RCMP·GRC

ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

Canadian Criminal Real Time Identification Services

RTID Technical Guidelines for Agencies

Date:	2015-02-10
Status:	Final
Version:	3.0
Classification	Unclassified
Owner	Biometric Business Solutions
RDIMS :	19086

RECORD OF AMENDMENTS

Version No.	Date	Comments
1.1	2005-11-02	Initial Draft version
1.2	2005-11-07	Modified to include comments from Client Commitment Team
1.3	2005-11-18	Modified to include comments from Technical Writer
1.4	2006-06-20	Modified as “RTID Phase 1 Technical Requirements”
1.5	2006-07-23	Edited by CCC Technical Writer
1.6	2006-08-10	Edited by CCC Team
1.7	2006-08-20	Edited by CCC Technical Writer
1.8	2006-08-29	Edited by CCC Technical Writer
1.9	2006-10-25	Edited by CCC Technical Writer – Distributed to RTID Resources – Suggested changes incorporated in final version
2.0	2008-05-29	Client-to-System Connections SCNet details added
2.1	2009-01-22	Updated Federal / CPIC text
2.2	2009-05-15	Changed SPOI to SPOC (Single Point of Contact)

DOCUMENT ORIGIN AND APPROVAL RECORD

Approvals	Position (Actual signatures are found on a formal deliverable checklist)
Acceptor	CCRTIS Director General
Acceptor	OIC, CCRTIS Operational Support & Client Services
Acceptor	OIC, CCRTIS Biometric Business Solutions
Policy Centre	CCRTIS Operational Support & Client Services

DISCLAIMER

The purpose of this document is to provide agencies with an overview of the network and security infrastructure between the agency's network and the National Police Services Network (NPSNet) for Real Time Identification (RTID) purposes.

While the Royal Canadian Mounted Police (RCMP) has provided guidelines for preparing an agency to connect to the NPSNet, the RCMP makes no claims as to the completeness and accuracy of the documentation herein. It is the user of this information who is ultimately responsible for the adaptation and integration of changes into existing systems and the ensuing results. The RCMP, Forensic Science and Identification Services (FS&IS), and the Canadian Criminal Real Time Identification Services (CCRTIS) disclaim any responsibility, liability, costs, loss of efficiencies or other economic loss whether direct or consequential, flowing from any use made by the user of this information and other materials provided herein.

The RCMP makes no warranties, express or implied, and specifically disclaims any implied warranty of merchantability or fitness for a particular purpose. The RCMP will not be responsible for any errors or omissions which may have occurred in the drafting of this information and expressly disclaim liability whether under contract or in negligence to any user of the work whether a direct user, any person who may borrow or use it or to any client of such a person.

In taking possession of this document, the user agrees to not release this document to a third party without the expressed written permission of the RCMP. The user of this document acknowledges, agrees and accepts the foregoing and releases, agrees to indemnify and hold harmless the RCMP, FS&IS and CCRTIS.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to provide agencies with an overview of the communications infrastructure between the agency's network and the National Police Services Network (**NPSNet**) for Real Time Identification (**RTID**) purposes. This document provides Agencies with an overview of the RTID Single Point of Contact (**SPOC**) connectivity model and the network connectivity options that are available to agencies.

1.2 AUDIENCE

This document is intended for the following types of agencies. All agencies are addressed in this document in conjunction with their respective network connectivity options:

1. Law Enforcement Agencies

   e.g. RCMP, Provincial Police, Municipal Police and Military Police that process criminal, civil, and refugee fingerprints and federal agencies with law enforcement capabilities

2. Federal Government Agencies

   e.g. Public Works and Government Services Canada, Canada Revenue Agency, and other federal agencies that process non-criminal fingerprints

3. Private Companies

   e.g. Private sector organizations that have been accredited to take fingerprints for civil purposes

1.3 RTID NETWORK CONNECTION OPTIONS

The following table applies to all agencies and their available network connectivity options:

Table 1: RTID Network Connection Options

Agency Type	RTID Network Connection Options [1]		
	NSP	SCNet	Secure Internet
Law Enforcement	All	Not Available	Not Available
Federal	Not Available	Federal Agencies Only[2]	Not Available
Private	Not Available	Not Available	All

[1] Network connectivity options for provincial, municipal and territorial government agencies will be evaluated on a case- by-case basis by the RCMP.

[2] Federal government agencies must connect to the NPSNet via shared VPN tunnel over the SCNet.

2 SINGLE POINT OF CONTACT (SPOC)

SPOC is an RTID concept identifying that an agency has a single network connection to the NPSNet. The agency may communicate directly with the National Police Services – National Institute of Standards and Technology (**NPS-NIST**) Server via Simple Mail Transfer Protocol (**SMTP**) through the network connectivity option that is applicable to the agency.

The agency's SPOC may be a single Electronic Fingerprint Capture Device (**EFCD** e.g. Live Scan or Card Scan), or a central messaging server with multiple EFCDs and other systems that reside behind the agency's server on the agency's network. The agency's SPOC would connect directly to the NPS-NIST Server (**Workflow Manager**), and would be the agency's only point of access to the NPSNet.

The SPOC model may imply the integration of EFCDs with other system components that reside behind a central messaging server at the agency's site. In turn, the agency's server would communicate directly with the Workflow Manager on behalf of all the EFCDs / system components at the agency's site.

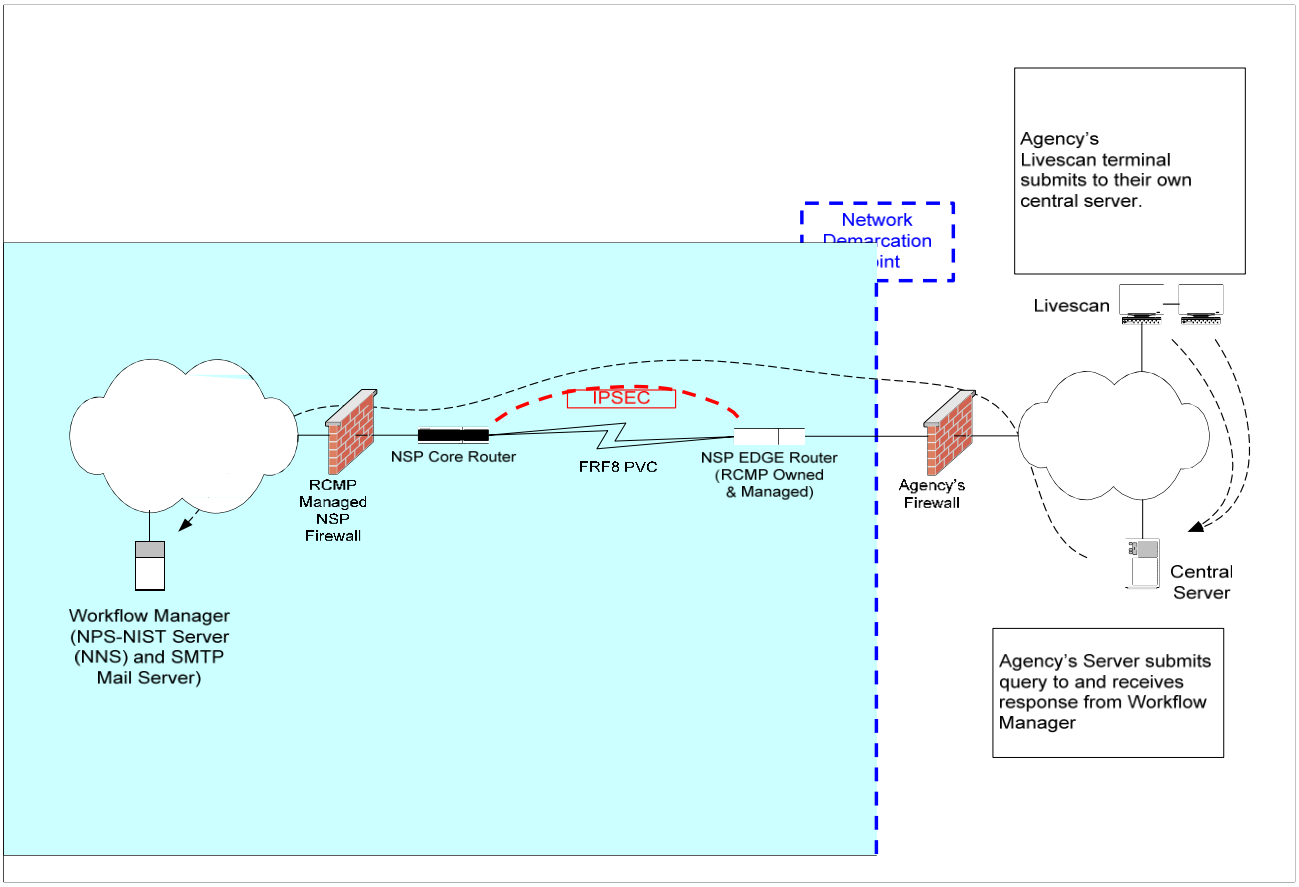
All agencies that intend to submit transactions to the Workflow Manager must adhere to the SPOC concept.

Note: For further details on the SPOC concept, refer to **Section 2** in the *Best Practices for the Implementation of Civil Electronic Fingerprint Capture Devices Workflows* document.

3 NETWORK SECURITY POSTURE

3.1 LAW ENFORCEMENT AGENCY: SYSTEM-TO-SYSTEM CONNECTION

Figure 1 - Law Enforcement Agency: System-to-System Connection



3.1.1 Overview

- A System-to-System network connection promotes the implementation and usage of a SPOC connectivity model.
- Connectivity occurs via a Network Security Posture (**NSP**) circuit between the law enforcement agency's server and the Workflow Manager.

3.1.2 Requirements

- Link state encryption, provided by the RCMP managed routers (NSP Core and Edge Routers), is required for its traversal over the frame relay communications circuit. The RCMP managed routers will incorporate an RCMP Entrust Device Certificate.
- The agency's server will reside on the agency's network.
- Communication from the agency's server to the Workflow Manager will use SMTP.

- Communication from the agency's server to the Workflow Manager will leverage an NSP connection as the network carrier.
- The agency's server will appear to the RCMP as either an agency owned Internet Assigned Numbers Authority (**IANA**) registered Internet Protocol (**IP**) address or through the Network Address Translation (**NAT**) as an RCMP assigned NSP IP address.
- The network demarcation point between the agency's network and the NSP will be the cable used to connect the RCMP managed NSP router to the agency's firewall (or the agency's server if no firewall is implemented).
- All data traversing NSP Wide Area Network (**WAN**) circuits is encrypted using IPSEC between an agency NSP spoke router and the NSP core router.

3.2 LAW ENFORCEMENT AGENCY - RESPONSIBILITIES

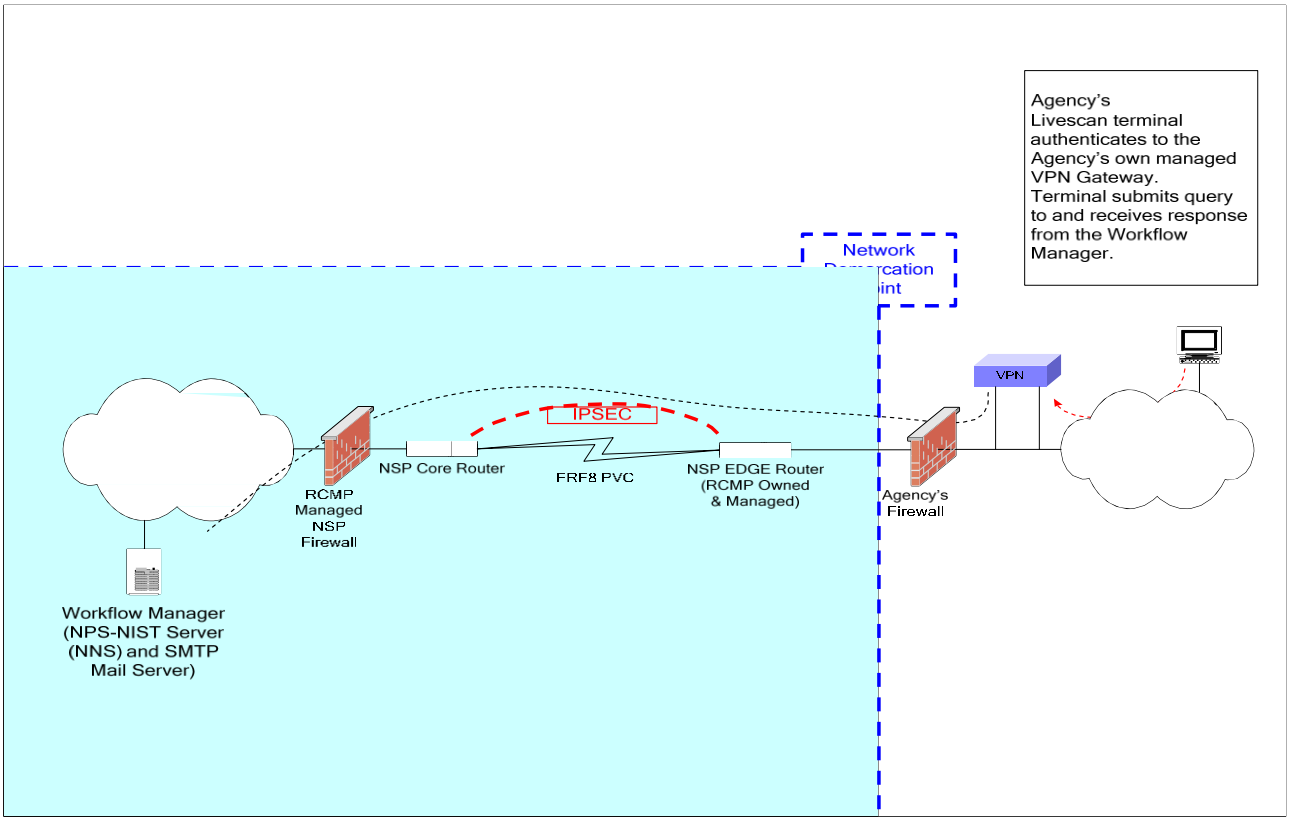
- The agency's server must communicate to the Workflow Manager via SMTP. It is the agency's responsibility to obtain and validate the SMTP functionality of their connection.
- It is the agency's responsibility to distribute RTID services to their various geographic locations using their own WAN as a carrier.
- All services that the RCMP offers and receives to and from the NSP agency networks must ingress and egress an RCMP firewall that resides in Ottawa, Ontario.
- Any modification to the agency's firewall must be scheduled no less than two weeks in advance. **Note**: Advance notice of firewall modification is important in the event that an agency changes their server IP address that is recognized by the NSP.
- The agency must collaborate with the RCMP security and network technical authorities on an ongoing basis in maintaining, modifying or upgrading their network as required in response to information security threats, changing technology standards, or migration to new equipment.
- The agency must provide the names and contact information for both a principal and secondary person responsible for technical and operational issues (e.g. network and security contacts) on an ongoing basis.

3.2.1 Recommendations

- The agency is strongly recommended to acquire and implement an EAL-4 compliant firewall device.

3.3 LAW ENFORCEMENT AGENCY: CLIENT-TO-SYSTEM CONNECTION

Figure 2 - Law Enforcement Agency: Client-to-System Connection
Agency Provides Client-to-Gate VPN



3.3.1 Overview

- Client-to-System network connection promotes the implementation and usage of a SPOC connectivity model.
- Connectivity occurs via an NSP circuit between the law enforcement agency's EFCD (e.g. Live Scan or Card Scan) and the Workflow Manager.

3.3.2 Requirements

- Link state encryption, provided by the RCMP managed routers (NSP Core and Edge Routers), is required for its traversal over the frame relay communications circuit. The RCMP managed routers will incorporate an RCMP Entrust Device Certificate
- The agency's EFCD will reside on its own network.
- The agency's EFCD will use SMTP for sending electronic transactions to the Workflow Manager, and Post Office Protocol (**POP**) for receiving electronic transactions from the Workflow Manager.
- Communication from the agency's EFCD to the Workflow Manager will leverage an NSP connection as the network carrier.

- The agency's EFCD will appear to the RCMP as either an Agency-owned IANA registered IP address or through the NAT as an RCMP assigned NSP IP address.
- The network demarcation point between the agency's network and the NSP will be the cable used to connect the RCMP-managed NSP router to the Agency's firewall (or the Agency's EFCD if no firewall is implemented).
- A client-to-gateway encrypted session of the agency's VPN device must be established.

3.4 LAW ENFORCEMENT AGENCY - RESPONSIBILITIES

- It is the agency's responsibility to obtain and validate the SMTP and POP functionality of their EFCD.
- It is the agency's responsibility to distribute RTID services to their various geographic locations using their own WAN as a carrier.
- All services that the RCMP offers and receives to and from the NSP agency networks must ingress and egress an RCMP firewall that resides in Ottawa, Ontario.
- Any modification to the agency's firewall must be scheduled no less than two weeks in advance. **Note**: Advance notice of firewall modification is important in the event that an agency changes their IP address that is recognized by the NSP.
- The agency must collaborate with the RCMP security and network technical authorities on an ongoing basis in maintaining, modifying or upgrading their network as required in response to information security threats, changing technology standards, or migration to new equipment.
- The agency must provide the names and contact information for both a principal and secondary person responsible for technical and operational issues (e.g. network and security contacts) on an ongoing basis.
- The agency must establish a client-to-gateway encrypted session of their VPN device.

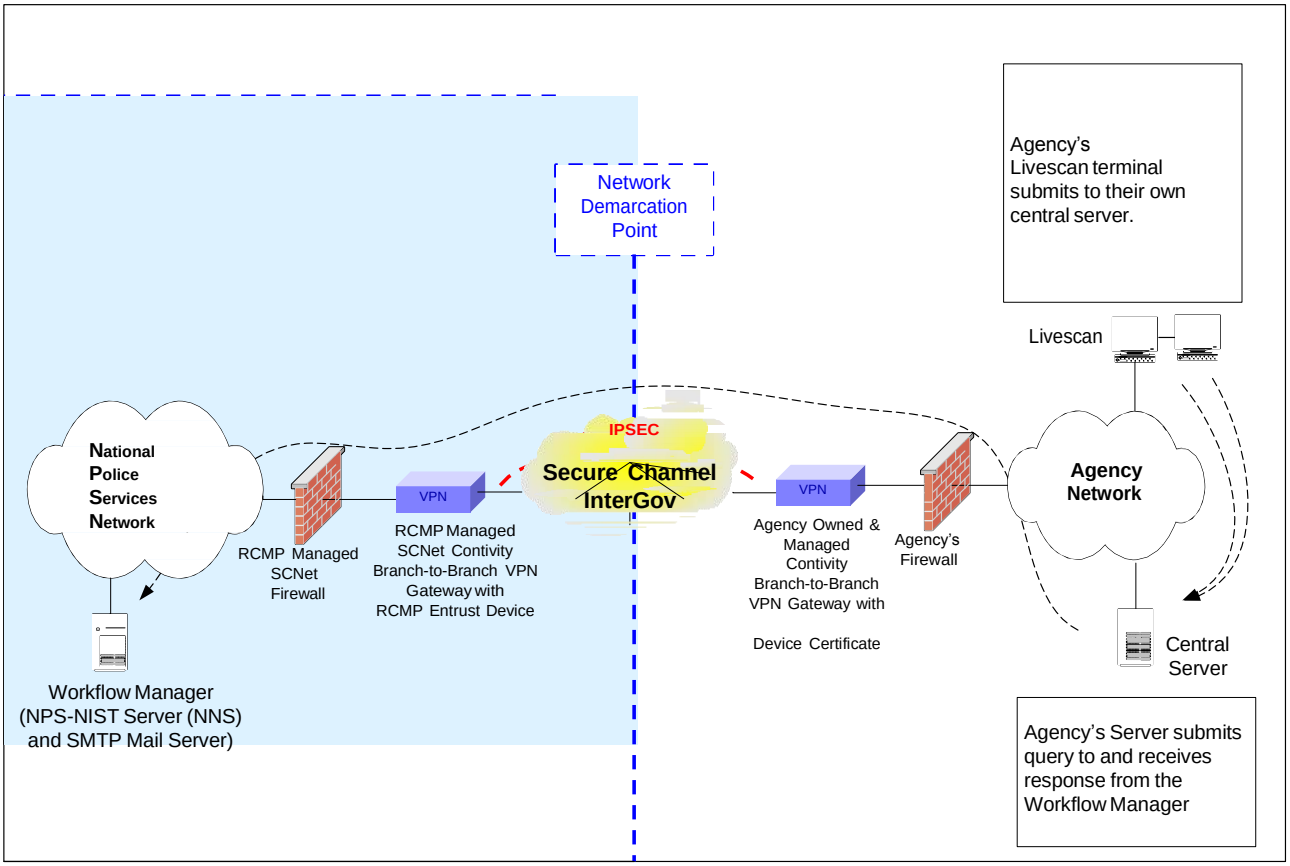
3.4.1 Recommendations

- An agency is strongly recommended to acquire and implement an EAL-4 compliant firewall device.

4 SECURE CHANNEL NETWORK (INTERGOV)

4.1 FEDERAL GOVERNMENT AGENCY: SYSTEM-TO-SYSTEM CONNECTION

Figure 3 - Federal Agency: System-to-System Connection



4.1.1 Overview

- A System-to-System network connection promotes the implementation and usage of a SPOC connectivity model.
- Connectivity occurs via an SCNet connection between the federal agency's server (e.g. SPOC) and the Workflow Manager.

4.1.2 Requirements

- A trusted VPN using the SCNet as a carrier will be established between the agency's VPN and the RCMP SCNet Branch-to-Branch VPN Gateway.
- Link state encryption provided by the trusted VPN between the agency's VPN Gateway and the RCMP SCNet Branch-to-Branch VPN Gateway.
- An RCMP cross-certified Entrust Device Certificate[3]

[3] Federal agencies may contact Public Works and Government Services Canada (PWGSC) Internal Credential Management (ICM) to inquire about PKI certificate services.

- The agency's Server will appear to the RCMP as an Agency-owned IANA registered IP address.

4.2 FEDERAL AGENCY RESPONSIBILITIES

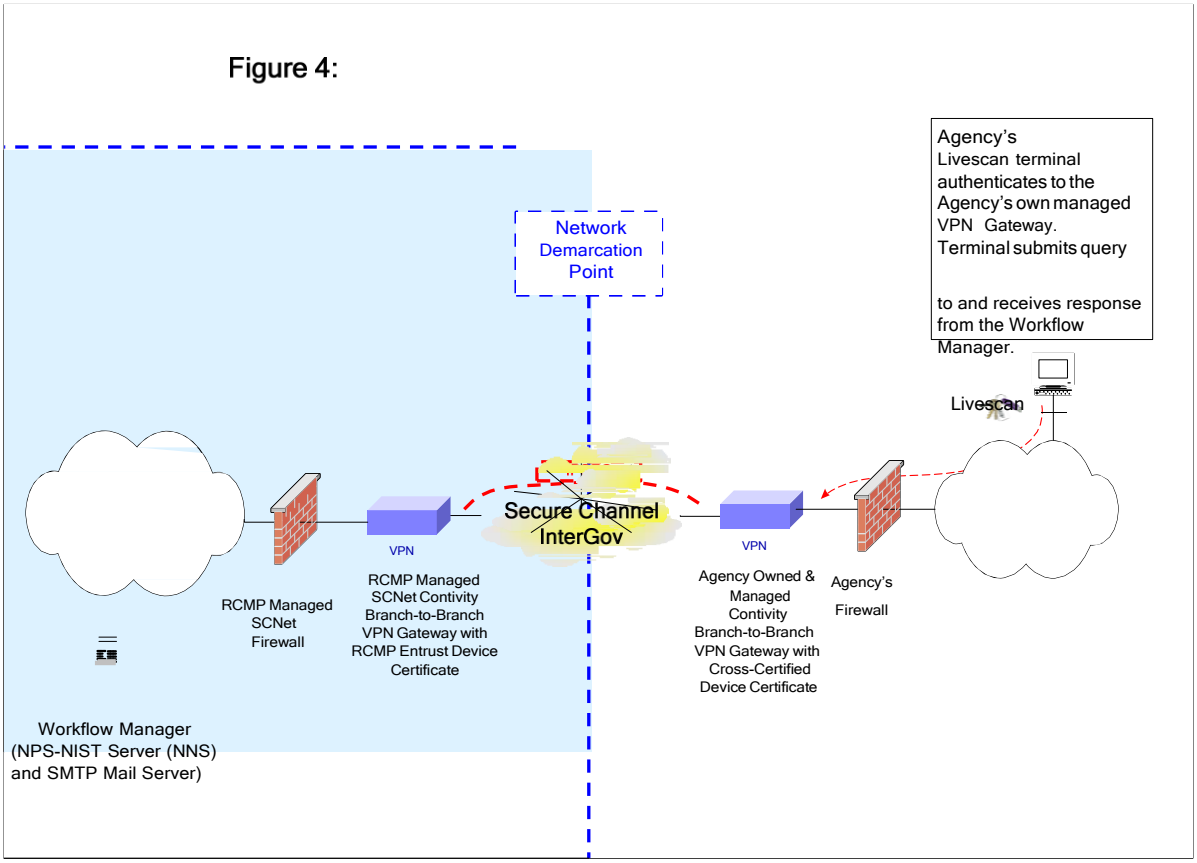
- The agency must purchase its own VPN Gateway Device – with an RCMP cross-certified Entrust Device Certificate - compatible with the RCMP's VPN deployment.
- The agency must supply the VPN device with well regulated and conditioned mains power, typically from a server room's in-line UPS or similar source, and install the VPN device in a well ventilated and secure area.
- It is the agency's responsibility to repair/replace their VPN device as required.
- The agency must collaborate with the RCMP security and network technical authorities on an ongoing basis in maintaining, modifying or upgrading their equipment (i.e. VPN) as required in response to information security threats, changing technology standards, or migration to new equipment.
- The agency must provide the names and contact information for both a principal and secondary person responsible for technical and operational issues on an ongoing basis.

4.2.1 Recommendations

- An agency is strongly recommended to acquire and implement an EAL-4 compliant firewall device.

4.3 FEDERAL AGENCY: CLIENT-TO-SYSTEM CONNECTION

Figure 4 - Federal Agency: Client-to-System Connection
Agency Provides Client-to-Gate VPN



4.3.1 Overview

- A Client-to-System network connection promotes the implementation and usage of a SPOC connectivity model.
- Connectivity occurs via an SCNet connection between the federal agency's EFCD (e.g. Live Scan or Card Scan) and the Workflow Manager.

4.3.2 Requirements

- A trusted VPN using the SCNet as a carrier will be established between the agency's VPN and the RCMP SCNet Branch-to-Branch VPN Gateway.
- Link state encryption provided by the trusted VPN between the agency's VPN Gateway and the RCMP SCNet Branch-to-Branch VPN Gateway.
- An RCMP cross-certified Entrust Device Certificate[4]
- The agency's EFCD will appear to the RCMP as an Agency-owned IANA registered IP address.

[4] Federal agencies may contact Public Works and Government Services Canada (PWGSC) Internal Credential Management (ICM) to inquire about PKI certificate services.

- A client-to-gateway encrypted session of the agency's VPN device must be established.

4.4 FEDERAL AGENCY RESPONSIBILITIES

- The agency must purchase its own VPN Gateway Device – with an RCMP cross-certified Entrust Device Certificate - compatible with the RCMP's VPN deployment.
- The agency must supply the VPN device with well regulated and conditioned mains power, typically from a server room's in-line UPS or similar source, and install the VPN device in a well ventilated and secure area.
- It is the agency's responsibility to repair/replace their VPN device as required.
- The agency must collaborate with the RCMP security and network technical authorities on an ongoing basis in maintaining, modifying or upgrading their equipment (i.e. VPN) as required in response to information security threats, changing technology standards, or migration to new equipment.
- The agency must provide the names and contact information for both a principal and secondary person responsible for technical and operational issues on an ongoing basis.
- The agency must establish a client-to-gateway encrypted session of its VPN device.

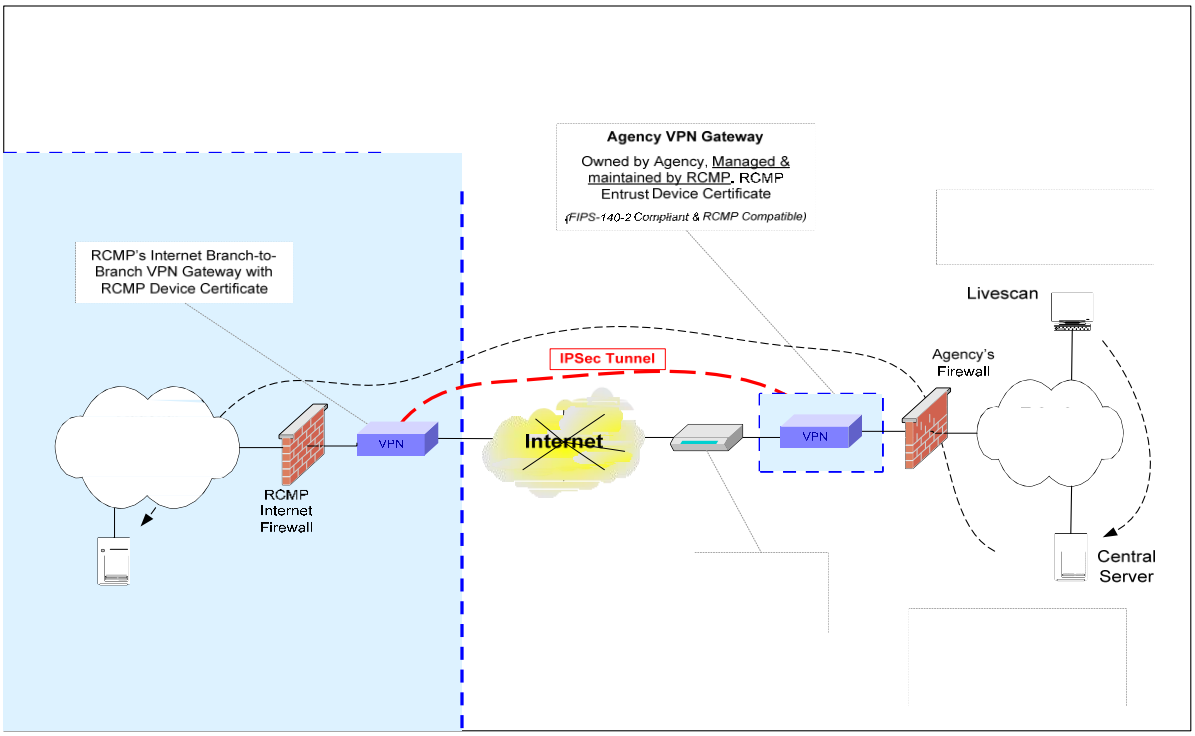
4.4.1 Recommendations

- An agency is strongly recommended to acquire and implement an EAL-4 compliant firewall device.

5 SECURE INTERNET

5.1 PRIVATE COMPANY: SYSTEM-TO-SYSTEM CONNECTION

Figure 5 - Private Company: System-to-System Connection



5.1.1 Overview

- A System-to-System network connection promotes the implementation and usage of a SPOC connectivity model.
- Connectivity occurs via the secure Internet connection between a private company's server (e.g. SPOC) and the Workflow Manager.

5.1.2 Requirements

- The IP address of the private company's server that appears to the NPSNet must be a Static[5] Registered IP address[6].
- If the Internet access device (e.g. router, Ethernet switch, etc.) is shared by private company network devices other than the VPN device, the access device must be able to support an IPSec tunnel. Otherwise, the VPN device will not be able to communicate with the RCMP.

[5] Static IP-addresses are assigned to permanent devices on a network whose IP addresses are constant and unchanging.

[6] Dynamic Host Configuration Protocol (DHCP) is not supported for this type of connection, as it complicates the maintenance and troubleshooting of the connection. **Note**: This requirement rules out using dial-up access over the PSTN, as this type of service does not support static IP addresses.

- An RCMP Entrust Device Certificate will be issued to the private company for their VPN. The RCMP will configure and install the private company's VPN with the RCMP Entrust Device Certificate.

5.2 PRIVATE COMPANY RESPONSIBILITIES

- Connection to the RCMP must be done by employing a Static Registered IP address only, which is either registered to the private company, or is owned on their behalf by a third party, such as an Internet Service Provider (**ISP**). [7]
- The private company must collaborate with the RCMP security and network technical authorities on an ongoing basis in maintaining, modifying or upgrading their network as required in response to information security threats, changing technology standards, or migration to new equipment.
- The private company must provide the names and contact information for both a principal and secondary person responsible for technical and operational issues on an ongoing basis.
- The private company is responsible for maintaining and/or troubleshooting their equipment (excluding the VPN device).
- The private company must purchase a VPN device compatible with the RCMP's VPN deployment.
- The private company must supply the VPN device with well regulated and conditioned mains power, typically from a server room's in-line UPS or similar source, and allow for the secure installation of the VPN device in a well ventilated area.
- The private company must provide free and reasonable access for authorized RCMP technicians to service, maintain or inspect the VPN device, in response to either a service issue, or for regular maintenance or equipment review.
- For private companies, if the VPN device malfunctions, an RCMP technician may install a "loaner" VPN device to assure that the private company can continue operating while their VPN device is being repaired. It is the private company's responsibility to submit their VPN device for repair / replacement.
    - The private company is expected to have the device repaired / replaced in a reasonable amount of time. The private company will contact the RCMP Central Help Desk (**CHD**) when the device is repaired, and an RCMP technician will be dispatched to swap out the RCMP "loaner" VPN device for the private company's repaired VPN device.
    - Collaboration with RCMP security and network technical authorities is expected on an ongoing basis. With respect to the VPN device, there may be need to upgrade the hardware, software and/or firmware to maintain the device's performance[8] (e.g. ability to secure traffic, compatibility with RCMP equipment, ability to maintain support from the manufacturer, etc).

[7] IP addresses officially registered to the private company either by their ISP or telecom service provider, or directly with a Regional Internet Registry (RIR).

[8] It is the private company's responsibility to decide whether to obtain hardware, software, firmware or other maintenance program with the VPN device manufacturer, or a third party.

- If upgrades are required, the private company will procure the appropriate upgrades for the VPN device within a reasonable timeframe (e.g. 30 - 60 days or less). In the case of upgrades required to mitigate a security threat, the private company will be expected to quickly respond (e.g. timeline will depend on the severity of the threat).

5.2.1 Recommendations

- A commercial grade of Internet service will usually have a better underlying availability and mean-time-to-repair (MTTR) than residential or non-commercial services.
- A private company is strongly recommended to acquire and implement an EAL-4 compliant firewall device.
- If a private company chooses to implement a firewall device, the private company must review its firewall (e.g. configuration requirements) with RCMP NSB. [9]

[9] The private company will share information about their firewall configuration in confidence, sufficient to enable a secure connection. In particular, the firewall must be configured to accept only the VPN tunnel traffic from the RCMP. The sharing of this information will not in any way imply a certification or validation of the company's firewall configuration by the RCMP.

6 FEDERAL AGENCY CONNECTION TO THE NPSNET

6.1 CONNECTION TO RTID

A federal agency must connect to the NPSNet via a shared VPN tunnel over the SCNet as described in Section 4 of this document.

6.2 BUSINESS-TO-BUSINESS MIGRATION

The RCMP is working towards migrating all agencies to a single point of connection for NPSNet services. This VPN tunnel over the SCNet into the NPSNet for RTID is considered a business-to-business connection between a federal government agency and the NPSNet. The RCMP intends to leverage this permanent connection to each federal agency's network as the sole medium to deliver RTID and all other NPSNet applications, such as a Canadian Police Information Centre (**CPIC**) application (e.g. **CPICWeb**).

Currently, several federal government agencies access NPSNet services (e.g. CPICWeb) via one or more RCMP provided direct-connect NPSNet circuits. As part of the SPOC business model, federal agencies must work towards integrating any other current NPSNet services (e.g. CPICWeb) they may receive into their own network. To summarize, all NPSNet services that a federal agency may require will be delivered to the agency's network via a single SCNet VPN in a business-to-business fashion.

6.3 ADVANTAGES OF BUSINESS-TO-BUSINESS MIGRATION

The RCMP can deliver multiple NPSNet services to a federal agency by means of a single network connection. In turn, the federal agency may integrate NPSNet applications (e.g. CPICWeb) as additional icons on the agency's current internal desktops, thereby eliminating the need for workstations that are only dedicated to NPSNet applications.

- The diagrams on the following pages provide an overview of the RCMP's transition towards business-to-business SCNet connections for federal agencies

Figure 6 - Federal Agency – RCMP Managed End-to-End

Overview of the present connectivity model that several Federal Government agencies may employ to access NPSNet applications.

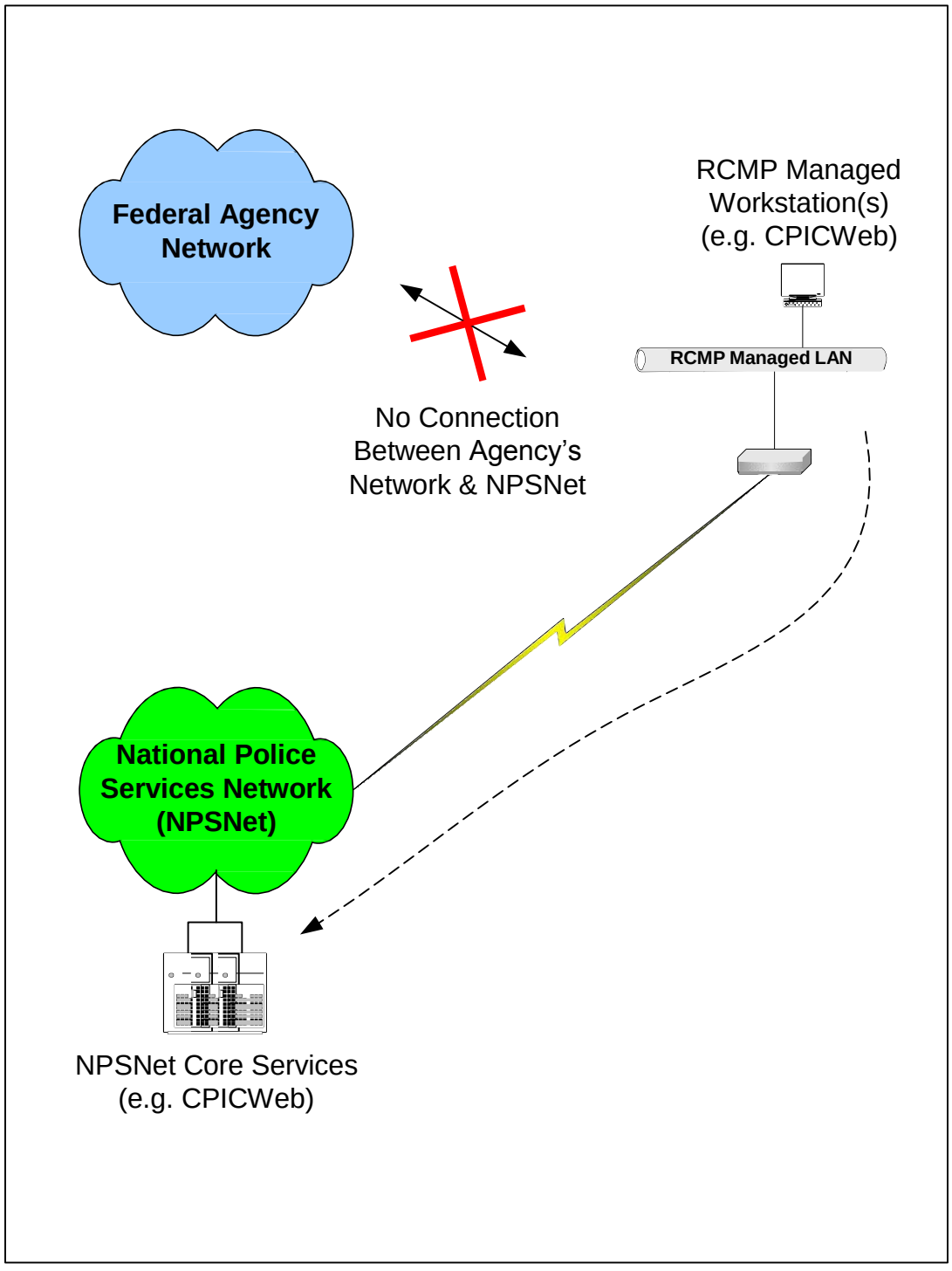
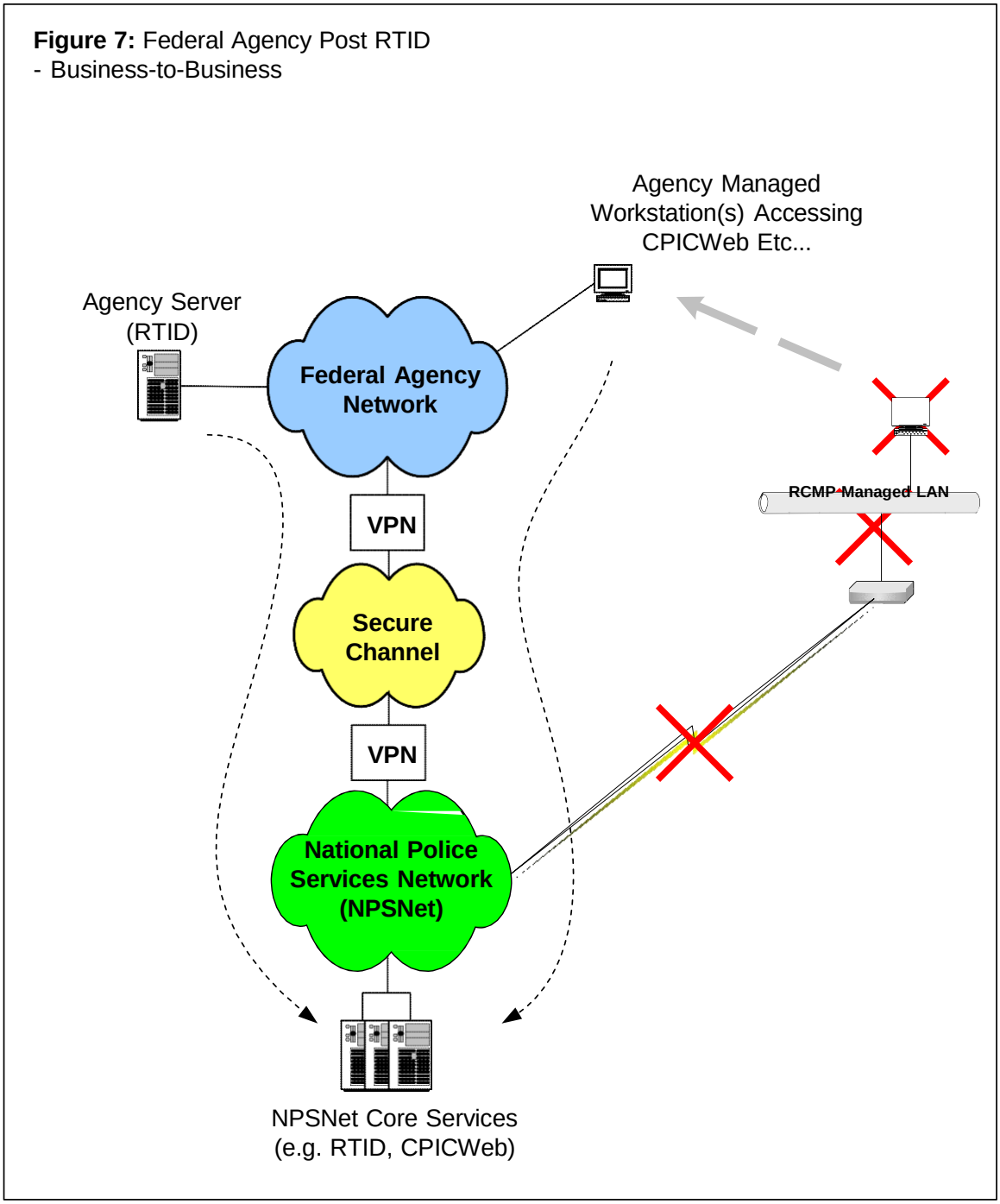


Figure 7 - Federal Agency Post RTID - Business-to-Business

Overview of a federal government agency's migration towards a business-to-business SCNet connection to the NPSNet.

Figure 7: Federal Agency Post RTID - Business-to-Business



6.4 RTID and CPIC Applications

In order for a federal government agency to integrate a CPIC application into its own network, the agency's network must be approved by CPIC. Any federal government agency presently accessing NPSNet services from an RCMP managed network will be asked to enter into the NPSNet Connection Authorization Change / Request (NCACR) process with the intention of migrating all NPSNet services to the federal agency's shared VPN tunnel over the SCNet. Once the migration has commenced, and a tentative date is scheduled for the cancellation of any RCMP provided direct-connect NPSN circuits, the federal agency may begin interfacing with the NPSNet for RTID purposes.

7 CONTACT INFORMATION

CCRTIS Operational Support & Client Services

- Email: CCRTIS-SCICTR@rcmp-grc.gc.ca
- General business / certification inquiries

Central Help Desk (CHD)

- 1-800-461-7797
- RTID operational / technical support for authorized personnel
- **Note**: An agency must be certified by the RCMP prior to contacting CHD