RCMP·GRC
ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

Services canadiens d'identification criminelle en temps réel

L'identification en temps réel pour les organismes

Date : 10-02-201
État : Final
Version : 17.0
Classification : Non classifié
Propriétaire : Solutions biométriques d'entreprise
SGDDI : 19085

REGISTRE DES MODIFICATIONS

Nº de version	Date	Commentaires
1.8 (finale)	25-10-2006	Mises à jour du rédacteur technique du CCC.
2.0 (ébauche)	09-07-2008	Mise à jour de l'avertissement (page 3). Ajout du texte actuel et mise à jour de la section 1. Mise à jour des sections 2 et 3 visant à refléter le processus de certification actuel.
2.1 (ébauche)	31-12-2008	Élimination des éléments relatifs aux essais de la section portant sur la certification des organismes.
2.2 (ébauche)	30-12-2010	Suppression des sections sur les bons de travail et les essais Télénet. Ajout des exigences mises à jour sur le profil de l'organisme. Remplacement du terme « gestionnaire des flux de travaux » par « système d'ITR ». Ajout de renseignements à la section 2.3, Considérations.
3.0 (ébauche)	24-01-2011	Suppression du formulaire de demande de certification des organismes (annexe A). Mise à jour de la page couverture en fonction des SCICTR. Mise à jour de la section « Origine et approbation du document » en fonction des SCICTR. Ajout d'une mise en garde relative aux ANS (section 1.10).

ORIGINE ET APPROBATION DU DOCUMENT

Approbations	Postes (Les signatures réelles se trouvent sur une liste de vérification officielle livrable.)
Accepté par	Directeur général des SCICTR
Accepté par	Officier responsable, Soutien opérationnel et Services à la clientèle des SCICTR
Accepté par	Officier responsable, Solutions biométriques d'entreprise des SCICTR
Centre stratégique	Soutien opérationnel et Services à la clientèle des SCICTR

AVERTISSEMENT

Le présent document vise à fournir aux organismes contributeurs un aperçu du processus de certification des organismes selon les normes du *National Institute of Standards and Technology* (NIST) des États-Unis et des Services nationaux de police (SNP) du Canada (certification NIST-SNP).

Bien que la Gendarmerie royale du Canada (GRC) fournisse aux organismes des lignes directrices visant à les préparer au processus d’ITR, elle n’offre aucune garantie quant à l’intégralité et à l’exactitude de cette documentation. Toutefois, l’utilisateur demeure en définitive responsable de l’adaptation des systèmes existants, de l’intégration des changements qui s’imposent et des résultats obtenus. La GRC, les Services des sciences judiciaires et de l’identité (SSJ&I) et les Services canadiens d’identification criminelle en temps réel (SCICTR) rejettent toute responsabilité et obligation, ainsi que les coûts, la perte d’efficacité ou toute autre perte financière, directe ou indirecte, découlant de tout usage fait par l’utilisateur de l’information présentée ici et de tout autre matériel du présent document.

La GRC n’offre aucune garantie, expresse ou implicite, et rejette en particulier toute garantie implicite de qualité marchande ou de valeur adaptative pour un usage précis. La GRC ne peut être tenue responsable de toute erreur ou omission qui a pu se produire au moment de la préparation des présentes lignes directrices et rejette expressément toute responsabilité, en vertu d’un contrat ou par négligence, envers un utilisateur direct ou tout autre emprunteur ou utilisateur, ou n’importe lequel de leurs clients.

En prenant possession du présent document, l’utilisateur accepte de s’abstenir d’en divulguer le contenu à une tierce partie sans avoir préalablement obtenu l’autorisation explicite écrite de la GRC. L ’utilisateur du présent document reconnaît et accepte le présent avis et exonère la GRC, les SSJ&I et les SCICTR de toute responsabilité.

TABLE DES MATIÈRES

1 INTRODUCTION

1.1 OBJECTIF

Le présent document vise à fournir aux organismes contributeurs un aperçu du projet d'identification en temps réel (ITR) et du processus de certification des organismes selon les normes du *National Institute of Standards and Technology* (NIST) des États-Unis et des Services nationaux de police (SNP) du Canada (certification NIST-SNP).

1.2 PORTÉE

Le présent document offre un aperçu du système d'ITR et des processus nécessaires à la certification des organismes contributeurs qui souhaitent transmettre au serveur NIST des SNP (le système d'ITR) des transactions électroniques conformes aux normes NIST-SNP.

1.3 DESTINATAIRES

Le présent document s'adresse aux catégories d'organismes contributeurs ci-dessous. Nota : Dans le présent document, tous les types d'organismes contributeurs sont désignés par les termes « organisme » ou « organismes », selon le contexte.

- Organismes d'application de la loi :
    - GRC; services de police provinciaux, municipaux et militaires qui traitent des empreintes digitales de criminels, de civils et de réfugiés; et organismes fédéraux ayant des pouvoirs d'exécution de la loi.
- Organismes du gouvernement fédéral :
    - Travaux publics et Services gouvernementaux Canada, Agence du revenu du Canada et autres organismes fédéraux qui traitent des empreintes digitales aux fins d'emploi au sein de la fonction publique fédérale.
- Entreprises privées :
    - Organisations du secteur privé accréditées à prendre des empreintes digitales à des fins civiles, etc.
- Personnel du Soutien opérationnel et des Services à la clientèle des Services canadiens d'identification criminelle en temps réel (SCICTR).

1.4 DOCUMENTS DE RÉFÉRENCE PERTINENTS

- *Version 1.7.7 du DCI NIST des SNP pour les collaborateurs externes* (dernière révision)
- *Lignes directrices relatives aux messages SMTP NIST : Document d'accompagnement de la version 1.7.7 du DCI NIST externe des SNP*
- *Best Practices for the Capture of Charge Information in Support of NPS-NIST-ICD 1.7.7. (Implementation and Use of the NPS-NIST Charge Table)*[1]
- *Pratiques exemplaires de mise en œuvre des flux de travaux pour les dispositifs de lecture électronique des empreintes digitales à des fins civiles*

[1] À l'intention des organismes d'application de la loi seulement.

- *Lignes directrices techniques sur l'ITR à l'intention des organismes*
- *Lignes directrices et politiques de sécurité s'appliquant aux organismes non policiers*
- *Glossaire de la phase 2 du projet d'ITR*

1.5 STRUCTURE DU DOCUMENT

- Section 1 – Aperçu du projet d'ITR et conditions préalables à la certification des organismes
- Section 2 – Aperçu du processus de certification NIST-SNP des organismes
- Section 3 – Description de chacune des étapes du processus de certification NIST-SNP des organismes
- Section 4 – Coordonnées des SCICTR
- Annexes du document

1.6 DOCUMENTATION DE RÉFÉRENCE SUR L'ITR À L'INTENTION DES ORGANISMES

L'ITR pour les organismes

- Ce document fournit un aperçu de l'ITR et du processus de certification NIST-SNP des organismes, en plus d'expliquer les conditions préalables à la certification et les exigences de mise à l'essai aux fins d'ITR.

Version 1.7.7 du DCI NIST des SNP pour les collaborateurs externes (dernière révision)

- Ce document décrit les types de renseignements que la GRC s'attend à envoyer et à recevoir électroniquement, ainsi que le format de ces renseignements. Les organismes contributeurs qui choisissent de se relier électroniquement au système d'ITR doivent utiliser des transactions respectant les normes énoncées dans ce document.

Lignes directrices relatives aux messages SMTP NIST : Document d'accompagnement de la version 1.7.7 du DCI NIST externe des SNP

- Ce document décrit l'interface du sous-système NIST de protocole de transfert de courrier simple (SMTP) des SNP. En plus de fournir un tableau logique des composants de cette interface, le document décrit les conventions actuellement utilisées aux fins d'échange de transactions.

Best Practices for the Capture of Charge Information in Support of NPS-NIST-ICD 1.7.7. (Implementation and Use of the NPS-NIST Charge Table)

- Ce document aide les fournisseurs et les organismes d'application de la loi à interpréter le tableau des accusations NIST-SNP et formule des recommandations sur la façon d'utiliser la structure de ce tableau des accusations de manière à faciliter la sélection d'accusations exactes et les processus d'entrée de données nécessaires pour remplir les champs d'information sur ces accusations.

Pratiques exemplaires de mise en œuvre des flux de travaux pour les dispositifs de lecture électronique des empreintes digitales à des fins civiles

- Ce document offre des directives aux fournisseurs et aux organismes qui souhaitent élaborer et mettre en œuvre des logiciels de lecture électronique des empreintes digitales à des fins civiles qui pourront lire les transmissions d'empreintes conformes aux normes NIST-SNP et soumettre électroniquement des paquets de données NIST au système d'ITR.

Lignes directrices techniques sur l'ITR à l'intention des organismes

- Ce document offre aux organismes un aperçu de l'infrastructure de communications et des options de connectivité entre leur réseau informatique et celui des Services nationaux de police (RSNP) aux fins des opérations d'ITR.

Lignes directrices et politiques de sécurité s'appliquant aux organismes non policiers[2]

- Ce document énonce les politiques de sécurité et les lignes directrices auxquelles doivent se conformer les organismes fédéraux et les entreprises privées de dactyloscopie qui souhaitent transmettre électroniquement des empreintes digitales au système d'ITR.

Glossaire de l'ITR

- Ce document présente les définitions des termes couramment utilisés et les abréviations qui s'appliquent au projet d'ITR et aux organismes contributeurs.

1.7 APERÇU DE L'ITR

L'ITR est un grand projet en deux phases de la Couronne qui a été conçu pour accroître l'efficience du dépôt national des empreintes digitales et des casiers judiciaires du Canada en remplaçant les processus papier et les systèmes existants par des flux de travaux et une automatisation remaniés. L'ITR utilisera des technologies modernes pour répondre aux exigences opérationnelles et pour garantir l'interopérabilité avec tous les clients. Les gains d'efficience découlant de l'ITR sont directement liés à la réduction des transmissions d'empreintes digitales sur papier au profit de transmissions électroniques.

Les services d'identification dactyloscopique et de casiers judiciaires sont offerts par les SCICTR à la collectivité des organismes d'application de la loi et de justice pénale du Canada, ainsi qu'à des partenaires internationaux tels que le Federal Bureau of Investigation (FBI) des États-Unis et Interpol.

1.8 PORTÉE DU PROJET

Les phases 1 et 2 du projet d'ITR visent des objectifs distincts.

Phase 1 :

- Mise en œuvre d'un nouveau système automatisé d'identification dactyloscopique (SAID)
- Établissement d'une nouvelle infrastructure de transmission électronique (serveur NIST des SNP)

[2] Les organismes d'application de la loi doivent consulter le chapitre 1.4 du *Manuel de référence* du Centre d'information de la police canadienne (CIPC).

- Automatisation des processus de vérification des empreintes digitales à des fins civiles
- Mise en application des normes NIST relatives aux transmissions électroniques des SNP (DCI NIST des SNP)

Phase 2 :

- Automatisation des processus relatifs aux casiers judiciaires.
- Refonte des éléments des flux de travaux relatifs aux casiers judiciaires.
- Élimination des systèmes existants.

1.9 PRESTATION DES SERVICES

Lorsque la mise en œuvre des deux phases du projet d'ITR sera terminée, les délais d'exécution de tâches qui prenaient plusieurs semaines, voire des mois, ne seront plus que de quelques heures ou jours. Les délais estimatifs de prestation des services des SCICTR sont indiqués dans le tableau ci-dessous.

DÉLAIS ESTIMATIFS DE PRESTATION DES SERVICES DES SCICTR

****Les accords de niveau de service (ANS) relatifs à la phase 2 du projet d'ITR sont tributaires de la mise en œuvre complète du système d'ITR et ne sont pas en vigueur à l'heure actuelle.*

Services	**Délais d'exécution**		
	2001	**Phase 1 du projet d'ITR**	**Phase 2 du projet d'ITR**
Recherches décadactylaires à des fins criminelles	10 semaines	2 heures	
Recherches d'empreintes latentes prélevées sur les lieux de crimes	5 mois	24 heures	
Recherches décadactylaires à des fins civiles (non liées à un casier judiciaire)	6 semaines	72 heures (3 jours ouvrables)	
Recherches décadactylaires à des fins civiles (liées à un casier judiciaire)	6 semaines		72 heures*** (3 jours ouvrables)
Mises à jour de casiers judiciaires	9 mois		24 heures***

2 APERÇU DU PROCESSUS DE CERTIFICATION DES ORGANISMES

2.1 PROCESSUS DE CERTIFICATION NIST-SNP DES ORGANISMES – CONDITIONS PRÉALABLES

Entre autres conditions préalables à la certification NIST-SNP, un organisme doit s'assurer que le fournisseur qu'il a choisi (p. ex. appareils électroniques et logiciels d'application) s'est soumis au processus de certification NIST-SNP des fournisseurs et qu'il a obtenu la certification connexe.

Le processus de certification NIST-SNP des fournisseurs permet de confirmer que les appareils d'un fournisseur produisent des images de qualité et sont conformes au *DCI NIST des SNP* (p. ex. étiquettes, valeurs, structures de caractères). Aux fins de ce processus, les logiciels d'application NIST-SNP du fournisseur sont mis à l'essai selon différents scénarios de transmission électronique qu'un organisme contributeur peut exécuter dans le cadre de ses activités. Les appareils du fournisseur doivent être en mesure de créer, puis d'envoyer des transactions conformes aux normes NIST-SNP dans différentes conditions d'exploitation, ainsi que de recevoir des réponses électroniques connexes. Les cas types d'essai se fondent sur les étiquettes, les valeurs et les structures de caractères définies dans la plus récente version du *DCI NIST des SNP pour les collaborateurs externes*.

En plus de répondre aux exigences de conformité aux normes NIST-SNP mentionnées précédemment, les appareils du fournisseur doivent :

- être inscrits à la liste des produits certifiés selon la norme IAFIS du FBI (site Web : https://www.fbibiospecs.org/IAFIS/Default.aspx).

Nota : Avant d'obtenir la certification NIST-SNP, l'organisme est tenu de fournir aux SCICTR des exemplaires des certificats et de tout autre document qui confirment que les appareils de son fournisseur sont conformes à la norme de qualité des images IAFIS du FBI.

2.2 CERTIFICATION DES ORGANISMES – APERÇU

Le processus de certification NIST-SNP des organismes vise à attester qu'un organisme est en mesure de soumettre des transmissions électroniques d'empreintes digitales conformes aux normes NIST-SNP par le truchement d'une infrastructure de communications sécurisée dans un environnement de production.

Le réseau et l'infrastructure de sécurité d'un organisme doivent être configurés avant que cet organisme puisse migrer vers l'environnement de production. Les divers types d'organismes – tels que les organismes d'application de la loi et les ministères fédéraux – disposent de différents types de réseaux et doivent se conformer à différentes exigences de sécurité en vue d'accéder au Réseau des Services nationaux de police (RSNP). La durée et l'intensité des efforts requis pour configurer la liaison d'intercommunication de chaque organisme dépendent de la nature de celui-ci.

2.3 CONSIDÉRATIONS

C'est à l'organisme qu'il incombe en définitive de soumettre au système d'ITR des transmissions électroniques d'empreintes digitales conformes aux normes NIST-SNP. Tel que mentionné précédemment, les organismes doivent envoyer leurs transmissions conformément à la plus récente version de la spécification *DCI NIST des SNP*. Dans certaines situations

toutefois, un organisme peut soumettre ses transactions électroniques par l’entremise d’un collaborateur autorisé. Entre autres exemples de telles situations, des services de police et des ministères fédéraux peuvent conclure des accords relatifs à la transmission électronique d’empreintes digitales au système d’ITR par le truchement d’une entreprise privée de dactyloscopie accréditée. Dans ces situations, l’organisme est responsable de toutes les données électroniques échangées avec l’entreprise qui se connecte directement au système d’ITR. On recommande toutefois que l’organisme informe ses collaborateurs des flux de travaux associés à l’échange électronique de données avec le système d’ITR.

Nota : Le processus de certification des fournisseurs ne vérifie pas la conformité à chacune des exigences de la spécification *DCI NIST des SNP* et des règles fonctionnelles connexes. L’organisme pourrait être tenu de mettre à jour son logiciel d’application et de se soumettre à des essais supplémentaires afin de vérifier sa conformité à la spécification *DCI NIST des SNP* ou à toutes nouvelles spécifications NIST-SNP fournies par la GRC. Dans l’éventualité où une mise à jour du logiciel d’application s’impose, on suppose que l’organisme en assumera lui-même les coûts et procédera à cette mise à jour avant la date fixée par la GRC, à défaut de quoi sa certification pourrait être suspendue et ultérieurement annulée. Si l’organisme souhaite faire certifier des appareils supplémentaires ou de nouveaux logiciels aux fins d’autres types de transactions et d’applications civiles additionnelles, son fournisseur devra se soumettre à des essais supplémentaires.

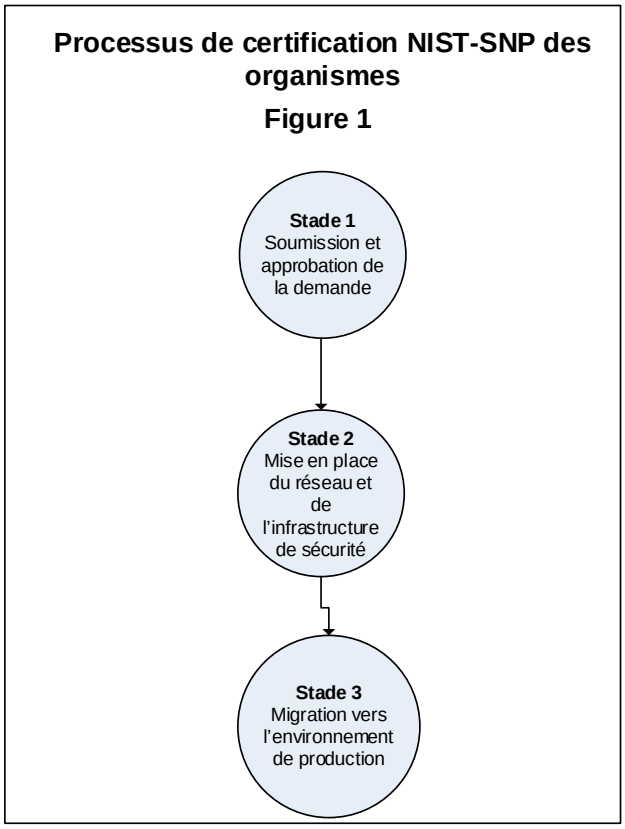
3 PROCESSUS DE CERTIFICATION NIST-SNP DES ORGANISMES

3.1 PROCESSUS DE CERTIFICATION DES ORGANISMES - FLUX DES TRAVAUX

Le processus de certification NIST-SNP des organismes comprend trois stades, dont chacun est constitué de plusieurs étapes. Ces stades sont les suivants :

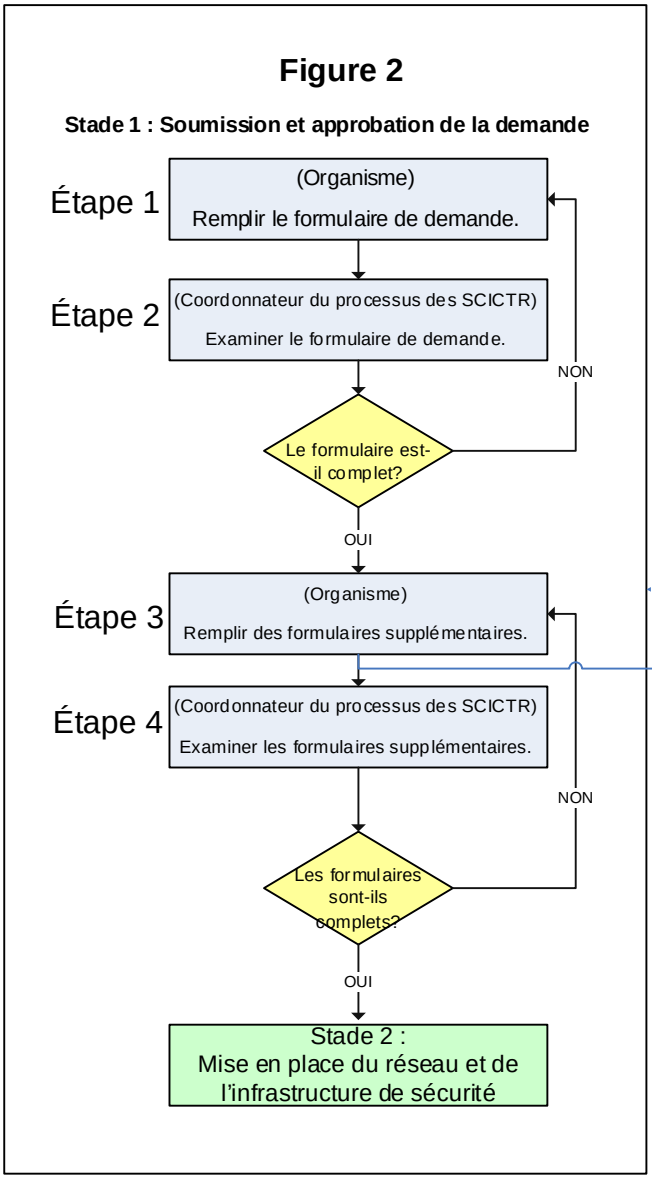
Stade 1	Soumission et approbation de la demande
Stade 2	Mise en place du réseau et de l'infrastructure de sécurité
Stade 3	Migration vers l'environnement de production

Figure 1 - Aperçu du processus de certification NIST-SNP des organismes



3.2 PROCESSUS DE CERTIFICATION DES ORGANISMES – ÉTAPES

Figure 2 - Aperçu du stade 1 – Soumission et approbation de la demande



Étape 1 Remplir le formulaire de demande

Effectué par : Organisme

Description : L'organisme doit remplir le formulaire de demande de certification NIST-SNP des organismes et le soumettre aux SCICTR, à l'adresse suivante : RTID_ITR_Certification@rcmp-grc.gc.ca.

Ce formulaire comprend des sections relatives aux coordonnées de l'organisme, aux renseignements sur le produit du fournisseur et aux types de transactions visées par la certification.

Nota : Les organismes peuvent obtenir un exemplaire électronique du formulaire de demande de certification NIST-SNP des organismes en communiquant avec les SCICTR, au RTID_ITR_Certification@rcmp-grc.gc.ca.

Étape 2 Examiner le formulaire de demande

Effectué par : Coordonnateur du processus des SCICTR

Description : Le coordonnateur du processus des SCICTR passe le formulaire en revue afin d'en vérifier l'exactitude et l'intégralité (p. ex. vérifier que la section relative aux caractéristiques techniques du produit du fournisseur a été remplie au complet, que le produit est conforme à la norme de qualité des images IAFIS du FBI, que les types de transactions ont été sélectionnés, etc.).

Si le formulaire n'est pas complet, le coordonnateur du processus des SCICTR le retournera à l'organisme et informera celui-ci des renseignements manquants qu'il doit fournir.

Une fois que le coordonnateur du processus des SCICTR a déterminé que le formulaire est complet, le processus de certification passe à l'étape 3.

Étape 3 Remplir des formulaires supplémentaires

Effectué par : Organisme

Description : Selon la nature de l'organisme, le coordonnateur du processus des SCICTR lui envoie des formulaires supplémentaires qu'il devra remplir afin d'obtenir la certification. Par exemple, les organismes de tous types doivent remplir un rapport sur l'infrastructure réseau de l'ITR à l'appui des exigences de sécurité et de connectivité associées à la configuration de leur liaison d'intercommunication aux fins d'exploitation.

Certains types d'organismes devront également remplir un rapport ITR de sécurité et d'inspection du sites, qui sert à vérifier les paramètres physiques des installations de réseau privé virtuel (RPV) de l'organisme.

Selon sa nature, l'organisme devra donc remplir les formulaires susmentionnés en vue d'obtenir la certification.

Nota : Pour obtenir les formulaires supplémentaires nécessaires, communiquer avec les SCICTR à l'adresse RTID_ITR_Certification@rcmp-grc.gc.ca.

Étape 4 Examiner les formulaires supplémentaires

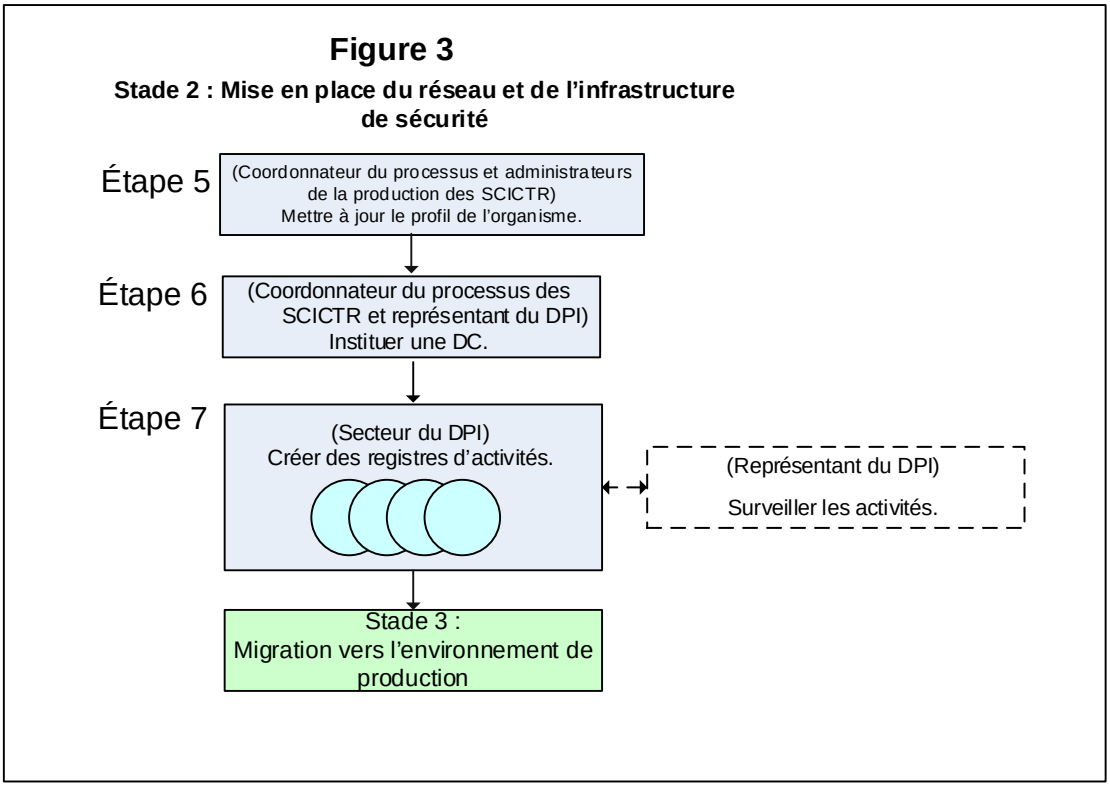
Effectué par : Coordonnateur du processus des SCICTR

Description : Le coordonnateur du processus des SCICTR passe les formulaires supplémentaires en revue afin d'en vérifier l'exactitude et l'intégralité. Selon les types de formulaires, le coordonnateur pourrait les transmettre à d'autres secteurs d'activité, aux fins d'évaluation.

Si les formulaires ne sont pas complets, le coordonnateur du processus des SCICTR les retournera à l'organisme et informera celui-ci des renseignements manquants qu'il doit fournir.

Une fois que le coordonnateur du processus des SCICTR a déterminé que les formulaires sont complets, le processus de certification passe au **stade 2 – Mise en place du réseau et de l'infrastructure de sécurité**.

Figure 3 - Aperçu du stade 2 – Mise en place du réseau et de l'infrastructure de sécurité



Étape 5 Mettre à jour le profil de l'organisme

Effectué par : Coordonnateur du processus des SCICTR
Administrateurs de la production des SCICTR

Description : Le coordonnateur du processus des SCICTR informe les administrateurs de la production des SCICTR des exigences de certification relatives au profil de l'organisme. Ces derniers doivent procéder aux mises à jour qui s'imposent. Le profil de l'organisme doit être configuré en fonction des exigences opérationnelles de l'organisme, puis versé aux applications nécessaires (p. ex. pupitre de commande du serveur NIST des SNP (SNS), sous-système de conversion des processus papier).

Ce profil sert à valider les transmissions qu'un organisme envoie par rapport aux autorisations de transmission accordées à cet organisme. Cette validation se fonde sur l'identificateur unique (IND) attribué à chaque organisme.

Étape 6 Instituer une DC

Effectué par : Coordonnateur du processus des SCICTR
Représentant du Secteur du DPI

Description : Une demande de changement (DC) est nécessaire pour configurer l'infrastructure réseau sécurisée de l'organisme aux fins d'exploitation.

Selon les renseignements fournis dans le rapport sur l'infrastructure réseau de l'ITR (voir l'étape 3), le coordonnateur du processus des SCICTR transmet à l'organisme les exigences réseau à respecter en vue de configurer la liaison d'intercommunication avec l'environnement de production. Le représentant du DPI institue ensuite une DC.

La DC décrit les changements qui devront être apportés aux secteurs d'activité et à la configuration technique du réseau de l'organisme afin d'établir une liaison d'intercommunication avec le RSNP.

Une fois la DC terminée, le représentant du DPI en informe le coordonnateur du processus des SCICTR et assure directement le suivi de tout domaine de responsabilité dont les exigences ne sont pas encore totalement respectées.

Nota : Les efforts nécessaires à la configuration de l'infrastructure réseau de l'organisme dépendent de la nature de celui-ci. Par exemple, une entreprise privée peut configurer son RPV au moyen d'un certificat pour périphérique d'Entrust de la GRC de manière à se connecter au RSNP par le truchement d'une connexion Internet sécurisée. De même, un ministère fédéral peut activer son RPV au moyen d'un certificat pour périphérique cocertifié et se connecter au RSNP par le truchement d'un tunnel partagé qui emprunte le Réseau de la Voie de communication protégée (RVCP) du gouvernement[3]. Dans le cas d'un organisme d'application de la loi, il pourrait être nécessaire de reconfigurer sa connexion actuelle au RSNP.

Étape 7 Créer des registres d'activités

Effectué par : Sections du Secteur du DPI

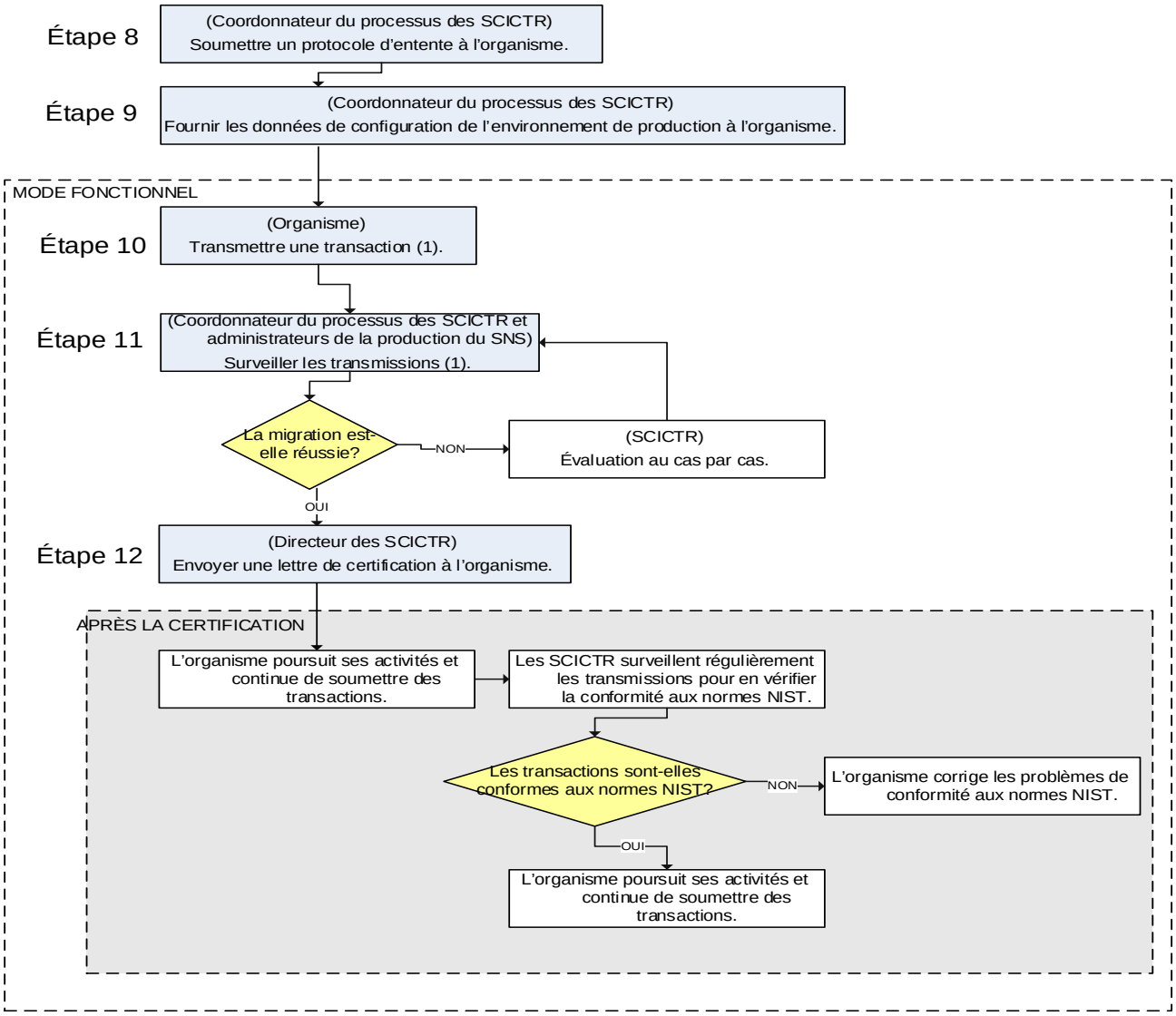
Description : Les différentes sections du Secteur du DPI (p. ex. Section des services de réseau de la Région du Centre (SSRRC); groupe de la technologie des réseaux et de la recherche-développement; Réseau RVP; Pare-feu de réseau; Services informatiques organisationnels (SIO); Opérations) établissent des registres d'activités et effectuent les travaux nécessaires pour établir une connexion sécurisée entre le réseau de l'organisme et le RSNP.

[3] Les organismes devraient consulter le document *Lignes directrices techniques sur l'ITR à l'intention des organismes* pour en apprendre davantage à propos des options de connectivité.

Nota : Les sections participantes du Secteur du DPI, les détails des travaux et l'échéancier d'achèvement des registres d'activités varient en fonction de la nature de l'organisme et de la méthode de connexion.

Figure 4

Stade 3 Migration vers l'environnement de production



Étape 8 Soumettre un protocole d'entente à l'organisme (à déterminer)

Effectué par : Soutien opérationnel et Services à la clientèle des SCICTR

Description : Le personnel du Soutien opérationnel et des Services à la clientèle des SCICTR enverra à l'organisme un protocole d'entente qui définit les conditions de participation continue que l'organisme et la GRC devront respecter. Afin de maintenir sa participation au système d'ITR, l'organisme doit s'acquitter des obligations établies dans le protocole d'entente.

Nota : La GRC et l'organisme doivent faire en sorte que le protocole d'entente entre en vigueur avant que l'organisme passe en mode fonctionnel. La GRC peut, à sa discrétion, autoriser l'organisme à passer en mode fonctionnel avant la signature du protocole d'entente, à condition que l'organisme travaille activement à la mise en vigueur du protocole d'entente.

Nota : Le personnel du Soutien opérationnel et des Services à la clientèle des SCICTR élabore actuellement un manuel de référence qui décrira toutes les exigences d'accès auxquelles devront se conformer les organismes qui se connectent au système d'ITR. À terme, ce manuel de référence appuiera la conclusion de protocoles d'entente entre les organismes et la GRC.

Étape 9 Fournir les données de configuration de l'environnement de production à l'organisme

Effectué par : Coordonnateur du processus des SCICTR

Description : Le coordonnateur du processus des SCICTR envoie à l'organisme les données de configuration dont il aura besoin afin d'établir une interface avec l'environnement de production. Ces données de configuration comprennent un indicatif de service émetteur (IND) que l'organisme doit fournir à chaque transmission (étiquette 1.008), ainsi que l'adresse de courriel qu'il doit utiliser dans le cadre des activités. Le protocole Internet (IP) à suivre sera fourni par la Section des services de réseau de la Région du Centre.

Étape 10 Transmettre une transaction (1)

Effectué par : Organisme

Description : L'organisme effectue sa première transmission électronique d'empreintes digitales à l'environnement de production. À l'origine, l'organisme ne transmettra qu'une seule transaction de manière à s'assurer que sa migration à l'environnement de production a été correctement effectuée.

Étape 11 Surveiller les transmissions (1)

Effectué par : Coordonnateur du processus des SCICTR
Administrateurs de la production du SNS

Description : Le coordonnateur du processus des SCICTR et les administrateurs de la production du SNS surveillent la première transmission électronique de

l’organisme de manière à s’assurer que sa migration à l’environnement de production a été correctement effectuée.

Si cette migration a été réussie, l’organisme pourra continuer à transmettre des transactions conformes aux normes NIST des SNP. Tout éventuel problème relatif à la migration sera évalué au cas par cas.

Nota : Conformément au protocole d’entente, les transmissions électroniques de l’organisme seront surveillées, validées et vérifiées de façon continue afin d’en confirmer la conformité aux normes NIST des SNP.

4 COORDONNÉES

Services canadiens d'identification criminelle en temps réel (SCICTR)

Courriel : RTID_ITR_Certification@rcmp-grc.gc.ca

Tél. : 613-990-8709 (coordonnateur du processus des SCICTR)

Fax : 613-993-4244

Adresse : Directeur général
Services canadiens d'identification criminelle en temps réel
GRC, Pavillon des SNP
1200, promenade Vanier
Ottawa (Ontario)
K1A 0R2