Livraison de systèmes et gestion de portefeuilles de projets (LSGPP)

DOC RELATIVE À LA DACTYLOSCOPIEUSE ÉLECTRONIQUE

ANNEXE A DE L'APPENDICE A : ARCHITECTURE ACTUELLE

Dernière mise à jour :	2020-03-11
État :	Ébauche finale
Version :	1.0
Nº SGDDI du document :	45383V2a

TABLE DES MATIÈRES

© (2016) SA MAJESTÉ LA REINE DU CHEF DU CANADA, représentée par la Gendarmerie royale du Canada (GRC).

FIGURES

© (2016) SA MAJESTÉ LA REINE DU CHEF DU CANADA, représentée par la Gendarmerie royale du Canada (GRC).

1. INTRODUCTION

1.1 But du document

1. Le présent document a pour but de décrire l'architecture actuelle de la GRC/du GC/des agences provinciales et municipales canadiennes (APMC) dans laquelle fonctionnent les dactyloscopieuses électroniques/serveurs SMTP-PAU/SGD/SPS. Les dactyloscopieuses électroniques et les serveurs SMTP-PAU doivent fonctionner efficacement dans cette architecture de la GRC/du GC/des APMC, et satisfaire à toutes les exigences énoncées dans le présent EDT.

2. Ce document donne une brève description de haut niveau de l'architecture de la GRC/du GC/des APMC, ainsi qu'une description plus précise de l'architecture de la GRC/du GC/des APMC architecture liée aux dactyloscopieuses électroniques/appareils SMTP/PAU.

1.2 Renseignements généraux

1. La GRC joue un rôle primordial dans la collecte, le stockage et la gestion de renseignements policiers. Le Réseau des Services nationaux de police (RSNP) fournit aux organismes canadiens d'application de la loi le moyen d'accéder électroniquement à ces renseignements centralisés. Le RSNP appuie également des applications internes de la GRC. De plus, le RSNP assure un soutien réseau national à la GRC et à ses partenaires affinitaires par l'entremise d'un réseau dédié privé. Le RSNP donne des services de réseau pour le transport d'information électronique à l'appui des services opérationnels et administratifs utilisés par les organismes clients. Il sert quelque 60 000 utilisateurs à environ 1200 endroits du Canada et dans le Haut Arctique.

2. Par ailleurs, le RSNP assure la connectivité aux services policiers nationaux, aux forces policières internationales, à des organismes fédéraux, provinciaux et municipaux canadiens, et à des agences privées qui ont besoin des capacités de l'ITR. Toute connectivité des agences à l'ITR se fait par l'une des méthodes ci-dessous qui seront décrites dans l'ensemble de ce document :

    a. RPV sécurisé contrôlé et géré par Services partagés Canada (SPC), que l'on appelle la posture de sécurité de nationale (PSN);

    b. RPV sécurisé par l'entremise du Réseau de la Voie de communication protégée (VCP) du GC;

    c. RPV sécurisé par l'entremise du Nuage du GC;

    d. RPV sécurisé par l'entremise d'Internet.

1.3 Organisation du document

1. Ce document contient une brève description de haut niveau de l'architecture de la GRC/du GC/des APMC dans laquelle les dactyloscopieuses électroniques et les serveurs SMTP-PAU doivent fonctionner.

2. Après cette architecture de haut niveau, on trouve une description de la connectivité que doivent prendre en charge les dactyloscopieuses électroniques et les serveurs SMTP-PAU.

2. ARCHITECTURE DE HAUT NIVEAU DE LA GRC/DU GC/DES APMC

2.1 Architecture de sécurité conceptuelle de la GRC/du GC/des APMC

1. La Figure 2-1 montre une vue conceptuelle de l'architecture de sécurité de la GRC/de SPC dans laquelle doivent fonctionner les dactyloscopieuses électroniques/appareils SMTP-PAU.

2. Certains ministères/certaines divisions du GC/des APMC possèdent des réseaux privés semblables au RSNP de la GRC, et bon nombre de ministères/organismes GC/des APMC ont accès à la VCP/Nuage du GC. Les dactyloscopieuses électroniques/appareils SMTP-PAU doivent fonctionner dans ces réseaux privés de la GRC/du GC/des APMC et la VCP/le Nuage du GC.

3. Les dactyloscopieuses électroniques/appareils SMTP-PAU doivent pouvoir répondre à toutes les exigences de l'ÉB et des documents connexes pour communiquer dans ces différents réseaux privés ou par Internet avec les serveurs NIST dans un ministère/organisme ou avec l'ITR.

4. Le diagramme illustre le réseau privé et dédié RSNP de la GRC, ainsi que la connectivité avec la PSN et la VCP/le Nuage du GC/Internet par RPV pour les agences externes.

5. Remarque : Certains sites subissent une migration d'une connexion RPV à une Commutation multiprotocole par étiquette (MPLS) sécurisée. Cependant, ceci n'a aucun impact sur l'ITR ou sur les dactyloscopieuses électroniques/appareils SMTP-PAU. Il ne s'agit que d'une méthode différente d'établissement d'une connexion chiffrée sécurisée.

6. Le diagramme illustre les dactyloscopieuses électroniques/appareils SMTP-PAU applicables qui sont utilisés dans les différents types de connectivité.

7. De plus, le diagramme illustre une vue conceptuelle des composantes de l'ITR situées dans l'architecture de la GRC/de SPC.

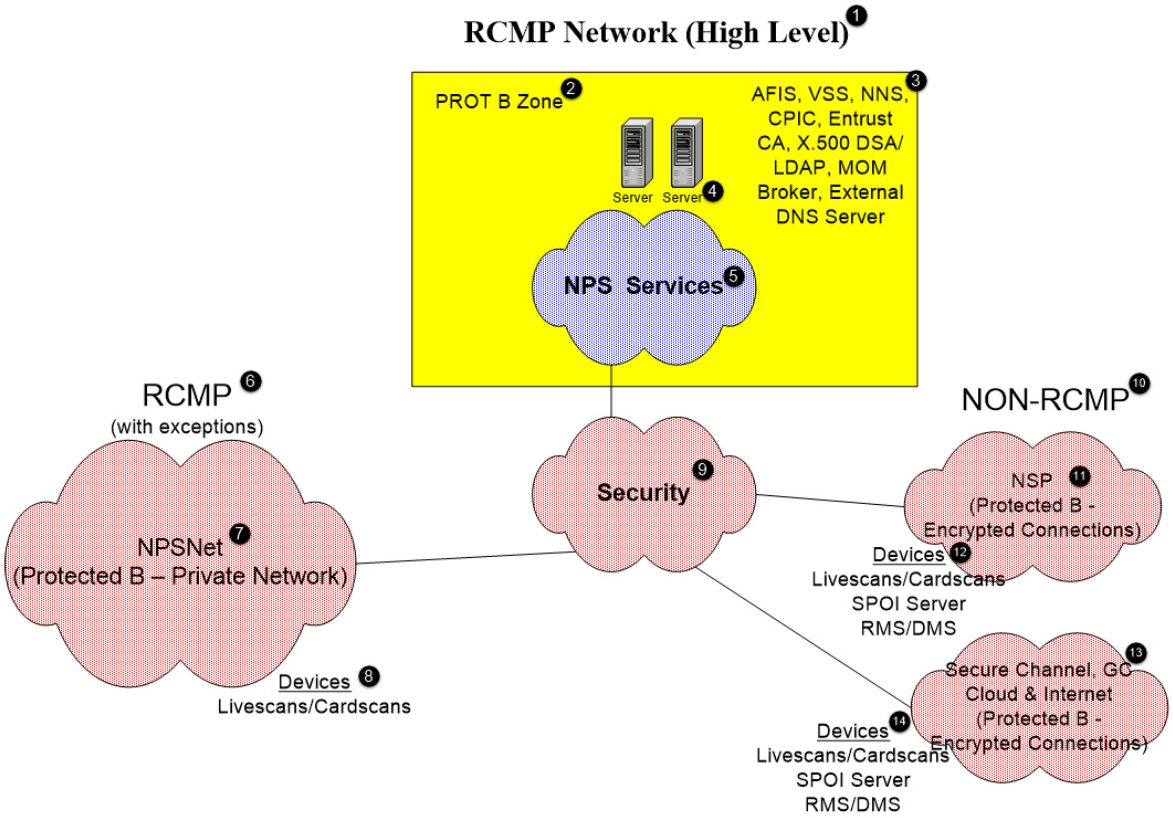

Figure 2-1 : Architecture conceptuelle de l'ITR

1	Réseau de la GRC (haut niveau)	8	Appareils LiveScan/CardScan
2	Zone PROT B	9	Sécurité
3	SAID, SSV, SNS, CIPC, Entrust CA, X.500 DSA/LDAP, répartition MOM, serveur DNS externe	10	NON GRC
4	Serveur	11	PSR (Protégé B – connexions chiffrées)
5	SNP	12	Appareils LiveScan/CardScan Serveur PAU SGD/SPS
6	GRC (avec exceptions)	13	Voie protégée, nuage du GC et Internet (Protégé B – connexions chiffrées)
7	NSPnet (Protégé B – réseau privé)	14	Appareils LiveScan/CardScan Serveur PAU RMS/DMS

2.2 Sécurité de l'ITR dans l'architecture de la GRC

2.2.1 CHIFFREMENT

1. Toutes les données de l'ITR transmises à l'extérieur de la zone de sécurité Protégé B doivent être chiffrées lors de la transmission de l'organisme contributeur ou de dactyloscopieuses électroniques/serveurs SMTP-PAU, ou vers un tel organisme ou appareil.

2. RSNP est un réseau privé MPLS protégé qu'utilisent la GRC et SPC.

3. La NSP est une extension du réseau de la GRC/de SPC, que l'on appelle généralement un RL géré. Des RPV contrôlés et gérés par la GRC et SPC à chaque site permettent à des capacités comme l'ITR de s'étendre à des sites qui n'appartiennent pas à la GRC avec des communications protégées.

4. La VCP/le nuage du GC est un réseau de communication protégé contrôlé et géré par le GC au moyen de RPV. La VCP/le nuage du GC permettent la connectivité entre des ministères qui doivent accéder à l'ITR.

5. De plus, des RPV permanents et temporaires peuvent être établis grâce à une connexion à Internet pour des agences privées qui soumettent des données à l'ITR.

2.2.2 IDENTIFICATION ET AUTHENTIFICATION

1. L'accès direct d'un utilisateur à une dactyloscopieuse électronique exige une authentification à deux facteurs. Un certificat (jeton ou carte intelligente) et un mot de passe sont nécessaires pour authentifier les utilisateurs qui accèdent à l'ITR.

2. Les personnes qui utilisent une dactyloscopieuse électronique et qui établissent une connexion directe avec l'ITR doivent établir un RPV sécurisé à l'aide de l'authentification à deux facteurs. Une fois ce RPV établi, la dactyloscopieuse électronique pourra échanger des paquets NIST conformes avec l'ITR. Les dactyloscopieuses électroniques doivent prendre en charge l'établissement d'une connexion sécurisée et la communication avec l'ITR pour répondre à toutes les exigences contenues dans l'ÉB et les documents connexes.

3. Pour ce qui est des RPV sécurisés établis en permanence, les dactyloscopieuses électroniques/appareils SMTP-PAU doivent fonctionner dans le tunnel sécurisé créé pour répondre à toutes les exigences énoncées dans l'ÉB et les documents connexes. Il incombera à la GRC/au GC/aux APMC d'établir des RPV sécurisés permanents.

2.3 Architecture de haut niveau actuelle de la GRC/du GC/des APMC

1. La Figure 2-2 : Architecture de haut niveau actuelle de l'ITR, illustre la connectivité des dactyloscopieuses électroniques/appareils SMTP-PAU dans l'architecture de la GRC/du GC/des APMC. On la présente ainsi pour montrer la relation entre l'architecture de sécurité conceptuelle de la GRC/de SPC et les dactyloscopieuses électroniques/appareils SMTP-PAU.

2. Une brève description de chaque composante est donnée dans l'Appendice A de l'ÉB. Des descriptions plus détaillées des composantes sont incluses à la Section 3

Nouvelle portée des dactyloscopieuses électroniques et des PAU dans l'architecture actuelle.

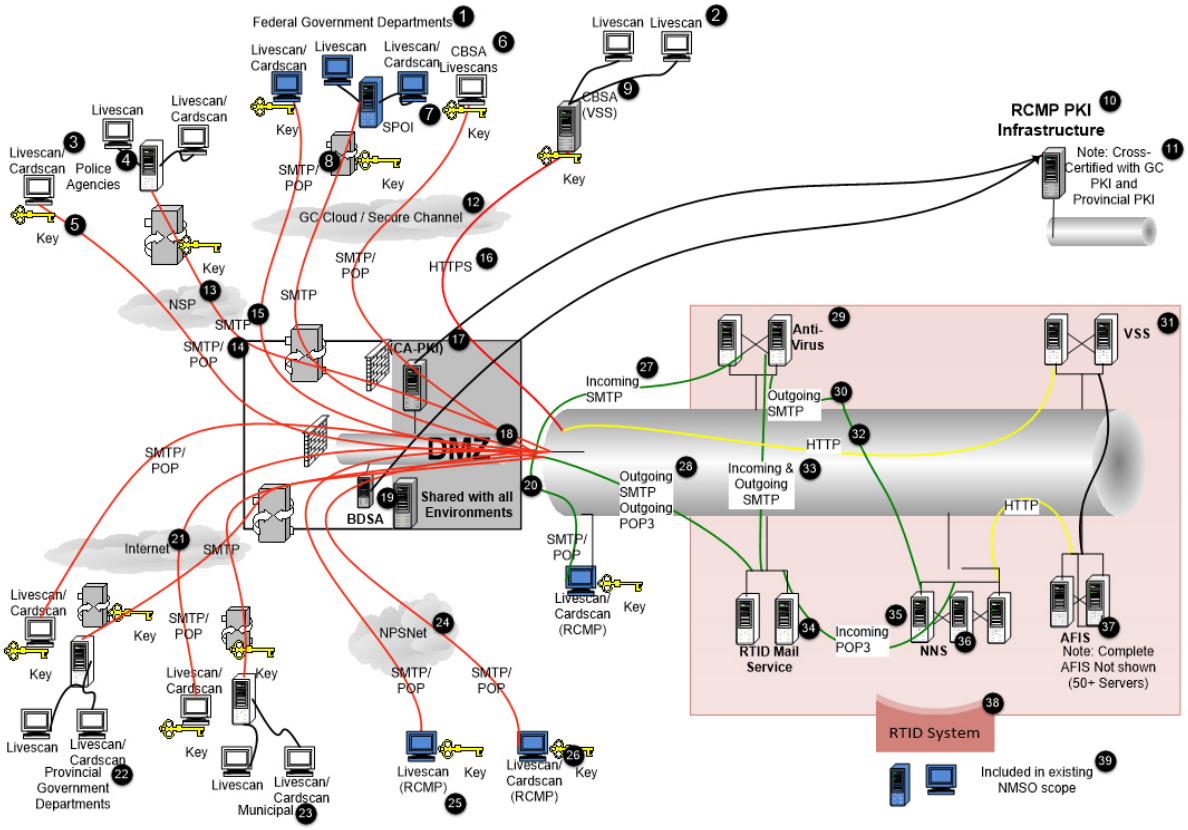

Figure 2-2 : Architecture de haut niveau actuelle de l'ITR

1	Ministères fédéraux	21	Internet
2	LiveScan	22	Ministères provinciaux
3	LiveScan/CardScan	23	Municipalités
4	Services de police	24	NSPNet
5	Clé	25	LiveScan (GRC)
6	ASFC LiveScan	26	LiveScan/ CardScan (GRC) Clé
7	PAU	27	SMTP entrant
8	SMTP/POP	28	SMTP sortant POP3 sortant
9	ASFC SSV	29	Antivirus
10	ICP de la GRC	30	SMTP sortant
11	Remarque : cocertifiée avec l'ICP de la GRC et l'ICP provinciale	31	SSV
12	Nuage du GC/Voie de communication	32	HTTP

	protégée		
13	SNP	33	SMTP entrant et sortant
14	SMTP/POP	34	Service de messagerie de l'ITR
15	SMTP	35	POP3 entrant
16	HTTPS	36	SNP
17	(CA – ICP)	37	SAID Remarque : Le SAID n'est pas illustré au complet (plus de 50 serveurs)
18	DMZ	38	Système de l'ITR
19	BDSA	39	Inclus dans la portée de l'OCPN actuelle
20	Partagé avec tous les environnements		

3. NOUVELLE PORTÉE DES DACTYLOSCOPIEUSES ÉLECTRONIQUES ET DES PAU DANS L'ARCHITECTURE ACTUELLE

3.1 Exemple d'architecture de connectivité des dactyloscopieuses électroniques et des PAU

1. Le diagramme ci-dessous, la Figure 3-1 : Exemple d'architecture de connectivité dactyloscopieuse électronique/PAU, illustre un exemple de connectivité entre une dactyloscopieuse électronique et un PAU. Le diagramme présente différentes combinaisons d'appareils dans l'architecture pour montrer les options de connectivité communes entre les dactyloscopieuses électroniques/appareils PAU et d'autres appareils dans l'architecture de l'ITR.

2. Un appareil LiveScan ou CardScan peut être relié directement à l'ITR par l'établissement d'une connexion chiffrée sécurisée. Une fois la connexion établie, à supposer que l'utilisateur possède un certificat valide qui lui permet d'accéder à l'ITR, la dactyloscopieuse électronique pourra communiquer avec l'ITR grâce aux protocoles SMTP et POP.

3. De multiples dactyloscopieuses électroniques peuvent être reliés à un PAU, et le PAU communique directement avec l'ITR grâce à une connexion chiffrée sécurisée. Le PAU appuie la communication avec l'ITR par SMTP bidirectionnelle et la communication des résultats de l'ITR à la dactyloscopieuse électronique voulue. La communication entre une dactyloscopieuse électronique de l'OCPN et le PAU se fait par SMTP/POP. Un autre protocole de communication pourrait être acceptable pour la GRC/le GC/des APMC. Cependant, ce protocole doit satisfaire aux exigences de sécurité de l'ITR/la GRC et être approuvé par la GRC/le GC/les APMC.

4. Une dactyloscopieuse électronique peut aussi communiquer avec un SGD/SPS par SMTP et/ou POP. Par exemple, l'information concernant une personne dont l'on prélève les empreintes digitales peut être fournie par le SGD à la dactyloscopieuse électronique, que la dactyloscopieuse électronique utilise pour créer des paquets conformes SNP-NIST qui seront envoyés à l'ITR. Les exigences détaillées concernant cette communication entre les dactyloscopieuses électroniques et un SGD/SPS sont décrites à l'Annexe B de l'Appendice A – Exigences détaillées des dactyloscopieuses électroniques.

5. Une dactyloscopieuse électronique peut aussi demander des données sur une personne dont l'on prélève les empreintes digitales d'un système ministériel/organisationnel afin d'obtenir des données qui seront insérées automatiquement dans les champs voulus de l'IU de la dactyloscopieuse électronique et les paquets SNP-NIST, selon les besoins. On utilise l'ASFC comme exemple à la Figure 3-1 : Exemple d'architecture de connectivité dactyloscopieuse électronique/PAU pour illustrer cette connectivité HTTP. Les exigences détaillées concernant cette communication entre les dactyloscopieuses électroniques et systèmes ministériels/organisationnels sont décrites à l'Annexe B de l'Appendice A – Exigences détaillées de la dactyloscopieuse électronique.

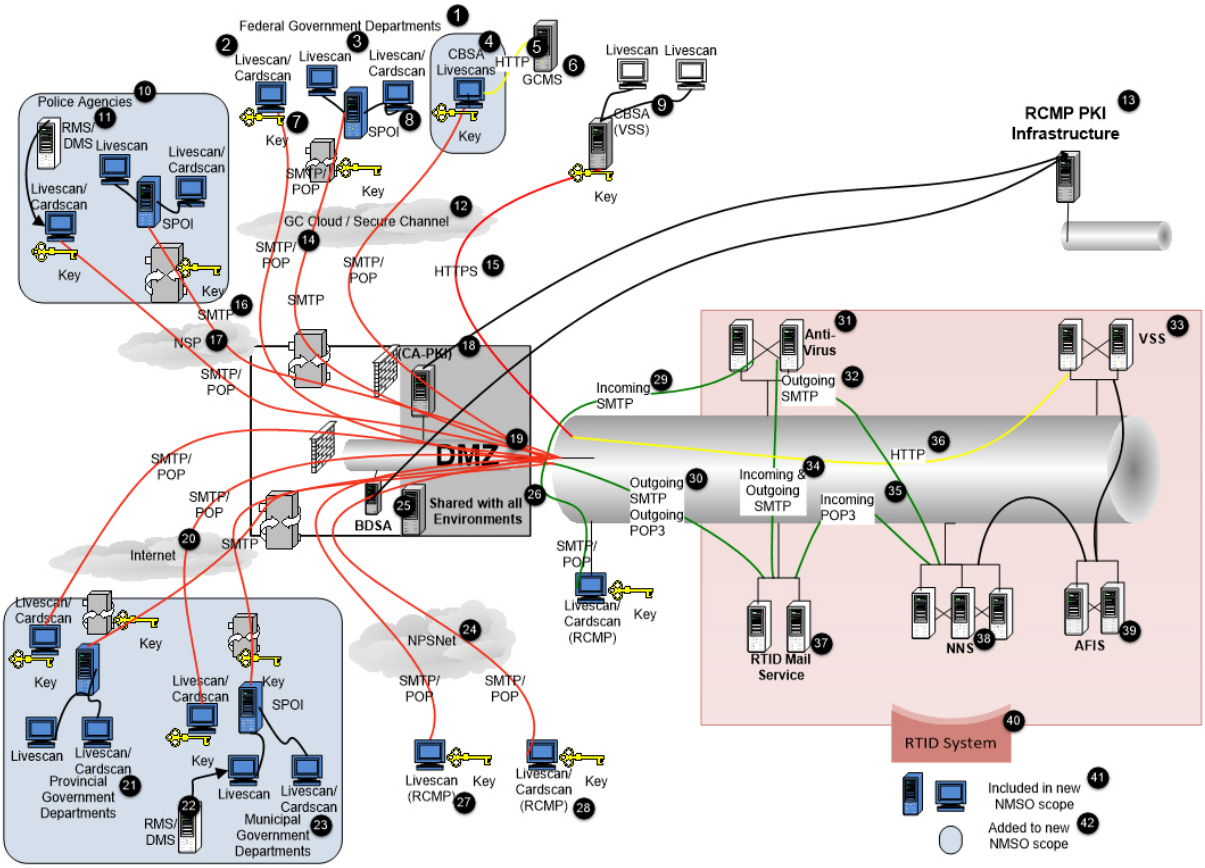

Figure 3-1 : Exemple d'architecture de connectivité dactyloscopieuse électronique/PAU

1	Ministères fédéraux	22	SGD/SPS
2	LiveScan/ CardScan	23	Divisions d'administrations municipales
3	LiveScan	24	NSPNet
4	ASFC LiveScan	25	BDSA
5	HTTP	26	Partagé avec tous les environnements
6	SMGC	27	LiveScan (GRC)
7	Clé	28	LiveScan/CardScan (GRC)
8	PAU	29	SMTP entrant
9	ASFC (SSV)	30	SMTP sortant POP3 sortant
10	ICP de la GRC	31	Antivirus
11	Remarque : cocertifiée avec l'ICP de la GRC et l'ICP provinciale	32	SMTP sortant
12	Nuage du GC/Voie de communication protégée	33	SSV
13	PSN	34	SMTP entrant et sortant
14	SMTP/POP	35	POP3 entrant
15	SMTP	36	HTTP
16	HTTPS	37	Service de messagerie de l'ITR

17	PSN	38	SNP
18	(CA – ICP)	39	SAID
19	DMZ	40	Système de l'ITR
20	Internet	41	Inclus dans la portée de la nouvelle OCPN
21	Ministères provinciaux	42	Ajouté à la portée de la nouvelle OCPN

3.2 Exemple de connectivité de site détaillée des dactyloscopieuses électroniques et des PAU

1. La Figure 3-2, Exemple de connectivité de site détaillée des dactyloscopieuses électroniques et des PAU, illustre les différents types de dactyloscopieuses électroniques, d'appareils PAU et de périphériques configurés dans un site. Ce diagramme détaillé montre un exemple de comment de multiples dactyloscopieuses électroniques pourraient être reliés dans un site avec un PAU servant à communiquer avec l'ITR.

2. La Figure 3-3 : Exemple de connectivité de site LiveScan avec kiosque unique illustre un kiosque LiveScan unique établissant une connexion sécurisée avec l'ITR par l'entremise du nuage du GC.

3. La Figure 3-4 : Exemple de connectivité de site LiveScan avec ordinateur de bureau unique illustre un ordinateur de bureau LiveScan unique établissant une connexion sécurisée avec l'ITR par l'entremise d'Internet.

4. Tous ces exemples illustrent une architecture de sécurité commune, où n'importe quel appareil doit utiliser une connexion sécurisée existante ou établir une connexion sécurisée avec l'ITR avant que toute communication puisse être effectuée. Quand on utilise un PAU, il incombe à l'agence de s'assurer que toutes les communications avec les dactyloscopieuses électroniques et le PAU sont suffisamment sécurisées pour répondre aux exigences de l'ITR.

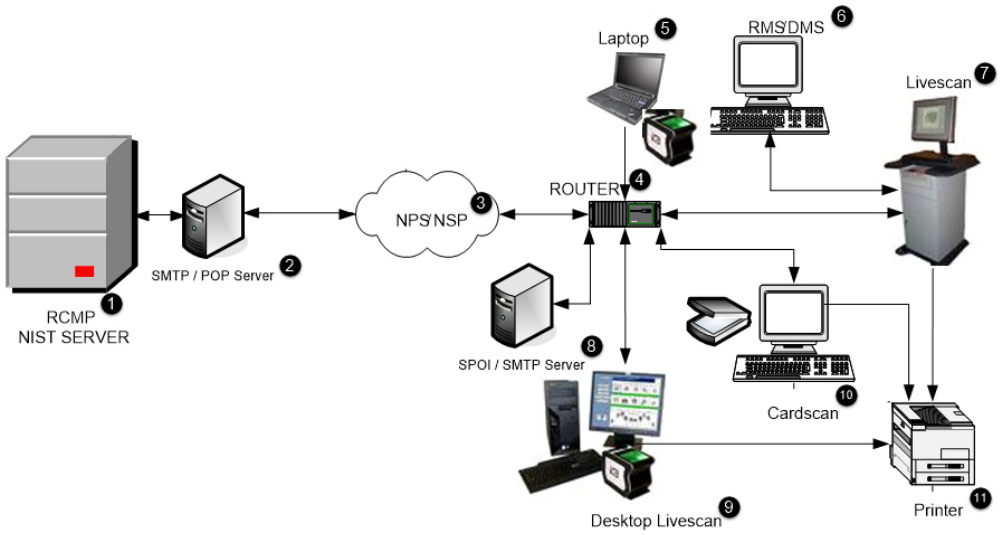

Figure 3-2 : Exemple de connectivité de site dactyloscopieuse électronique/PAU

1	Serveur NIST de la GRC	7	LiveScan

2	Serveur SMTP/POP	8	Serveur PAU/SMTP
3	SNP/PSN	9	Ordinateur de bureau LiveScan
4	Routeur	10	CardScan
5	Ordinateur portable	11	Imprimante
6	SGD/SPS		

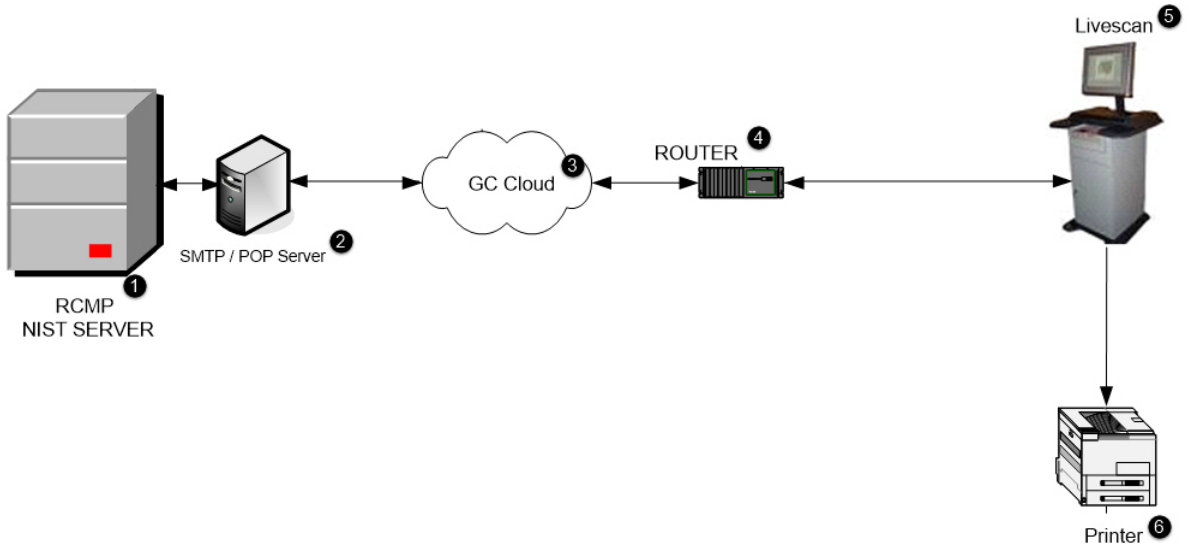

Figure 3-3 : Exemple de connectivité de site LiveScan avec kiosque unique

1	Serveur NIST de la GRC	4	Routeur
2	Serveur SMTP/POP	5	LiveScan
3	Nuage du GC	6	Imprimante

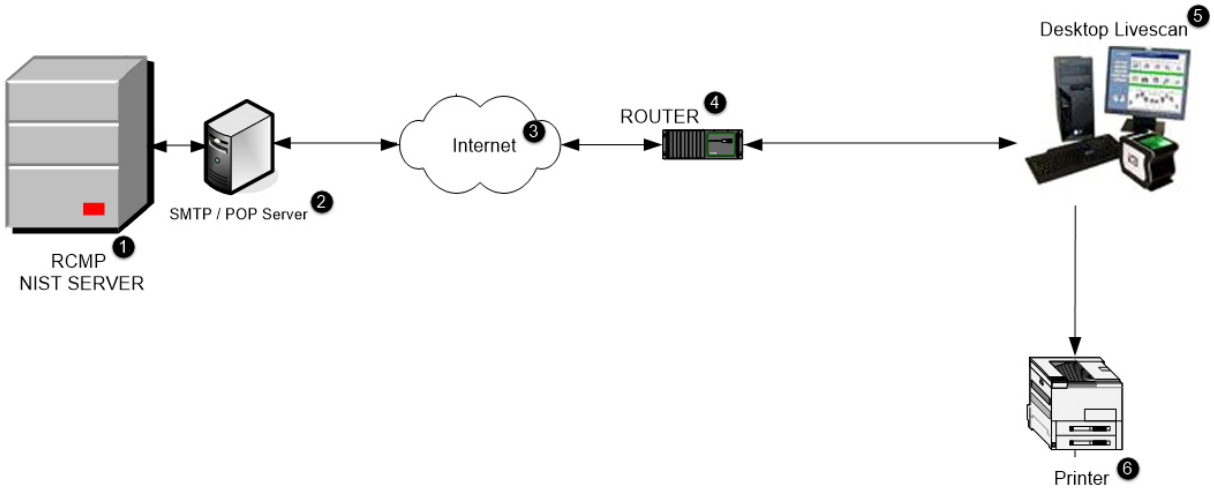

Figure 3-4 : Exemple de connectivité de site LiveScan avec ordinateur de bureau unique

1	Serveur NIST de la GRC	4	Routeur
2	Serveur SMTP/POP	5	Ordinateur de bureau LiveScan
3	Internet	6	Imprimante