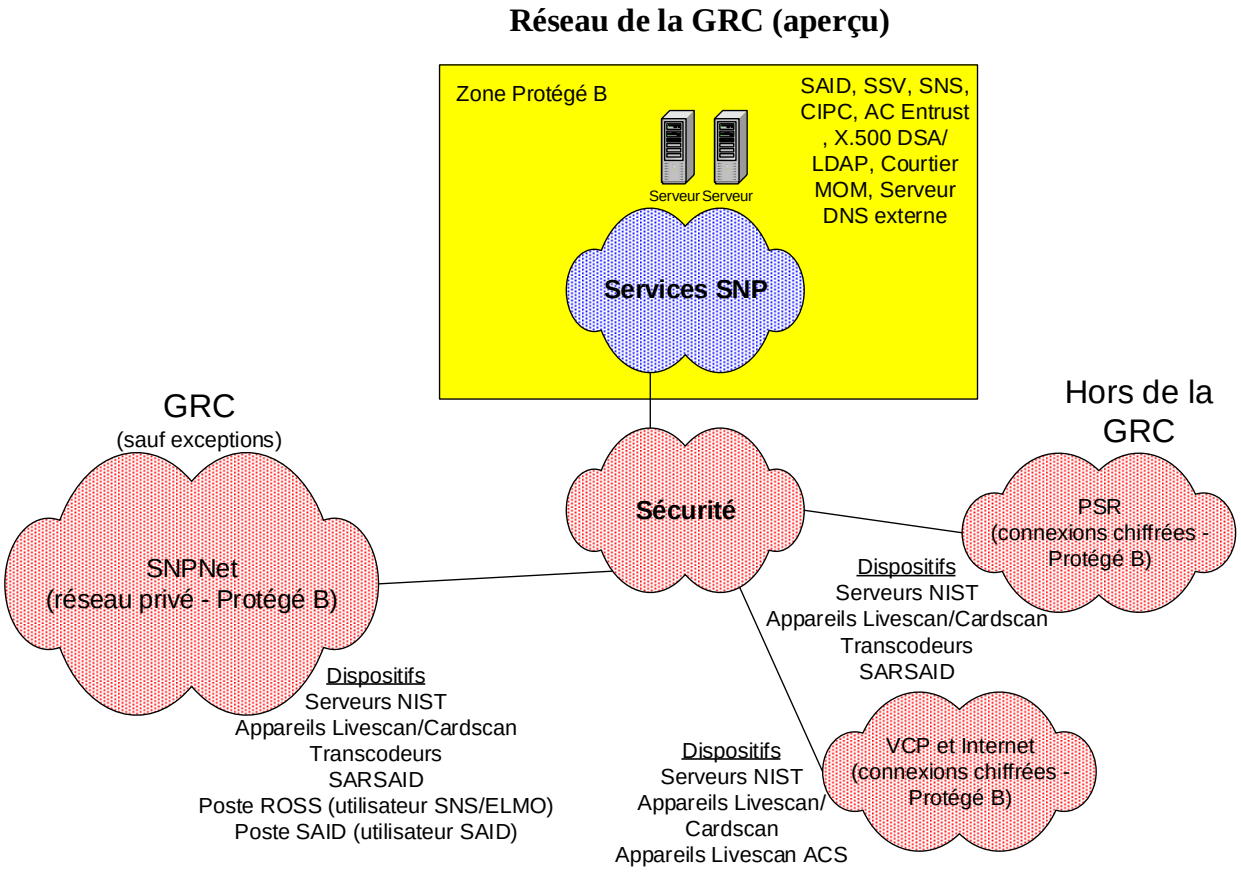

Figure 1 : Architecture conceptuelle du système d'ITR

2.2 SÉCURITÉ DE L'ITR DANS L'ARCHITECTURE DE LA GRC

2.2.1 CHIFFREMENT

1. Il est impératif de chiffrer toutes les données d'ITR hors de la zone de sécurité Protégé B, qu'elles soient transmises à un service contributeur ou un utilisateur SNS de l'ITR ou reçues de celui-ci.
2. Le SNPNet est un réseau privé MLPS Sécurisé destiné à la GRC et de SPC.
3. La PSR est une extension du réseau de GRC/SPC, ce qu'on appelle couramment un réseau local géré. À chaque site, des dispositifs RPV commandés et gérés par la GRC et SPC permettent à des sites hors de la GRC d'avoir accès par connexion sécurisée à des services comme l'ITR.
4. La VCP est un réseau sécurisé contrôlé et géré par le GC; il utilise les RPV. La GRC et SPC ont mis en place les connexions nécessaires pour les autres ministères et agences du gouvernement ayant besoin des services d'ITR.
5. Les agences du secteur privé ayant besoin des services d'ITR peuvent aussi établir par Internet des RPV permanents ou temporaires.

2.2.2 IDENTIFICATION ET AUTHENTIFICATION

1. Pour l'accès direct à l'ITR, un utilisateur doit utiliser une méthode d'authentification à deux facteurs, c'est-à-dire soit certificat (jeton ou carte à puce) et mot de passe, soit identification biométrique et mot de passe.
2. Comme les postes de travail du SAID sont déjà dans une zone Protégé B isolée, il n'est pas nécessaire de chiffrer les données transmises entre ces postes et les serveurs SAID/SSV. Le système SAID authentifie ses utilisateurs par deux facteurs : l'identification biométrique et un mot de passe. Seul le personnel local de la DG de la GRC a accès au SAID.
3. Les utilisateurs de la PSR, de la VCP ou d'Internet peuvent créer un RPV temporaire à l'aide d'un jeton ou d'une carte à puce (le 2^{e} facteur d'authentification) afin d'envoyer des transmissions d'ITR et recevoir les réponses du système par une interface SMTP/POP. Les utilisateurs des transcodeurs utilisent des RPV chiffrés permanents et établissent une connexion à l'aide de deux facteurs d'authentification (identification biométrique et mot de passe afin d'envoyer des transmissions d'ITR et recevoir les réponses du système par une interface SMTP. Ces utilisateurs ne peuvent communiquer avec l'ITR que par courriel, par un RPV sécurisé; ils n'ont aucun droit d'accès d'utilisateur à l'ITR, au SAID ou au SNS.

2.3 ÉQUILIBRAGE DES CHARGES ET TRADUCTION D'ADRESSES RÉSEAU

1. Par souci de sécurité, de rendement, d'extensibilité et d'équilibrage des charges, la GRC a mis en place une architecture de commutation des couches OSI 4 à 7 à l'aide de dispositifs réseau ACE; cette architecture prend aussi en charge la traduction des adresses réseau (NAT) et l'équilibrage des charges. Les demandes des services ou des applications peuvent ainsi être acheminées à un serveur virtuel puis aiguillées à plusieurs serveurs gérés par le système d'équilibrage des charges. À l'aide du protocole NAT, les adresses IP des serveurs matériels restent confidentielles, de façon parfaitement transparente pour l'utilisateur, car NAT « traduit » l'adresse IP indiquée dans la requête en l'adresse IP des serveurs matériels. Ensemble, ces services permettent d'envoyer les demandes à une adresse IP virtuelle, ce qui dissimule l'adresse IP réelle, et de créer un environnement échelonnable qui améliore considérablement le rendement. Ils permettent aussi d'aiguiller les demandes au serveur approprié, selon leur contenu. De plus, l'équilibrage des charges par le réseau met intrinsèquement en place des fonctions de basculement réseau intrasite et intersite. Les serveurs SAID/SSV transmettent leurs réponses à des serveurs virtuels. Ces critères sont incontournables, et devront être respectés par la solution de renouveau du SAID proposée par tout soumissionnaire dans le but de répondre aux exigences du présent EDT.

2.4 APERÇU DE L'ARCHITECTURE ACTUELLE DE L'ITR

1. L'organigramme suivant montre un aperçu des divers composants de l'architecture de l'ITR. On le présente ici pour montrer les liens entre l'architecture conceptuelle de GRC/SPC, les composants de l'ITR et les diagrammes de l'architecture du SAID qui seront présentés dans la section suivante.
2. Vous trouverez à l'appendice A, EDT pour le renouvellement du SAID, une courte description de chaque composant.

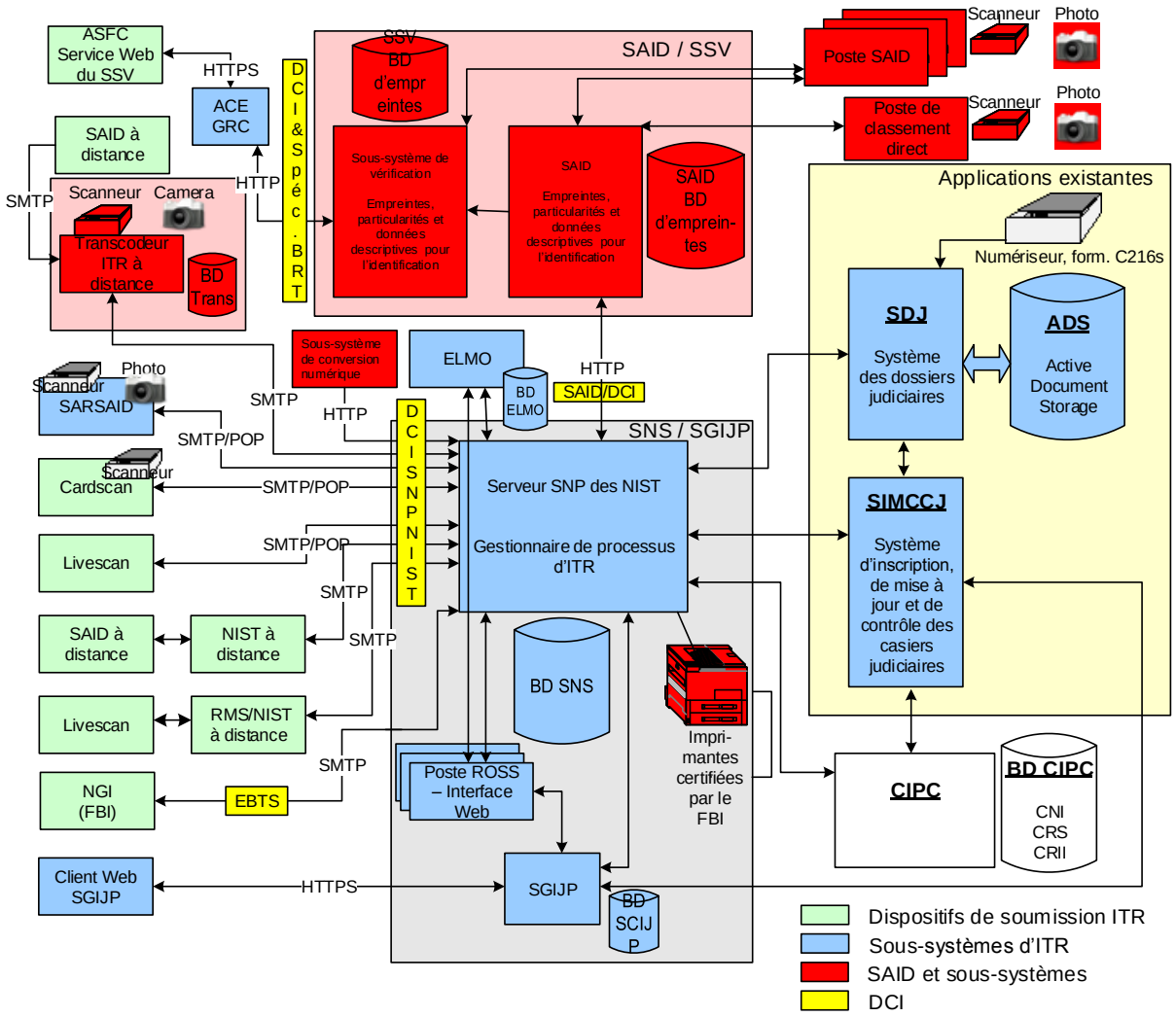

Figure 2 : Architecture conceptuelle actuelle de l'ITR

3. ARCHITECTURE DU SAID ET DU SSV

3.1 ARCHITECTURE CONCEPTUELLE DE LA BRT (SAID ET SSV)

1. Voici un aperçu de l'architecture conceptuelle du SAID et du SSV. Dans ce diagramme, les dactylogrammes enregistrés sont clairement transmis par CIC, mais cela s'effectue par l'interface d'ITR qu'utilisent tous les organismes contributeurs.
2. CIC enregistre les dactylogrammes de toute personne voulant entrer au Canada. CIC transmet des paquets NIST d'immigration (IMM) contenant les dactylogrammes et un code d'identification unique. Les dactylogrammes sont versés au SAID et une copie est transmise au SSV. À l'arrivée d'une personne à un point d'entrée, l'ASFC enregistre ses dactylogrammes et le numéro d'identification unique associé, puis transmet le paquet NIST de vérification (VER) au SSV, qui les compare avec les dactylogrammes enregistrés auparavant par CIC.
3. Toute transaction d'élimination (élimination d'un dossier d'immigration - IMP) transmise à CIC élimine aussi les dactylogrammes du SSV.

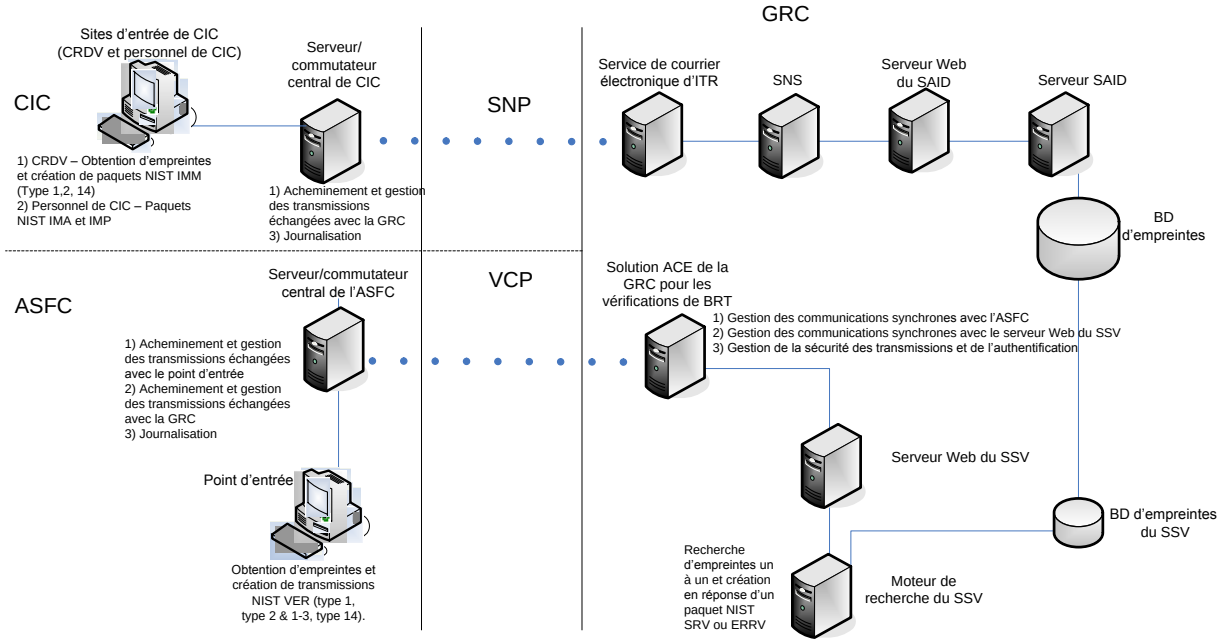

Figure 3 : Architecture conceptuelle de l'ITR, du SAID et du SSV de CIC et de la GRC

3.2 SAID ET SSV — ARCHITECTURE CONCEPTUELLE

1. Le diagramme suivant illustre l'architecture conceptuelle du SAID et du SSV et des divers éléments de l'ITR avec lesquels ils communiquent. L'ITR a été conçue en fonction des DCI, et permet d'ajouter ou de remplacer des composantes pour rester conforme avec la DCI.

2. Le SAID et le SSV peuvent fonctionner indépendamment, mais les enregistrements, éliminations ou mises à jour de dactylogrammes ne s'effectuent qu'à partir du SAID, et c'est le SAID qui transmet au SSV les enregistrements et éliminations des dactylogrammes et les mises à jour à ceux-ci. En d'autres termes, le SAID peut fonctionner sans le SSV, mais les mises à jour du SAID au SSV seront mises en attente jusqu'à la remise en service du SSV. Le SSV aussi peut fonctionner sans le SAID, mais il ne peut pas être mis à jour (enregistrements ou éliminations de dactylogrammes et mises à jour à ceux-ci) dans le SAID.

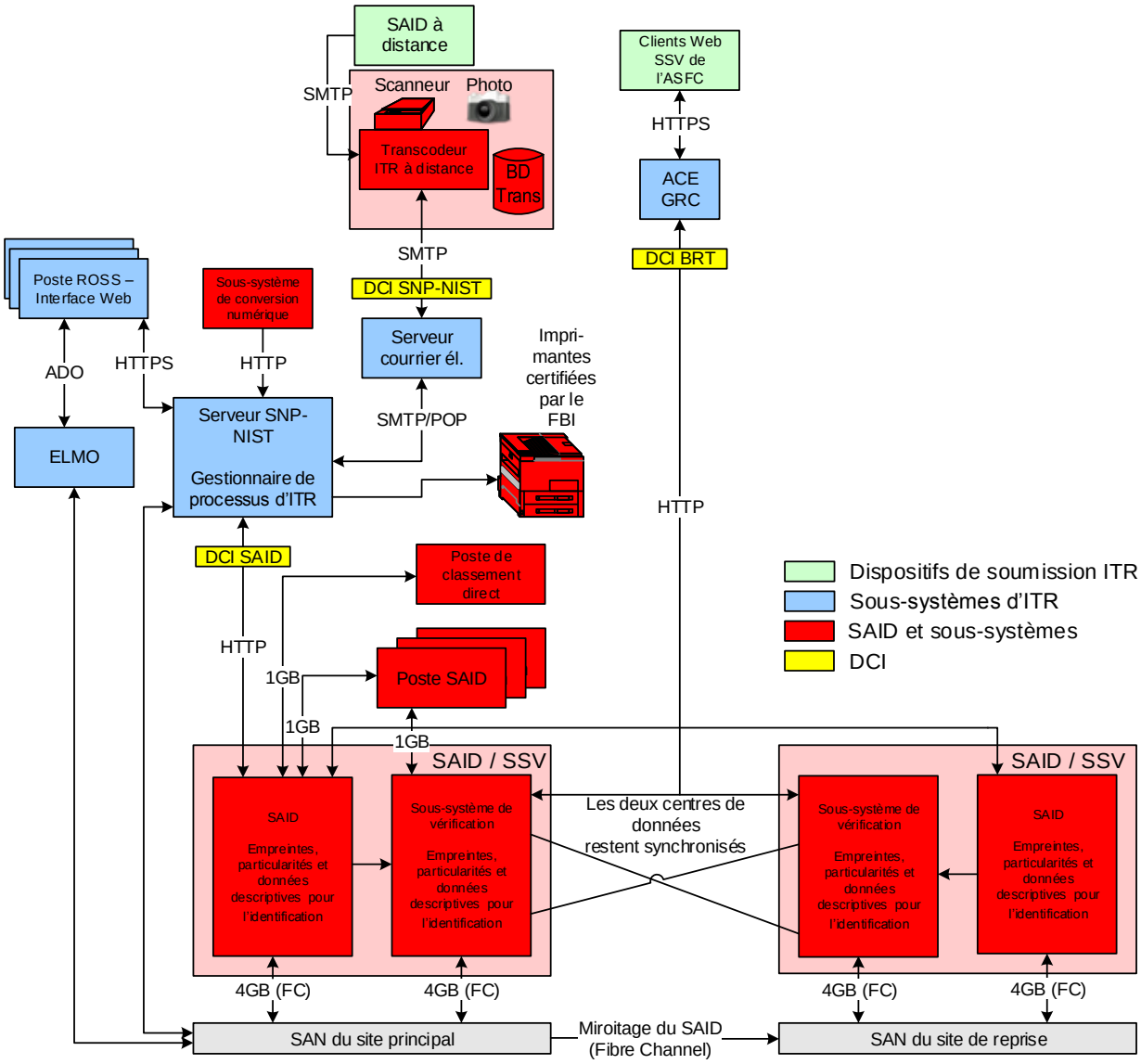

Figure 4 : Architecture conceptuelle actuelle du SAID et du SSV

3. Le SAID a été conçu comme une solution de reprise après sinistre en bascule semi-automatique. Les composantes du SAID sont en fonction tant au site principal qu'au site de reprise après sinistre. Toutes les bases de données et les fichiers système du SAID du site de reprise sont synchronisées avec celle du site principal (miroitage). En cas de sinistre, le SAID peut être redémarré à partir des composantes tenues à jour au site de reprise. Toute l'infrastructure réseau et de sécurité de GRC/SPC bascule automatiquement au site de reprise, ce qui permet aux composantes du SAID de communiquer avec les composantes accessibles de l'ITR. Les composantes de reprise du SAID se trouvent dans la même zone de sécurité que les composantes principales; l'architecture de sécurité est donc tenue à jour aux deux sites.

4. Le SSV est conçue selon un modèle de centre de données double à bascule automatique au site de reprise. Les composantes du SSV, au site principal et au site de reprise, sont conçus de façon à exploiter toutes les composantes de façon optimale et ainsi respecter les exigences opérationnelles. Comme l'illustre le diagramme conceptuel ci-dessus, le composant réseau ACE de GRC/SPC équilibre les charges également entre le site principal et le site de reprise. En cas de sinistre, le SSV fonctionne tous simplement à partir des composantes du site de reprise. Toute l'infrastructure réseau et de sécurité de GRC/SPC bascule automatiquement au site de reprise; les organismes contributeurs au SAID et au SSV dans l'environnement de production ne se rendent pas compte si le site principal est hors service. Que la panne touche le site principal ou de reprise, les sites se resynchronisent automatiquement dès que le site touché est remis en service, ce qui assure que les données des deux sites sont identiques. La resynchronisation démarre dès la remise en service et prend habituellement entre 5 et 10 minutes. Dans le modèle de centre de données dédoublé, les composantes du SSV fonctionnent dans la même zone de sécurité que le SAID.
5. Les postes du SAID sont branchés au serveur par un lien réseau de 1 Go.
6. Les serveurs du SAID et du SSV sont branchés au SAN par quatre liens réseau de 1 Go.
7. Les sites principal et de reprise sont liés par fibre optique.

3.3 ENVIRONNEMENTS D'ESSAI DU SAID ET DU SSV

3.3.1 GÉNÉRALITÉS

1. Les environnements d'essai de l'ITR comprennent le SAID, le SSV, le SNS et tous les autres éléments nécessaire pour faire l'essai de toute modification à l'ITR destinée à l'environnement de production.
2. Il existe trois environnements d'essai pour le SAID : DEVTEST, Quality Control Section (QCS) et MAINT. Chacun de ces environnements peut prendre en charge de multiples environnements ITR SNS.
3. Les environnements DEVTEST et MAINT du SAID prennent en charge de multiples environnements SNS. Cette configuration particulière est accessible dans tous les environnements d'essai, mais on ne l'utilise habituellement que dans les environnements DEVTEST et MAINT du SAID.
4. L'environnement DEVTEST du SAID prend en charge de nombreux environnements d'intégration SNS, environnements SYSTEST SNS, environnements de rendement SNS, et et environnements pour développeur individuel. Cette configuration spéciale permet à l'environnement DEVTEST du SAID de s'interfacer avec un environnement de développeur ou un environnement SNS. C'est là une caractéristique cruciale, car elle permet aux développeurs de communiquer avec l'environnement DEVTEST du SAID pour répondre à leurs besoins précis de développement ou d'essais, et ainsi de développer pius mettre à l'essai les modifications au SAID en parallèle avec la composante SNS de l'ITR.

5. L'environnement SYSTEST1 de l'ITR sert à mettre à l'essai toute modification à l'ITR destinée à l'environnement de production par le processus habituel de diffusion d'une nouvelle version. SYSTEST1 est l'environnement d'essai principal de toutes les composantes de l'ITR. Après des essais concluants dans l'environnement SYSTEST1, les modifications sont mises à l'essai dans l'environnement QCS de l'ITR.
6. L'environnement QCS du SAID ne prend en charge qu'un seul environnement SNS ITR. Il comprend tous les composantes du SAID qu'ont peut utiliser dans l'environnement de production. Avec les composantes SAID de l'environnement QCS, on peut mettre à l'essai tout problème de l'environnement de production. En d'autres termes, au moins une composante SAID de l'environnement QCS correspond à chaque composante unique de l'environnement de production; ainsi, on peut confirmer puis mettre à l'essai efficacement un correctif à tout problème possible survenant dans l'environnement de production.
7. L'environnement MAINT du SAID prend essentiellement en charge un environnement de maintenance et de certification du SNS, mais il peut en prendre d'autres en charge aussi.
8. L'environnement MAINT du SAID prend essentiellement en charge un environnement de maintenance et de certification du SNS, mais il peut aussi en prendre d'autres en charge. L'environnement de certification sert à certifier les systèmes des fournisseurs et de contributeurs par rapport au DCI NIST des SNP et au DCI de l'ITR. Par conséquent, la version logicielle du SNS de l'environnement de certification est identique à celle de l'environnement de production. L'environnement de certification du SNS est mis à jour deux semaines après la diffusion d'une nouvelle version du SNS dans l'environnement de production. L'environnement de maintenance du SNS a la même version du logiciel SNS jusqu'à une semaine avant la diffusion d'une nouvelle version de production.
9. Pour les nouvelles versions du SAID et du SSV, l'environnement MAINT du SAID sert à installer, configurer et mettre en œuvre les modifications et nouvelles versions du SAID et du SSV avant leur mise en place dans l'environnement DEVTEST du SAID. Ainsi, les modifications au SAID et au SSV sont mises à l'essai avec des versions stables du SNS. Deux semaines après une diffusion sans anicroche dans l'environnement de production, tout changement au SAID nécessaire pendant la mise à l'essai de la nouvelle version est déployé dans l'environnement MAINT du SAID.
10. Chaque environnement du SAID comprend les postes de travail et les transcodeurs nécessaires pour mettre à l'essai tout changement apporté. Les diagrammes suivants indiquent le nombre de postes de travail et de transcodeurs de chaque environnement.

3.3.2 ENVIRONNEMENT DEVTEST, SAID ET SSV

1. Le diagramme suivant illustre l'architecture de l'environnement DEVTEST du SAID.

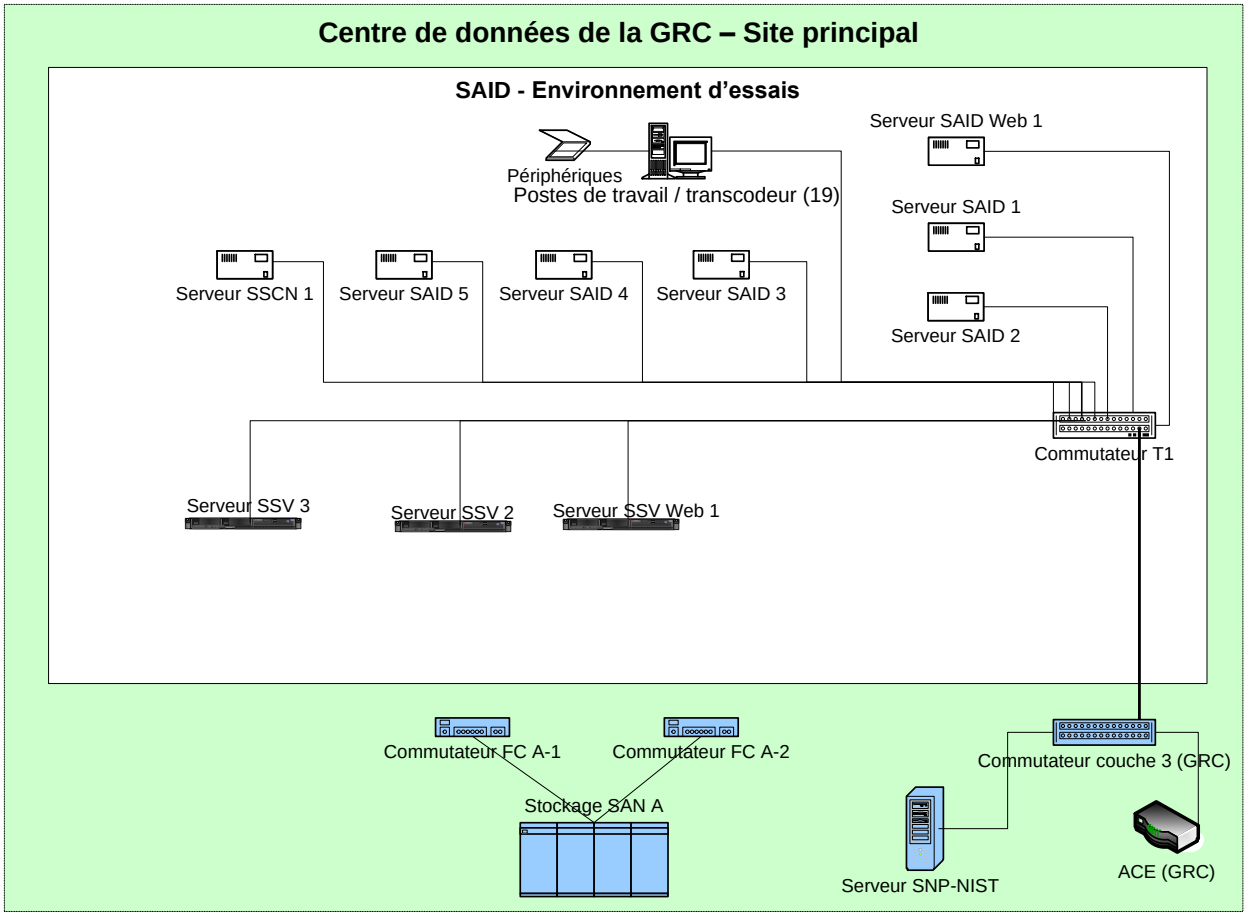

Figure 5 : Environnement de développement et d'essai

2. L'interface entre les systèmes SNS et SAID est mise en œuvre par le serveur Web du SNS et les serveurs Web du SAID.
3. Le système de commande des applications (ACE) de GRC/SPC assure une connexion sécurisée entre le SSV et l'ASFC ou la GRC. Le système ACE sert aussi à l'interface avec le serveur Web du SSV et, de concert avec celui-ci, il maintient une liaison synchrone qui transmet à l'ASFC les résultats des interrogations du SSV. CIC et l'ASFC font continuellement des essais dans les environnements d'essai de l'ITR. Il faut vérifier le bon fonctionnement de cette interface avec tout changement au système ou à l'ITR qui risque de les toucher. D'autres agences aussi font des essais dans les environnements d'essai de l'ITR. Tout accès d'une agence externe aux environnements d'essai est fait par l'une des connexions sécurisées décrites ci-dessus. Ces connexions d'essai sont configurées comme des interfaces de production contrôlées même si on y accède des environnements d'essai.
4. Vous trouverez plus de détails sur l'interface entre l'ASFC, le système ACE et les serveurs Web SSV des fournisseurs dans le document PDF sur les spécifications des interfaces de vérification (No SGDDI 39155) .

N.B. : Pour des raisons de confidentialité, nous n'identifions les serveurs dans ces diagrammes que par des noms génériques.

3.3.3 SAID ET SSV — ENVIRONNEMNET QUALITY CONTROL SECTION (QCS)

1. L'environnement QCS sert au contrôle de la qualité, c'est-à-dire confirmer la stabilité et la disponibilité opérationnelle de tout changement apporté aux systèmes avant leur mise en œuvre dans l'environnement de production. Les essais d'un changement ou d'une nouvelle version dans cet environnement doivent être réussis avant sa mise en œuvre dans l'environnement de production. L'environnement QCS est le seul où ont été mises en œuvre des configurations de haute disponibilité, et qui permet donc de mettre à l'essai les fonctions de redondance et de basculement.
2. Le diagramme suivant illustre l'architecture de l'environnement QCS.

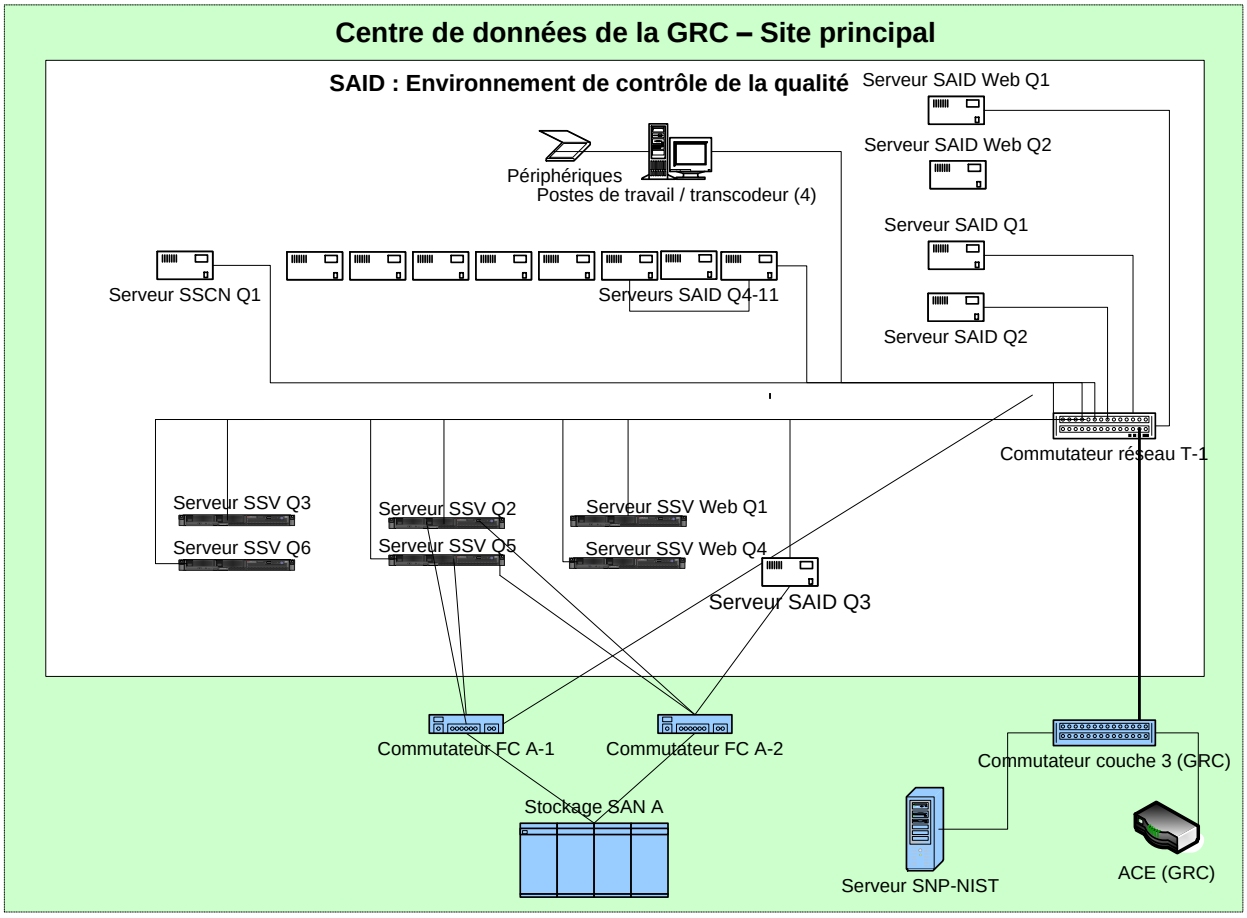

Figure 6 : Environnement de contrôle de la qualité

1. L'interface entre les systèmes SNS et SAID est mise en œuvre par le serveur Web du SAID.
2. Les deux serveurs Web SAID de l'environnement QCS permettent les essais automatisés de la haute disponibilité, c'est-à-dire le basculement automatique des services entre l'un et l'autre des serveurs Web.
3. Trois types éléments de vérification d'empreintes latentes (deux de chaque type) permettent la mise à l'essai de divers scénarios de traitement latent.

4. Les serveurs SSV sont configurés en deux nœuds (l'environnement de production en a quatre); on peut ainsi mettre à l'essai la haute disponibilité de plus d'un nœud, et donc faire réellement l'essai de la solution de production dans l'environnement QCS.
5. Dans l'environnement QCS, la connexion SSV n'est mise à l'essai qu'à l'aide d'un client interne qui simule une connexion avec l'ASFC. Le système ACE de GRC/SPC assure la connexion sécurisée entre le client interne et le SSV comme il le fait pour la connexion avec l'ASFC. Le système ACE sert aussi à l'interface avec le serveur Web SSV de l'environnement QCS, l'équilibrage des charges entre les deux serveurs Web SSV, et le maintien de la liaison synchrone qui transmet au client interne les résultats des interrogations du SSV.
6. Le système ACE de GRC/SPC assure aussi l'équilibrage des charges entre le SNS et le SAID et vice-versa ainsi qu'entre les composantes du SAID, ce qui crée dans l'infrastructure réseau de GRC/SPC une configuration haute disponibilité échelonnable.
7. Reste quelques scénarios où l'environnement QCS ne permet pas de faire l'essai des fonctions de haute disponibilité. Ils mettent en scène une composante qui répond à toutes les exigences d'un site ou un mécanisme propriétaire qui utilise pleinement les dispositifs sans avoir besoin de l'infrastructure d'équilibrage des charges ou de basculement. Le traitement des empreintes décadactylaires en est un exemple : comme un dispositif répond à tous les besoins d'un site, l'infrastructure d'équilibrage des charges est superflue. Le site de reprise comprend aussi un dispositif de traitement des empreintes décadactylaires, qu'un mécanisme propriétaire permet d'utiliser pleinement. L'infrastructure de basculement est vérifiée tous les ans; comme les essais de haute disponibilité du traitement des empreintes décadactylaires exigent, pour être concluants, le basculement de toute l'infrastructure de GRC/SPC, on n'en fait pas l'essai dans l'environnement QCS. En outre, la mise à l'essai du basculement de la grappe des serveurs SAID fonctionnels ne se fait que dans l'environnement de production. Comme les serveurs SAID fonctionnels du site de reprise ne sont utilisés qu'en cas de panne, on peut s'en servir pour la mise à l'essai de tout problème touchant la grappe sans perturber la production.

Remarque : La GRC/SPC effectue chaque année un basculement complet au site de reprise, afin de s'assurer que le réseau et toutes les applications du site de reprise fonctionnent bien. Ces essais annuels servent à vérifier le basculement de tous les systèmes du SAID et du SSV afin d'assurer que le site de reprise est pleinement fonctionnel. On peut ainsi s'assurer du bon fonctionnement de la haute disponibilité du SAID et du SSV, car l'environnement QCS ne permet pas la mise à l'essai des fonctions de basculement de l'infrastructure réseau de GRC/SPC et du site de reprise du SAID, y compris les données et fichiers système miroités par le SAN.

3.3.4 ENVIRONNEMENT DE MAINTENANCE, SAID ET SSV

1. Les environnements de maintenance et de certification du SNS comprennent les versions les plus récemment diffusées du SNS et de toutes les autres composantes (à l'exception du SAID); ils permettent de tester tout changement au SAID sur des logiciels identiques à ceux utilisés en production. Pour les nouvelles versions du SAID et du SSV, l'environnement de maintenance du SAID sert à installer, configurer et mettre en œuvre les modifications et nouvelles versions du SAID et du SSV avant leur mise en place dans l'environnement DEVTEST.

2. L'environnement de maintenance du SAID sert à vérifier si les modifications apportées par un entrepreneur fonctionnent comme prévu et à assurer que les composantes de l'entrepreneur communiquent toujours bien avec le SNS. Les essais d'une nouvelle version dans cet environnement doivent être réussis avant sa mise en œuvre dans l'environnement DEVTEST.
3. Le diagramme suivant illustre l'architecture de l'environnement de maintenance.

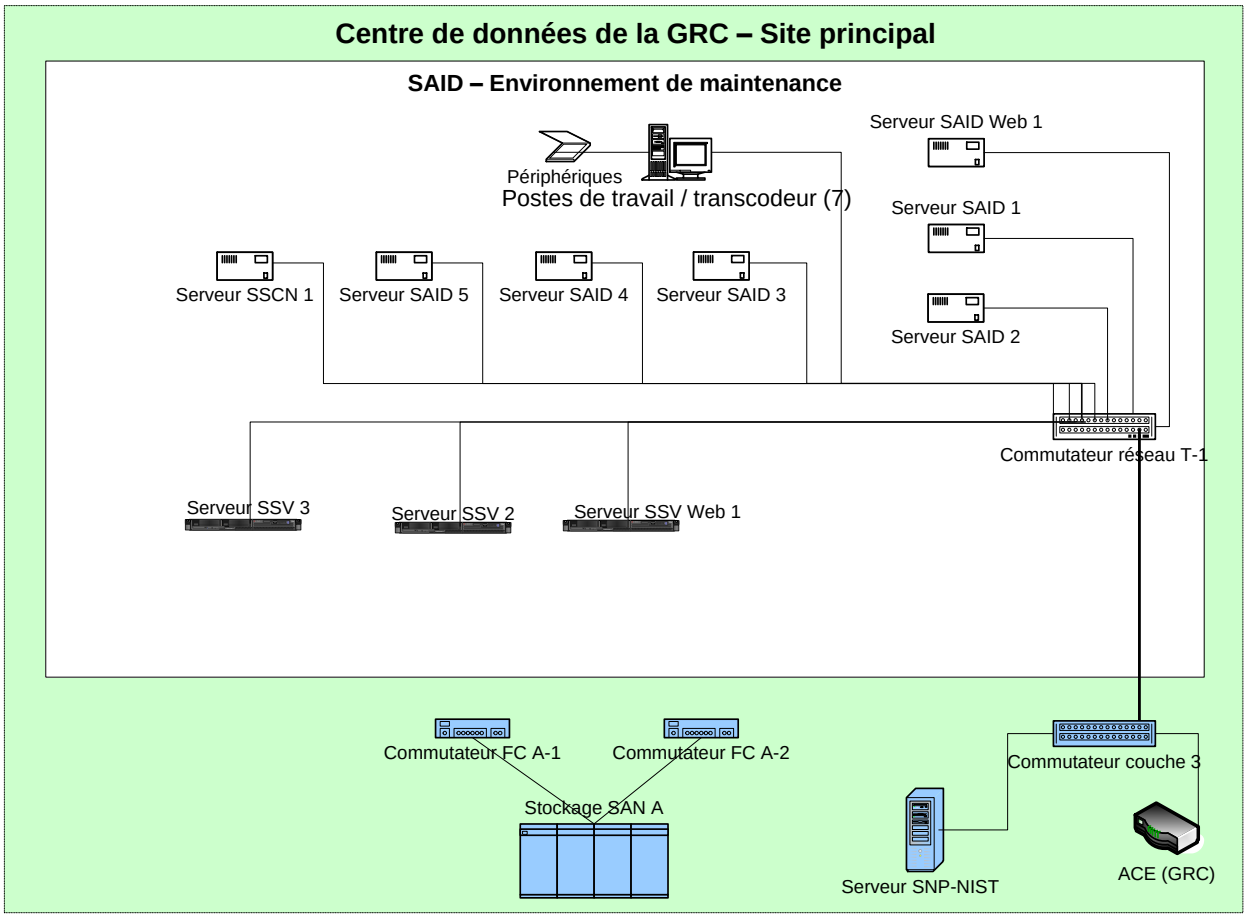

Figure 7 : Environnement de maintenance

4. L'interface entre les systèmes SNS et SAID est mise en œuvre par le serveur Web du SNS et les serveurs Web du SAID.
5. Le système de commande des applications (ACE) de GRC/SPC assure une connexion sécurisée entre le SSV et l'ASFC ou la GRC. Le système ACE sert aussi à l'interface avec le serveur Web du SSV, et il maintient une liaison synchrone qui transmet à l'ASFC les résultats des interrogations du SSV. CIC et l'ASFC peuvent, exceptionnellement, effectuer des essais dans l'environnement de maintenance, si l'environnement DEVTEST ne prend pas en charge les configurations nécessaires pour les essais.

3.4 SAID ET SSV — ENVIRONNEMENT DE PRODUCTION

3.4.1 GÉNÉRALITÉS

1. L'environnement de production du SAID et du SSV comprend un site de production et un site de reprise; l'un et l'autre prennent en charge toutes les fonctions de production des systèmes SAID et SSV de l'ITR. Le diagramme suivant illustre l'architecture des sites principal et de reprise.

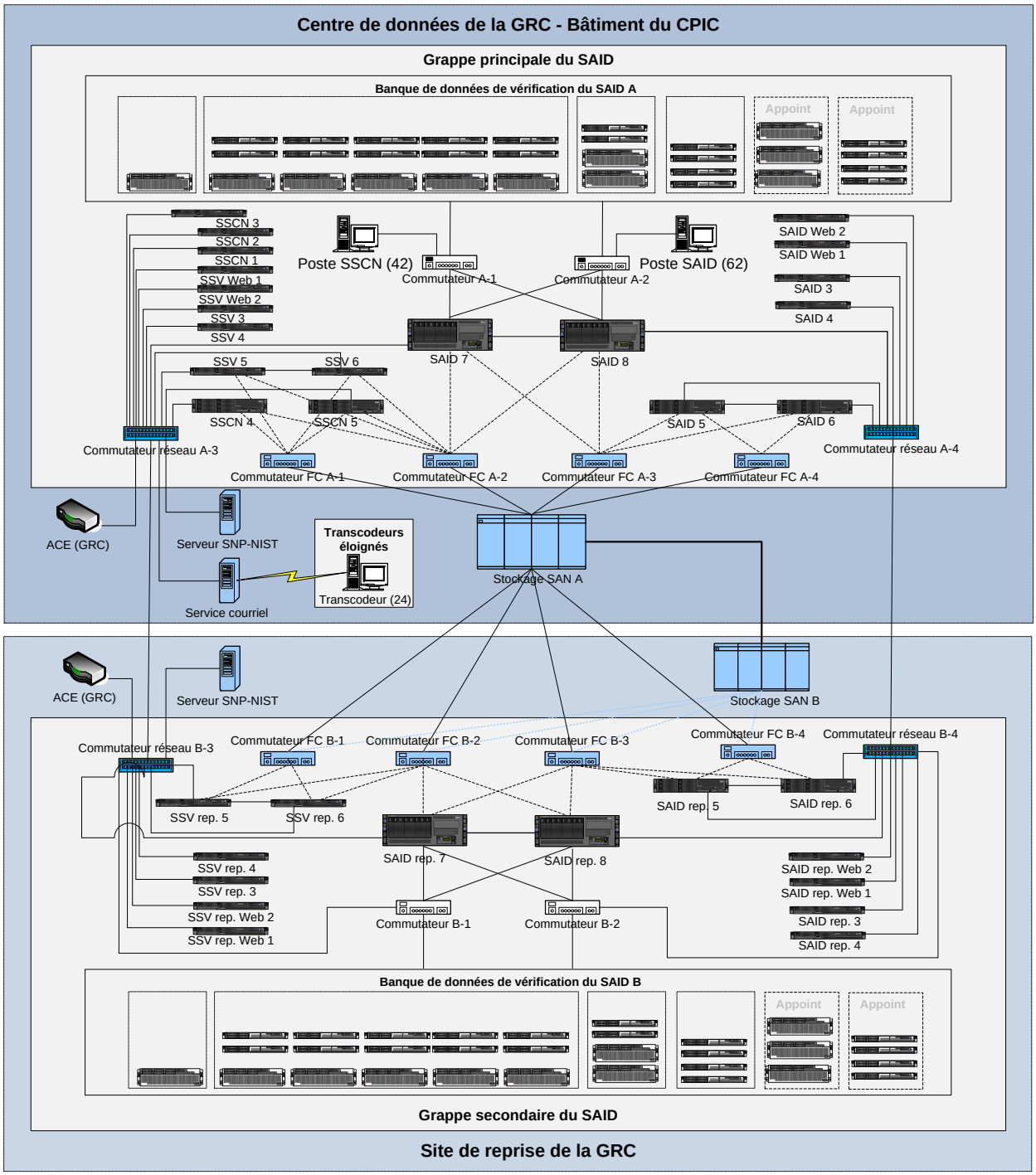

Figure 8 : Architecture de l'environnement de production

2. Toutes les composantes appariées des sites principal et de reprise du SAID sont utilisées à leur plein potentiel dans le cadre des activités courantes. L'architecture ainsi créée ressemble à un centre de données redondant où on exploite les composantes appariées des deux sites. Les serveurs SAID Web et fonctionnel du site de reprise ne sont utilisés que si le site principal tombe en panne et qu'il faut reprendre les activités au site de reprise à partir des données miroitées du SAN. En cas de panne du site principal, les serveurs SAID Web et fonctionnel du site de reprise n'utilisent que les données d'identification des empreintes du site de reprise.
3. Le SSV utilise une architecture de centre de données redondant totalement automatisée; tous les serveurs des sites principal et de reprise sont utilisés à leur plein potentiel, et la reprise d'une panne à l'un des sites n'exige aucune intervention humaine. La base de données intégrées est hébergée aux deux sites, ce qui permet à l'un et à l'autre de fonctionner tant de concert que de façon autonome en cas de panne. Les sites resynchronisent automatiquement la base de données intégrées dès que la panne est réglée.

3.4.2 SITE PRINCIPAL (DE PRODUCTION)

1. L'environnement de production sert à appuyer l'environnement opérationnel du SAID et du SSV. Les deux sites prennent en charge des configurations de haute disponibilité où les fonctions de basculement et la redondance de chaque site et entre les deux sites éliminent tout point unique de défaillance.
2. Le système ACE assure l'équilibrage de l'interface entre les systèmes SNS et SAID de l'ITR pour les serveurs Web du SAID ainsi que l'équilibrage de l'interface entre les systèmes SNS et SAID pour les serveurs Web du SNS.
3. Les deux serveurs Web du SAID au site principal prennent en charge la haute disponibilité. Les autres serveurs fonctionnels du SAID sont aussi configurés en paires afin de prendre en charge la haute disponibilité à chaque site.
4. De même, les serveurs fonctionnels du site principal exploitent aussi afin de prendre en charge la haute disponibilité toutes les composantes appariées des deux sites, sauf les composantes d'appoint en ligne.
5. Le système ACE de GRC/SPC assure une connexion sécurisée entre le SSV et l'ASFC ou la GRC. Le système ACE sert aussi à équilibrer l'interface avec les serveurs Web du SSV au site principal et de reprise, et il maintient une liaison synchrone qui transmet à l'ASFC les résultats des interrogations du SSV. Le SSV utilise une architecture de centre de données redondant totalement automatisée qui prend en charge la haute disponibilité à chaque site et entre ceux-ci.

3.4.3 SITE DE REPRISE

1. Le site de reprise est configuré de façon identique au site principal, à une exception près; il comprend tous les serveurs de celui-ci sauf le SSCN. Aussi, le site de reprise ne compte aucun poste de travail ni périphérique. Le cas échéant, il est simple de configurer poste de travail et périphériques pour qu'ils ne prennent en charge que le site de reprise.

3.5 INTÉGRATION PAR LE RÉSEAU DE GRC/SPC DES ENVIRONNEMENTS D'ESSAI ET DE PRODUCTION

3.5.1 GÉNÉRALITÉS

1. Les environnements de production et d'essai du SAID et du SSV sont intégrés aux fonctions de maintenance et de soutien technique de GRC/SPC. Cette intégration est crucial pour le bon fonctionnement du SAID et du SSV dans l'infrastructure de GRC/SPC. Les paragraphes suivants décrivent les fonctions prises en charge par l'infrastructure de GRC/SPC pour toutes les composantes des environnements d'essai et de production du SAID et du SSV.

3.5.2 SAUVEGARDE ET RESTAURATION

1. Le réseau de GRC/SPC comprend des fonctions de sauvegarde et de récupération complètes utilisées pour les bases de données et les fichiers système du SAID et du SSV, notamment Tivoli Storage Management (TSM) et le miroitage SAN.

3.5.3 RAPPORTS PAR SNMP

1. Tous les serveurs SAID et SSV prennent en charge les fonctions de rapports SNMP. Dans les environnements de production et QCS, on a activé sur les serveurs la surveillances des activités par la solution de surveillance des systèmes Spectrum/eHealth de GRC/SPC. Cette surveillance est aussi activée sur certains serveurs des environnements DEVTEST et MAINT; la surveillance de ces serveurs d'essai permet d'assurer un service ininterrompu dans ces deux environnements.
2. Parmi les rapports SNMP pris en charge, mentionnons la surveillance des systèmes, tant sur le plan matériel que les applications; ces fonctions émettent des messages ou alertes SMNP à la détection d'une défaillance logicielle ou matérielle. La surveillance SNMP couvre au minimum les aspects suivants : l'utilisation de la mémoire, du processeur et de l'espace disque, les défaillances de processus importants et les pannes matérielles.

3.5.4 BALAYAGE ANTIVIRUS (MCAFEE)

1. Sauf quelques rares exceptions, tous les serveurs et les postes de travail du SAID et du SSV, dans tous les environnements, participent à ePolicy Orchestrator, et reçoivent ainsi automatiquement les dernières signatures de maliciels McAfee du réseau de GRC/SPC. Pour les exceptions, les signatures sont mises à niveau manuellement d'une façon approuvée par la GRC; tout changement à ces systèmes est consigné dans un historique de gestion de la configuration. Cela vise quelques composantes spécialisées; les mises à niveau de signatures sont vérifiées dans l'environnement QCS avant de les appliquer dans l'environnement de production.

3.5.5 MISES À NIVEAU LOGICIELLES ET MATÉRIELLES

1. Les mises à niveau au SE Windows de tous les serveurs, postes de travail et transcodeurs de tous les environnements sont automatisées à l'aide du serveur WSUS (Windows Server Update Services) de GRC/SPC. Sur les postes de travail, les mises à niveau WSUS sont imposées après un délai préétabli si l'utilisateur ne les permet pas avant l'échéance du délai fixé. Les serveurs reçoivent automatiquement toute mise à niveau; le personnel de soutien du SAID et du SSV les appliquent à l'extérieur des heures normales de travail.

2. Sur les serveurs autres que Windows, GRC/SPC fournit les correctifs et mises à niveau approuvées pour le SE et les logiciels, avec lesquels on met à niveau ces serveurs SAID et SSV. Le personnel de soutien du SAID et du SSV les appliquent à l'extérieur des heures normales de travail.

3.5.6 PORTS SPÉCIALISÉS DÉSIGNÉS

1. Les serveurs SAID et SSV sont aussi configurés pour utiliser des ports préétablis pour divers types de connectivité, conformément aux politiques de GRC/SPC.

ANNEXE A-1 – LISTE DE DÉFINITIONS

La présente annexe vise à définir les termes utilisés dans le présent énoncé des besoins.

Tableau A-11 – Liste de définitions

Terme	Définition
DCI SAID	Description des transactions NIST utilisées pour communiquer avec le SAID. Cette norme d'interface permet à la GRC de rester indépendante du SAID, un système propriétaire, et de communiquer quand même toutes les données nécessaires pour l'interroger sur des empreintes.
ID de sujet SAID	Code d'identification unique attribué à un sujet (une personne) par le système SAID d'ITR, et qui permet d'associer à ce sujet toutes ses empreintes, quel que soit le type de fichier.
Journal de vérification	Liste d'événements système préétablis; la GRC doit savoir quand, où, pourquoi et par qui ces événements ont été déclenchés afin d'établir un historique de ces événements.
Certification automatique	Configuration du SAID d'ITR qui permet d'associer automatiquement des empreintes décadactylaires à un sujet déjà enregistré dans le SAID.
Données biographiques	Données numériques et alphanumériques intégrées à une transmission RT. Exemples : nom, date de naissance ou sexe.
Paramètre configurable	Paramètre pouvant être réglé par tout utilisateur disposant des droits d'accès voulus. Cela désigne souvent des fonctions définies par le système, comme une ENS ou un délai de rétention des fichiers.
Organisme contributeur	Agence autorisée à soumettre des demandes de service aux SCICTR, comme des transactions de casier judiciaire à conserver (CAR-Y), des demandes de renseignements sur un casier judiciaire (CAR-N), des demandes sur des civils (MAP), sur des réfugiés (REF) ou sur des résidents temporaires (IMM).
Demandes au CIPC	Dans le cadre de la BRT, les seules demandes au CIPC nécessaires sont des interrogations du FJN (fichier judiciaire nominatif). On peut exécuter cette transaction en même temps que le nettoyage hebdomadaire des données du CIPC.
Données dactylaires biométriques	Images d'empreintes dactylaires intégrées à une transmission RT.
Numéro d'IID (numéro de dossier d'immigration)	Code d'identification unique généré par la GRC servant à identifier chaque résident temporaire dans les dossiers internes de la GRC. • Un numéro d'IID n'est jamais réutilisé, même après l'élimination du dossier.

Tableau A-11 – Liste de définitions

Terme	Définition

Document de contrôle d'interface
(DCI)
	Description des méthodes de communication avec un sous-système, système ou service existant, interne ou externe.
	• Voici quelques-uns des DCI et autres documents connexes pertinents au projet BRT :
	  • DCI internes, comme DCI du SAID ou DCI SII;
	  • DCI externes, comme DCI NIST-SNP à l'intention des contributeurs externes;
	  • DCI de transformation et spécification de conversion du FBI.

DCI NIST des SNP	Le DCI NIST des services nationaux de police (SNP) désigne la version du DCI NIST des SNP externe qui intègre les transactions RT et les mises à jour aux transactions existantes destinées à être utilisées à l'appui du projet BRT. Voici les genres de transactions ajoutés : • Enregistrement d'un RT - IMM • Modification d'un dossier de RT - IMA • Élimination d'un dossier de RT - IMP • Vérification d'un RT - VER • Réponse d'élimination d'un dossier de RT - IMPR • Réponse de modification d'un dossier RT - IMAR • Résultats d'une recherche de vérification – SRV • Réponse à une transaction de vérification erronée – ERRV Les genres de transaction suivants seront modifiés pour prendre en charge le traitement des résidents temporaires : • Résultats d'une recherche – SRE • Demande d'image – IRQ • Réponse à une demande d'images – IRR • Accusé de réception d'empreintes décadactylaires – ACKT • Réponse à une transaction d'empreintes décadactylaires erronée – ERRT
Vérification un à un	Aux fins de vérification à un point d'entrée de l'ASFC, comparaison des empreintes dactylaires soumises aux empreintes correspondantes déjà enregistrées (identifiées par IID) du dossier de RT et et du dépôt de dossiers de RT.
IND	Indicateur de l'organisme d'origine (IND). Code alphanumérique de sept caractères servant à identifier l'organisme ayant envoyé une transaction à la GRC.

Tableau A-11 – Liste de définitions

Terme	Définition
Soumission	Demande de service envoyée par un organisme contributeur afin d'ajouter, de consulter, de modifier ou de vérifier des données du dépôt national des empreintes digitales de la GRC. Une soumission peut comporter plus d'une transaction; une transaction d'enregistrement, par exemple, peut consister en : • une demande IMM; • le cas échéant, une ERRT; • une ACKT; • une SRE,
Accessibilité du système	Capacité, évaluée par statistiques mensuelles, qu'a le système de recevoir et d'accuser réception d'une transmission de RT. Ne s'applique pas aux périphériques comme postes et travail et imprimantes.
Sujet	Personne identifiée dans une demande de visa, de permis d'étude ou de permis de travail de résident temporaire.
Dossier de RT	Données biographiques d'un résident temporaire créées et conservées dans la base de données biographiques des RT et les images d'empreintes dactylaires correspondantes du dépôt de dossiers de RT.
Dépôt de dossiers de RT	Données biométriques (empreintes dactylaires) de résident temporaire versées et conservées dans le SAID de la GRC.
Transaction de RT	Toute transaction visant un résident temporaire reçue par le système. Désigne sauf indication contraire les transactions d'enregistrement (IMM), de modification (IMA), d'élimination (IMP) et de vérification (VER) d'un dossier de résident temporaire.
Données de transaction de RT	Données sur un résident temporaire créées par le traitement d'une transaction de RT; par exemple, entrées du journal d'activités, historiques de l'état, transactions internes du SAID et d'autres sous-systèmes, etc.
Dépôt de vérification des RT	Données biométriques et particularités des empreintes dactylaires de résident temporaire versées et conservées dans le SAID de la GRC aux fins de vérification. Ces données comprennent ainsi les images d'empreintes et les données biographiques.
Transaction	Interaction définie d'une soumission, ou échange de données entre un système ou un sous-système.
empreintes d'identification plaquées, type 14	Format d'enregistrement normalisé du DCI NIST des SNP. L'enregistrement de type 14 sert à transmettre des empreintes dactylaires plaquées obtenues par un appareil d'enregistrement des empreintes, sans devoir rouler le doigt pour obtenir un empreinte complète. En anglais, on appelle parfois ces empreintes des « slaps ». La norme de la GRC visant les empreintes plaquées prescrit en 1 et 3 empreintes parmi les suivantes : • quatre doigts de la main droite; • quatre doigts de la main gauche; • les deux pouces.

Tableau A-11 – Liste de définitions

Terme	Définition
Utilisateur	Tout utilisateur autorisé des SCICTR ayant accès aux fonctions ou interfaces décrites dans le présent document.
Vérification d'empreinte	Comparaison entre les empreinte d'un candidat et les empreintes correspondantes enregistrées dans la base de données du SAID de la GRC.
Sous-système de vérification	Toutes les composantes nécessaires pour répondre aux exigences du sous-système de vérification.
En cours	Durée entre la réception de la demande et la fin du traitement, à laquelle on ajoute une période-tampon, c'est-à-dire un certain nombre de jours qui varie selon le type de soumission. Un enregistrement de RT, par exemple, peut être conservé pendant 30 jours après la fin du traitement avant d'être éliminé.
Données des travaux en cours	Données produites par le traitement d'une transmission RT, comme itérations d'une recherche de noms, résultats d'une recherche de noms, résultats d'une interrogation sur l'état d'un dossier, entrées au fichier journal des activités, etc.

ANNEXE A-2 – LISTE DES ACRONYMES

Tableau A-2 1 : Liste des acronymes

Acronyme	Définition
ACKT	Accusé-réception d'une transaction
SAID	Système automatisé d'identification dactyloscopique
ANSI	American National Standards Institute
ATP	Plan des tests d'acceptation du système
ATR	Rapport sur les tests d'acceptation du système
ASF	Agent des services frontaliers
ASFC	Agence des services frontaliers du Canada
SCICTR	Services canadiens d'identification criminelle en temps réel
LDEC	Liste des exigences prévues au contrat
CIC	Citoyenneté et Immigration Canada
DPI	Dirigeant principal de l’information
COG	Demande de changement d'un entrepreneur
CONOPS	Concept des opérations
COTS	Commercial sur étagère
CIPC	Centre d’information de la police canadienne
CSR	Rapport d’étape de l'entrepreneur
DPL	Description des produits livrables
DCN	Numéro de contrôle de document
EFCD	Dactyloscopieuse électronique
ERRIN	Erreur interne dans la transaction
ERRT	Erreurs de transaction
ERRV	Erreur dans une transaction de vérification
FBI	Federal Bureau of Investigation
DCI	Document de contrôle d’interface
No IID	Numéro de dossier d’immigration
ILRI	Récupération d'une liste d'images
IMA	Modification d'un dossier de RT
IMAR	Réponse à une modification d'un dossier de RT
IMM	Enregistrement d'un dossier de RT

Tableau A-2 1 : Liste des acronymes

Acronyme	Définition
IMP	Élimination d'un dossier de RT
IMPR	Réponse à une transaction d'élimination d'un dossier de RT
IRQ	Demande d'images dactylaires
IRR	Réponse à une demande d'images dactylaires
CPC	Calendrier principal du contrat
DCI NIST	DCI NIST des SNP externe
SNP	Services nationaux de police
NIST	National Institute of Standards and Technology
IND	Expéditeur
PMA	Programmable Matching Accelerator (optimisateur programmable des mises en correspondance)
POE	Point d'entrée
PRM	Réunion d'examen de l'état d'avancement des travaux
GRC	Gendarmerie royale du Canada
ITR	(système) d'identification en temps réel
SDD	Documentation sur la conception du système
SIP	plan d'installation
SIR	Rapport d'incident logiciel
SATP	Plan d'essai de réception sur place
SATR	Rapport d'essai de réception sur place
ENS	Entente sur les niveaux de service
EDT	Énoncé des travaux
SRE	Réponse à la recherche
SRV	Résultat de la recherche de vérification
STI	État de la transaction
TBD	À déterminer
TCN	Numéro de contrôle de transaction
TPAI	Modification d'empreintes décadactylaires
TPCNI	Regroupement d'empreintes décadactylaires
TPCNRI	Rapport de regroupement d'empreintes décadactylaires
TPDI	Élimination d'empreintes décadactylaires

Tableau A-2 1 : Liste des acronymes

Acronyme	Définition
TPQCI	Réponse au contrôle de la qualité d'empreintes décadactylaires
TPREI	Réponse à une demande d'empreintes décadactylaires
TPRI	Demande d'empreintes décadactylaires
RT	Résident temporaire
BRT	Biométrie pour les résidents temporaires
IU	Interface utilisateur
VER	Vérification d'un dossier de RT
WI	Activité; à la GRC, remplace SIR, mais on utilise parfois ce dernier.
En cours	Travail en cours