RCMP
ROYAL CANADIAN MOUNTED POLICE

MAJOR PROJECTS DIRECTORATE

ANNEX A to Appendix A SOW

CURRENT RTID/AFIS/VSS ARCHITECTURE

AFIS RENEWAL

Last Updated Date:	2015-02-17
Status:	Draft
WBS:	REB-11
Version:	0.1
RDIMS Document No.:	TBD
Classification:	Protected A

RECORD OF AMENDMENTS

Version No.	RDIMS Ver.	Date	Comments	Author (s)

TABLE OF CONTENTS

FIGURES

TABLES

1. INTRODUCTION

1.1 PURPOSE

1. The purpose of document is to describe the current RCMP/SSC architecture within which RTID operates. The AFIS renewal and all its subsystems must operate effectively within this RCMP/SSC architecture and satisfy all the requirements stated in this SOW.
2. This document provides a brief high level description of the RCMP/SSC architecture and a more focused description of the RCMP/SSC architecture related to the AFIS components.

1.2 GENERAL

1. The RCMP performs a crucial role in the collection, storage and management of police related information. The National Police Services Network (NPSNet) provides the means by which the Canadian law enforcement organizations may electronically access this centrally located information. NPSNet also supports internal RCMP applications. NPSNet provides national network support to the RCMP and its business affinity partners over a private dedicated internetwork. NPSNet provides network services for the transport of electronic information in support of the operational and administrative services used by the client organizations. It serves approximately 60,000 users in approximately 1200 locations across Canada and the high Arctic.
2. NPSNet also provides connectivity to national police agencies, international police forces, Canadian federal, provincial and municipal organizations as well as private agencies requiring RTID capabilities. These connections are provided through a secure private VPN controlled and managed by Shared Services Canada (SSC) called the National Security Posture (NSP) and through establishing VPNs through the GOC Secure Channel Network (SCNet) or through secure VPNs through the Internet. All RTID agency connectivity is through one of these methods, which will be described throughout this document.

1.3 DOCUMENT ORGANIZATION

1. This document provides a brief high level description of the RCMP architecture. Following this high level architecture, a description of the current AFIS and VSS architecture is presented.
2. The AFIS and VSS architecture are described at a high level followed by detailed diagrams and descriptions of the connectivity between various AFIS and VSS components including the interfaces with RTID and RCMP/SSC components.

2. RCMP/SSC HIGH LEVEL ARCHITECTURE

2.1 RCMP/SSC CONCEPTUAL SECURITY ARCHITECTURE

1. The following diagram depicts a conceptual view if the RCMP/SSC security architecture within which RTID operates. Any details concerning the security architecture that are applicable to RTID can be discussed at the industry day associated with this AFIS Renewal SOW.
2. This diagram depicts the private dedicated RCMP network NPSNet as well as the NSP and SCNet/Internet VPN connectivity for external agencies.

   Note: Some sites are being migrated from a VPN connection to secure Multi-Protocol Label Switching (MPLS); however, there is no impact on RTID or AFIS. This is just an alternate method to establish a secure encrypted connection.
3. The diagram depicts the RTID devices that are used through the different types of connectivity.
4. Additionally, the diagram depicts a conceptual view of where NNS and the AFIS components are located within the RCMP/SSC architecture.

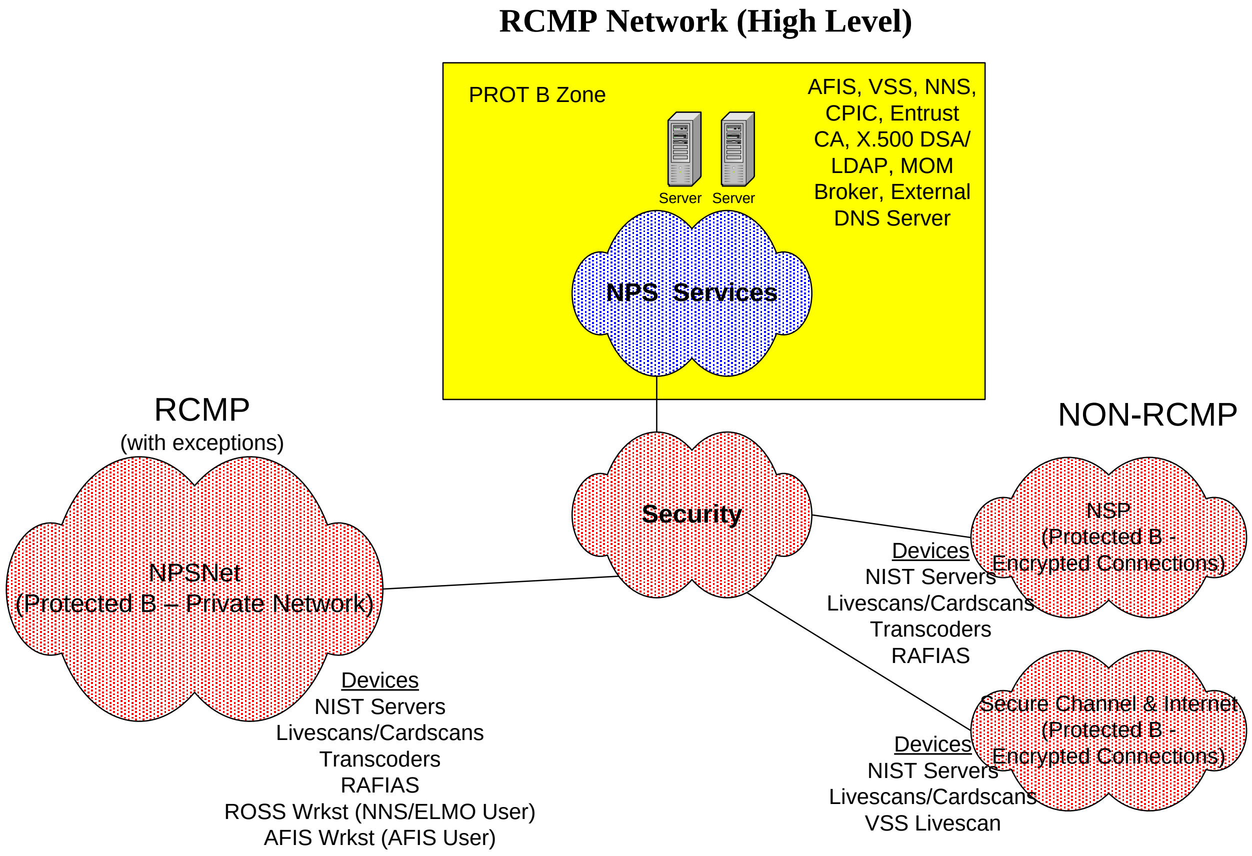
RCMP Network (High Level)
PROT B Zone
Server
Server
AFIS, VSS, NNS, CPIC, Entrust CA, X.500 DSA/ LDAP, MOM Broker, External DNS Server
NPS Services
RCMP
(with exceptions)
NPSNet
(Protected B – Private Network)
Devices
NIST Servers
Livescans/Cardscans
Transcoders
RAFIAS
ROSS Wrkst (NNS/ELMO User)
AFIS Wrkst (AFIS User)
Security
NON-RCMP
NSP
(Protected B - Encrypted Connections)
Devices
NIST Servers
Livescans/Cardscans
Transcoders
RAFIAS
Secure Channel & Internet
(Protected B - Encrypted Connections)
Devices
NIST Servers
Livescans/Cardscans
VSS Livescan

Figure 1: RTID Conceptual Architecture

2.2 RTID SECURITY WITHIN THE RCMP ARCHITECTURE

2.2.1 ENCRYPTION

1. All RTID data transmitted outside the Protected B security zone must be encrypted to/from the contributing agency or to/from the RTID NNS users.
2. NPSNet is a secure MPLS private network for RCMP/SSC use.
3. NSP is an extension of the RCMP/SSC network, typically referred to as a managed LAN. RCMP/SSC controlled and managed VPNs at each site allow capabilities including RTID to be extended to non-RCMP sites with secure communications.
4. SCNet is a GOC controlled and managed secure communication network using VPNs. RCMP/SSC enables connectivity with other government departments that require access to RTID.
5. Additionally, permanent and temporary VPNs can be established through an internet connection for private agencies submitting to RTID.

2.2.2 IDENTIFICATION AND AUTHENTICATION

1. Direct RTID user access requires two-factor authentication. Either a certificate (token or smart card) and password; or a biometric and password is required for authenticating users that access RTID.
2. AFIS user workstations are within an isolated Protected B zone; therefore, there are no encryption requirements for the communication between the AFIS workstations and the AFIS/VSS servers. AFIS users are authenticated with two-factor authentication using a biometric and password. Only local RCMP HQ users have access to AFIS.
3. Individuals on NSP, SCNet or the Internet can establish a temporary VPN using a token or smart card as two-factor authentication to be able to send RTID submissions and receive RTID responses through an SMTP/POP interface. Transcoder users use permanent encrypted VPNs and establish a session using a biometric and password, as two-factor authentication, to be able to send RTID submissions and receive RTID responses through an SMTP interface. These users can only send and receive email with RTID through a secure VPN. They do not have any RTID/NNS/AFIS user capabilities.

2.3 RTID LOAD BALANCING AND NETWORK ADDRESS TRANSLATION

1. For security, performance, scalability and load balancing reasons, the RCMP has implemented OSI layers 4-7 content switching with load balancing and Network Address Translation (NAT) support through Cisco network devices configured with ACE modules. This load balancing enables application and/or service requests to be directed to a virtual server and then distributed to multiple servers managed by the load balancing. NAT allows the IP addresses of the real servers to be concealed and transparent to the requester. NAT translates the IP address used in the request to the IP addresses of the real servers. This combination of services allows requests to be sent to a Virtual IP address (VIP) to conceal the real IP address and greatly improve performance by creating a scalable environment. This capability is also used to direct requests, based on content to the appropriate server. Additionally this network level load balancing inherently provides intra-site and inter-site fail-over at the network level. Additionally, the AFIS/VSS servers send responses to virtual servers. These are critical requirements that must be supported by the Contractor’s AFIS renewal solution proposed to satisfy the requirements in this SOW.

2.4 CURRENT HIGH LEVEL RTID ARCHITECTURE

1. The following high level RTID architecture depicts the RTID components. It is presented herein to show the relationship between the RCMP/SSC conceptual security architecture, the RTID components and the architecture diagrams for the AFIS components that follow in the next section.
2. A brief description of each component was provided in the Appendix A SOW for this AFIS Renewal.

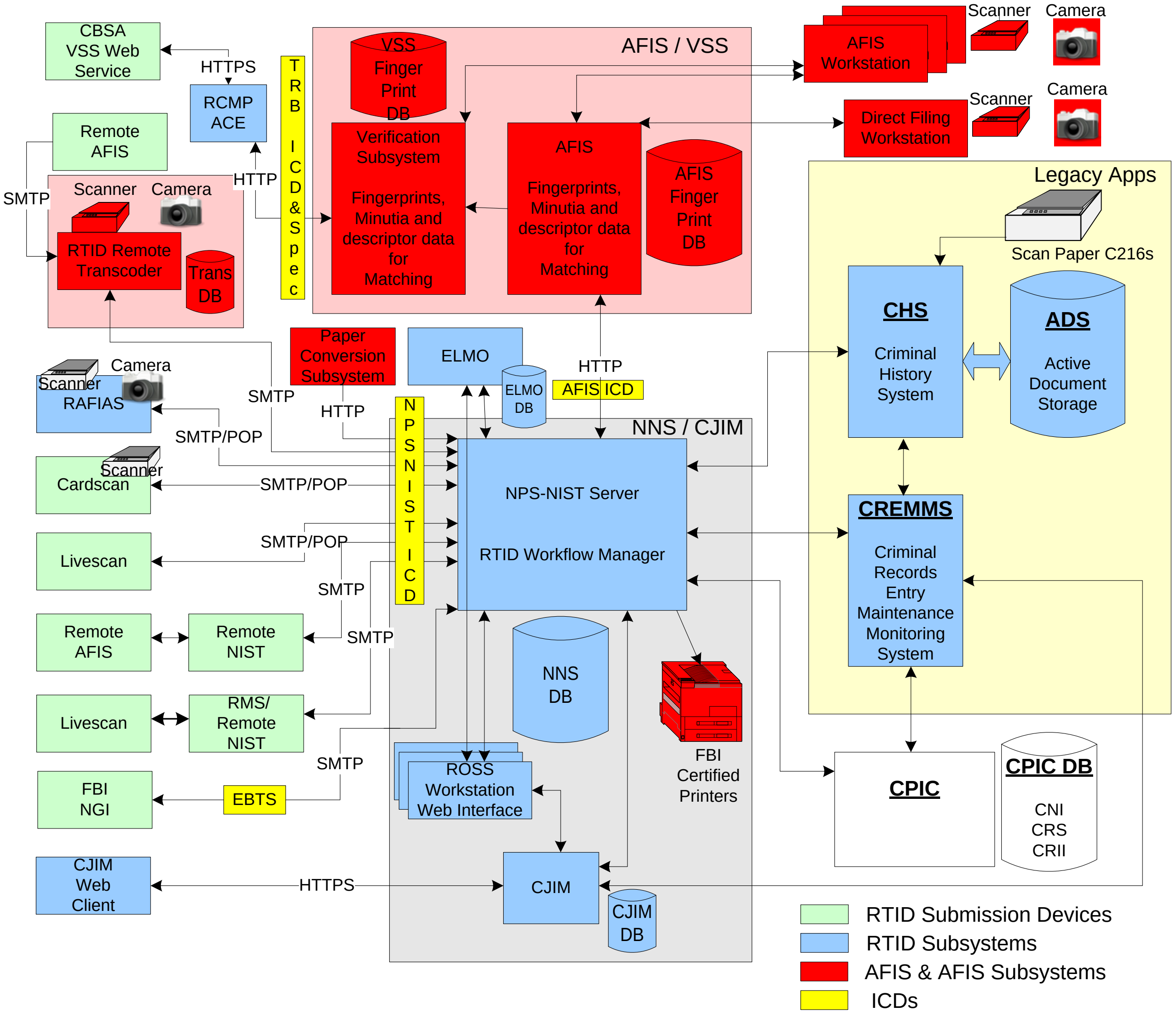

Figure 2: Current RTID High Level Architecture

3. AFIS & VSS ARCHITECTURE

3.1 AFIS & VSS TRB CONCEPTUAL ARCHITECTURE

1. The following diagram depicts the conceptual architecture for AFIS and VSS. This diagram specifically depicts CIC as the contributor of fingerprints that are enrolled; however, this is the common RTID interface used by other contributors.

2. CIC capture fingerprints for individuals seeking entry to Canada. CIC submit Immigration (IMM) NIST packets with the individuals fingerprints and a unique identification number. These fingerprints are enrolled in AFIS and a copy of the fingerprints is sent to VSS. When the individual arrives at a Port Of Entry (POE), CBSA capture the individual's fingerprints with their unique identification number and transmit the Verification (VER) NIST packet to VSS for comparison against the fingerprints previously captured by CIC.

3. Any purges (Immigration Purge - IMP) submitted by CIC will also purge the fingerprints from VSS.

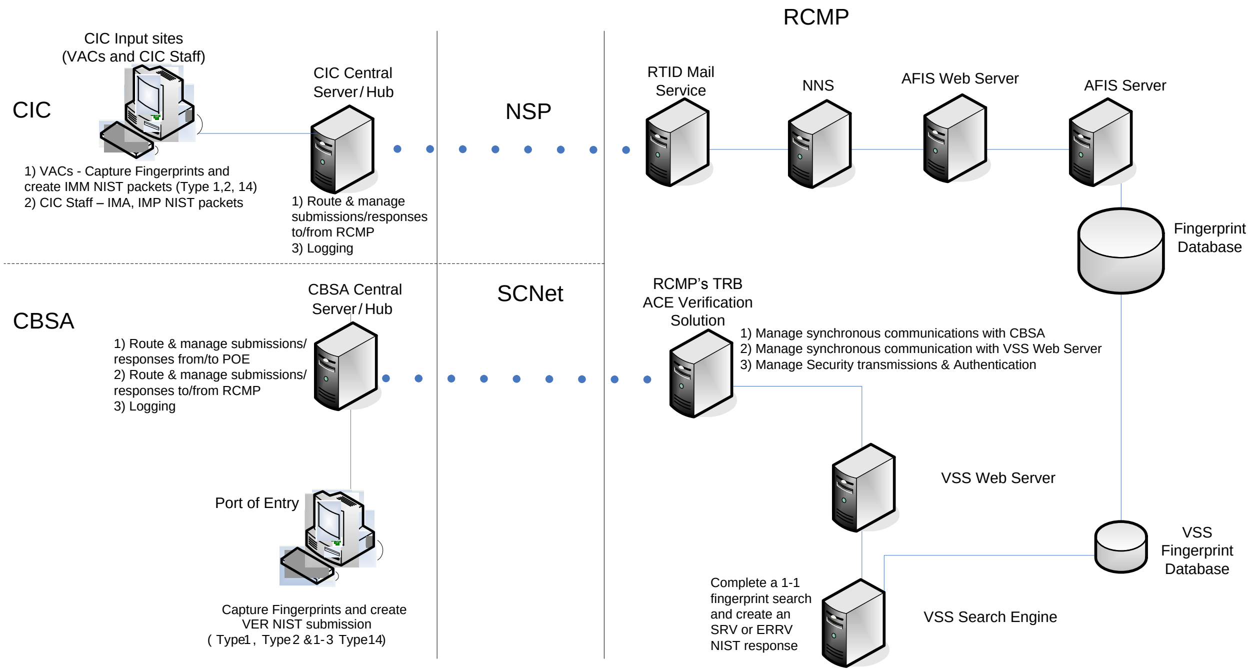

Figure 3: RTID/AFIS/VSS CIC/CBSA Conceptual Architecture

3.2 AFIS & VSS HIGH LEVEL ARCHITECTURE

1. The following diagram depicts the high level architecture of AFIS and VSS as well as the RTID components with which they interface. The RTID solution is designed based on ICDs and the ability to add or replace components based on adherence to the ICD.

2. AFIS and VSS can operate independently with the exception that fingerprint enrolments, purges or other updates are only through the AFIS; and AFIS communicates the TRB related fingerprints, purges and updates to VSS. That is, AFIS can operate without VSS; however, AFIS updates to VSS will be queued until VSS is online. As well, VSS can operate without AFIS; however, no enrollments, purges or updates will be received without AFIS.

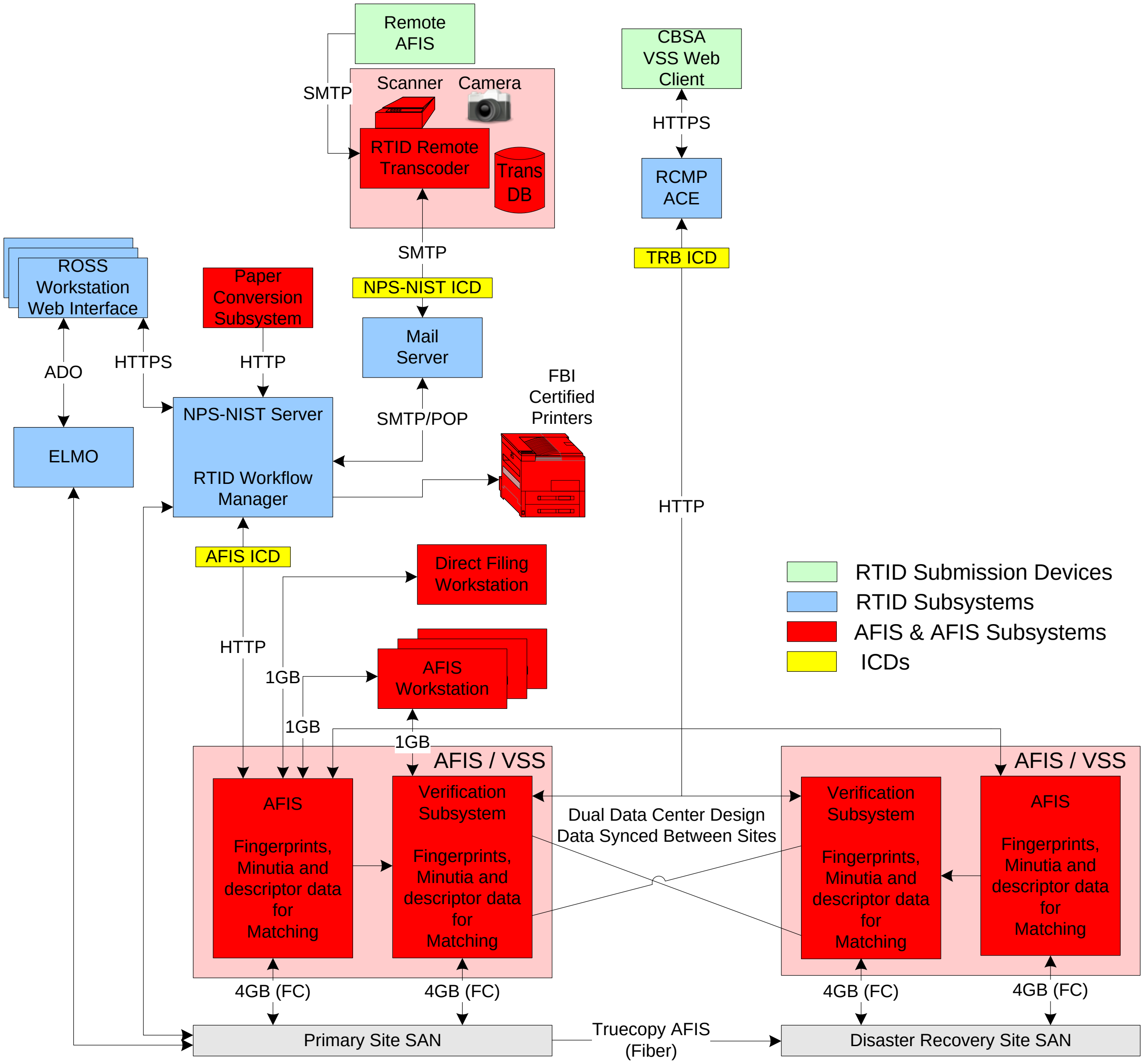

Figure 4: AFIS and VSS High Level Architecture

3. AFIS is designed as a semi-automatic fail-over Disaster Recovery (DR) site solution. Production AFIS components are operating at both the Primary (PR) site and the DR site. All required AFIS DB and file system files are mirrored to the DR site. In case of a disaster, AFIS will be restarted using the AFIS components at the DR site. The entire RCMP/SSC security/network infrastructure automatically fails over to the DR site therefore allowing the AFIS components to interface with any available RTID components. The AFIS DR components are in the same security zone as the PR components; therefore, the security architecture is maintained across both sites.
4. VSS is designed as a dual data center model with an automatic fail-over DR site solution. VSS components at both the PR and DR sites are fully utilized to maximize the capabilities of all components to satisfy the performance requirements. As depicted in the above high level architecture, the RCMP/SSC ACE load balances evenly to both the PR and DR sites. In case of a disaster, VSS will simply operate with the VSS nodes at the DR site. The entire RCMP/SSC security/network infrastructure automatically fails over to the DR site; therefore, Production CBSA VSS contributors would not know that the PR site was inoperable. Regardless of whether it is the PR or DR site that is out of service for a period of time, both sites will resynchronize each other automatically to ensure that both sites have the same data. This resynchronization occurs as soon as the service is restored and typically completed within five-ten (5-10) minutes. As a dual data center model VSS components fully operate within the same security zone as AFIS.
5. All AFIS workstations have one (1) GB connections.
6. AFIS and VSS servers have four (4) GB connection to the SAN.
7. There is fiber optic cabling between the PR and DR site.

3.3 AFIS AND VSS TEST ENVIRONMENTS

3.3.1 GENERAL

1. RTID Test environments include AFIS, VSS, NNS and all other components required to test any RTID changes destined for the Production environment.
2. There are three AFIS test environments, DEVTEST, Quality Control Section (QCS) and MAINT. Each AFIS test environment can support multiple RTID NNS environments.
3. The AFIS DEVTEST and MAINT environments support multiple NNS environments. This special configuration is available in all test environments; however, typically it is only used in the AFIS DEVTEST and MAINT environments.
4. The AFIS DEVTEST environment supports multiple NNS Integration environments, multiple NNS SYSTEST environments, multiple NNS performance environments and multiple individual developer environments. The special configuration enables the DEVTEST AFIS to interface with individual developer environments or to an NNS environment. This is a critical capability that allows developers to interface with the AFIS DEVTEST environment to satisfy their specific test/development requirements; and to complete development and release testing of the AFIS changes together with the NNS portion of RTID.

5. The RTID SYSTEST1 environment is used to test any RTID changes destined for the Production environment through the normal release process. SYSTEST1 is the primary test environment for all RTID components. Once successfully tested in the SYSTEST1 environment, changes will be tested in the RTID QCS environment.
6. The AFIS QCS environment supports one RTID NNS QCS environment. The AFIS QCS environment is configured with every possible AFIS components operating in the Production environment. The AFIS components in QCS allow for every possible Production issue to be tested. That is, at least one AFIS component exists in the QCS environment for every unique type of components in the Production environment to ensure every possible Production issue can be verified and the correction tested effectively.
7. The AFIS MAINT environment primarily supports an NNS Maintenance and Certification environment; however, it is capable of supporting additional environments.
8. The AFIS MAINT environment primarily supports an NNS Maintenance and Certification environment; however, it is capable of supporting additional environments. The Certification environment is used to certify vendor and contributor systems against the NPS-NIST ICD and the TRB ICD. Consequently, the NNS Certification environment has the same version of NNS software as Production. The NNS Certification environment is updated two (2) weeks after an NNS Production release. The NNS Maintenance environment has the same version of NNS software as Production until one (1) week prior to an NNS production release.
9. For AFIS and VSS releases, the AFIS MAINT environment is used to install, configure and implement new AFIS and VSS releases and changes prior to implementation in the AFIS DEVTEST environment. This ensures AFIS and VSS changes are initially tested against stable NNS software. Two weeks after successful deployment to Production any AFIS changes required during the release testing process are deployed in the AFIS MAINT environment.
10. Each AFIS environment is configured with the quantity of workstations and Transcoders necessary to effectively test any changes. The following diagrams depict the number of workstations/Transcoders in each environment.

3.3.2 AFIS AND VSS DEVTEST

1. The following diagram depicts the AFIS DEVTEST environment architecture.

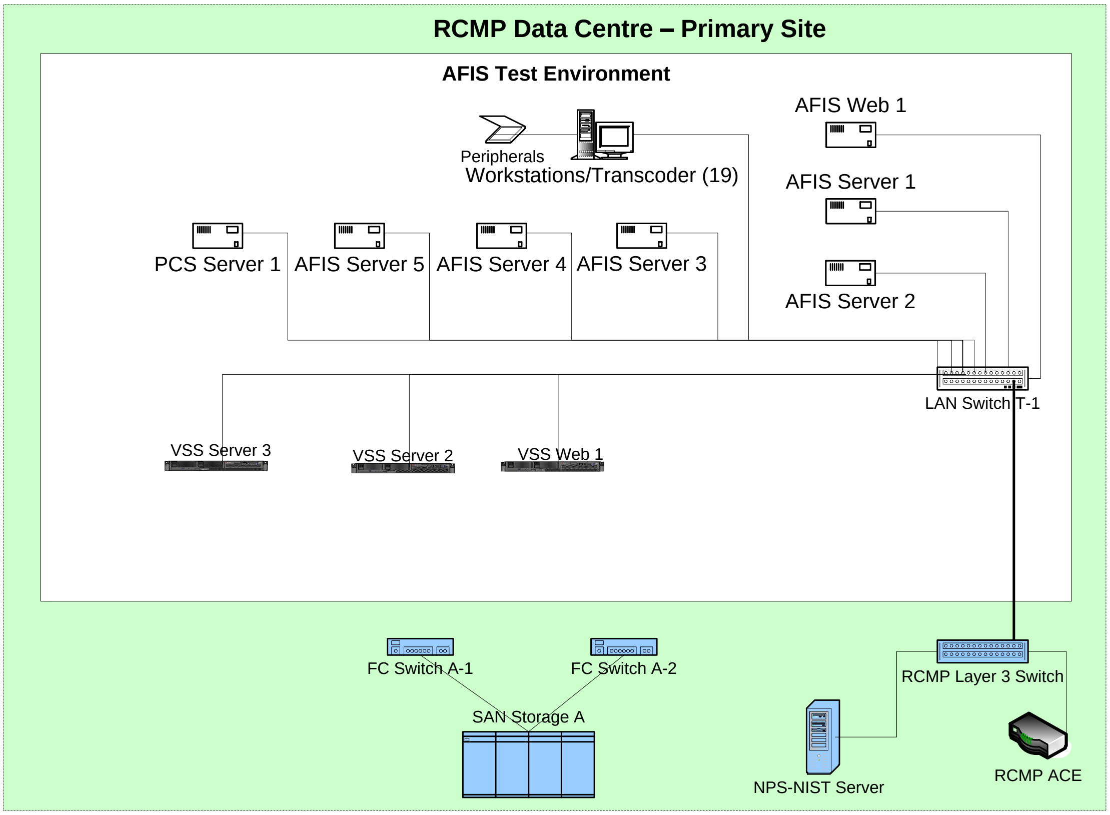

Figure 5: Development & Test Environment

2. The interface between the NNS and AFIS system is through the NNS Web server capability and the AFIS Web servers.

3. The RCMP/SSC’s Application Control Engine (ACE) provides a secure connection between CBSA and RCMP for the VSS. The ACE is also used to interface with the VSS Web server and together with the VSS Web server maintain a synchronous connection that provides results from the VSS Web server to CBSA. CIC and CBSA perform ongoing testing in the RTID test environments. They require the interface to test any changes to their systems or changes to RTID that potentially affect them. As well, other agencies occasionally test in the RTID test environments. All external agency access to the test environments is also through one of the secure connections previously identified. These external agency test connections are configured as Production controlled interfaces even though they access test systems.

4. Refer to the TRB Verification Interface Specifications PDF (RDIMS #39155) for details concerning the interface between CBSA, the ACE and the Contractor’s VSS Web servers.

Note: For proprietary reasons only generic names for the servers are used in the diagrams.

3.3.3 AFIS AND VSS QUALITY CONTROL SECTION (QCS)

1. The QCS environment is used for QCS testing to confirm the operational readiness and stability of any changes prior to implementation in the Production Environment. Successful testing in this environment is required before implementation of the change/release in the Production environment. This QCS environment is the only test environment with High Availability (HA) configurations that allow failover/redundancy capabilities to be tested.
2. The following diagram depicts the QCS architecture.

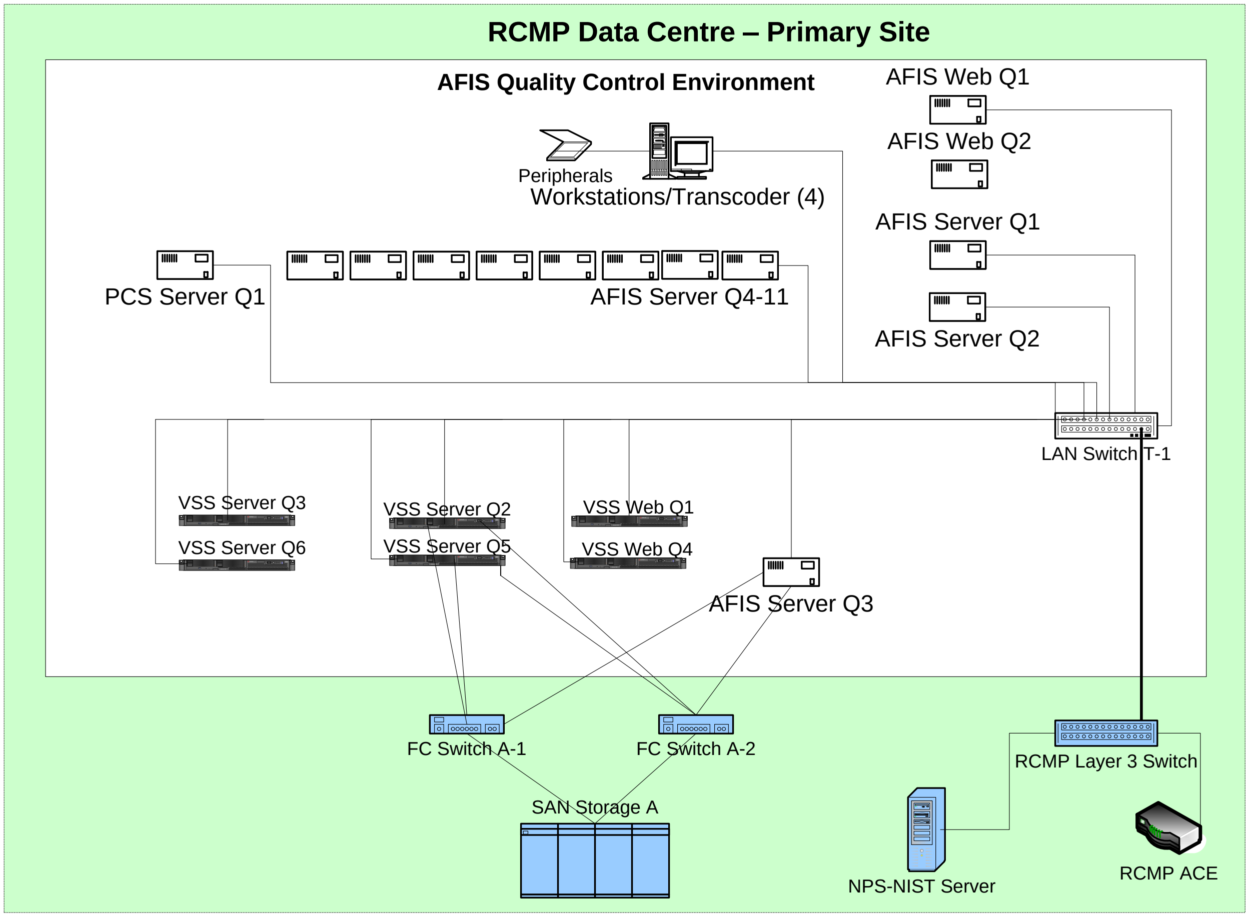

Figure 6: Quality Control Environment

1. The interface between the NNS and AFIS system is through the AFIS Web server.
2. The two AFIS Web servers in this QCS environment allow automated HA testing to be performed that allows services to fail-over between Web servers.
3. There are three (3) sets (two (2) of each type) of latent fingerprint matching components that allow various HA scenarios to be tested for latent processing.
4. The VSS servers are configured as two (2) nodes (with four (4) nodes configured in production), allowing multiple node HA testing to be performed to allow the production solution to be effectively tested in the QCS environment.

5. The QCS VSS connection is only tested with an internal client that simulates the CBSA connection. RCMP/SSC's ACE provides the secure connection between the internal client and VSS in the same manner as it does for the CBSA connection. The ACE is also used to interface with the QCS VSS Web servers, load balance traffic between the two (2) VSS Web servers and maintain a synchronous connection that provides results from the VSS Web servers to the internal client.
6. The RCMP/SSC's ACE is also used to provide load balanced communication from NNS to AFIS, from AFIS to NNS and between AFIS components to create a scalable HA configuration through the RCMP/SSC's network infrastructure.
7. There are a few scenarios for which HA testing cannot be performed in the QCS environment. These scenarios involve one (1) component that fully satisfies the requirements at a site or a proprietary mechanism to fully utilize the devices without requiring infrastructure load balancing or network level fail-over. For example Ten-Print (TP) fingerprint processing uses one (1) device to fully support the capacity requirements for RTID at a site; therefore, there is no infrastructure load balancing. There is also one (1) TP device at the DR site which is fully utilized through a proprietary mechanism. Since this fail-over is tested yearly and the TP HA test requires an RCMP/SSC infrastructure fail-over to effectively test, it is not tested in the QCS environment. Additionally, cluster fail-over testing of AFIS functional servers are only tested in Prod. Since the DR AFIS functional servers are only used in case of a failure, these DR servers can be used to test any cluster related issues without affecting production operations.

Note: On a yearly basis RCMP/SSC performs a complete DR site fail-over where the network and all applications are verified to operate at the DR site. This yearly test is used to test all AFIS and VSS fail-over to ensure all capabilities operate at the DR site. This allows AFIS and VSS HA capabilities that cannot be tested in the QCS environment to be tested with the RCMP/SSC network infrastructure fail-over and AFIS DR operation with the SAN mirrored database and file system data.

3.3.4 AFIS AND VSS MAINTENANCE

1. The NNS Maintenance and Certification environments have the latest release of NNS and all other non-AFIS components enabling AFIS changes to be verified against the current production release that matches the production environment. For AFIS and VSS releases, the AFIS Maintenance environment is used to install, configure and implement new AFIS and VSS releases and changes prior to implementation in the DEVTEST environment.
2. This AFIS Maintenance environment is used to verify the Contractor changes function as designed and ensure the Contractor components continue to interface correctly with the NNS. Successful testing in this environment is required before implementation of the release in the DEVTEST environment.
3. The following diagram depicts the Maintenance architecture.

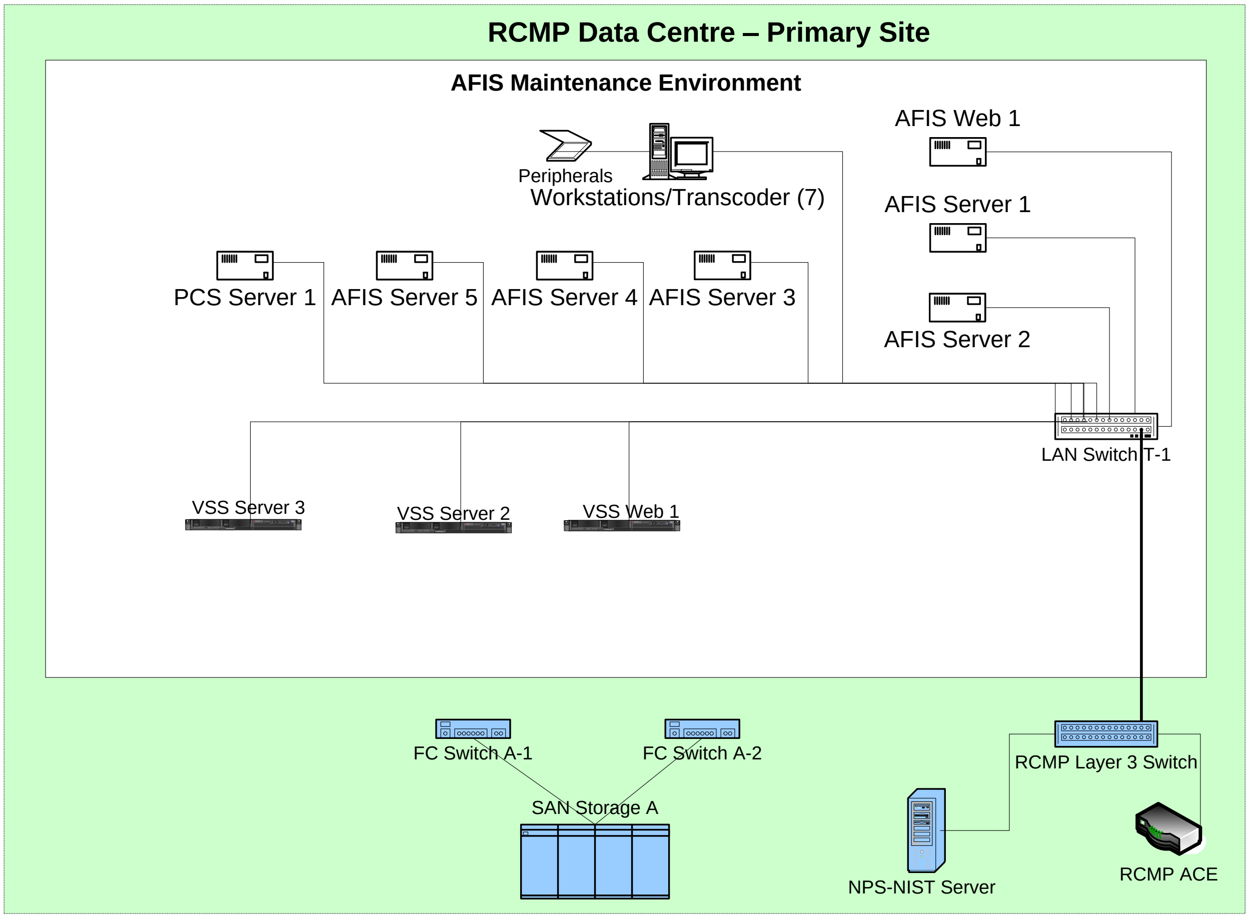

Figure 7: Maintenance Environment

4. The interface between the NNS and AFIS system is through the NNS Web server capability and the AFIS Web servers.
5. The RCMP/SSC's Application Control Engine (ACE) provides a secure connection between CBSA and RCMP for the VSS. The ACE is also used to interface with the VSS Web server and maintain a synchronous connection that provides results from the VSS Web server to CBSA. On an exceptional basis, CIC and CBSA will test in the Maintenance environment when the DEVTEST environment cannot be used to effectively support the conditions under which they need to test.

3.4 AFIS AND VSS PRODUCTION ENVIRONMENT

3.4.1 GENERAL

1. The AFIS and VSS production environment includes a Primary (PR) Production site and a Disaster Recovery (DR) site that supports all RTID AFIS and VSS production capabilities. The following diagram depicts the PR/DR architecture.

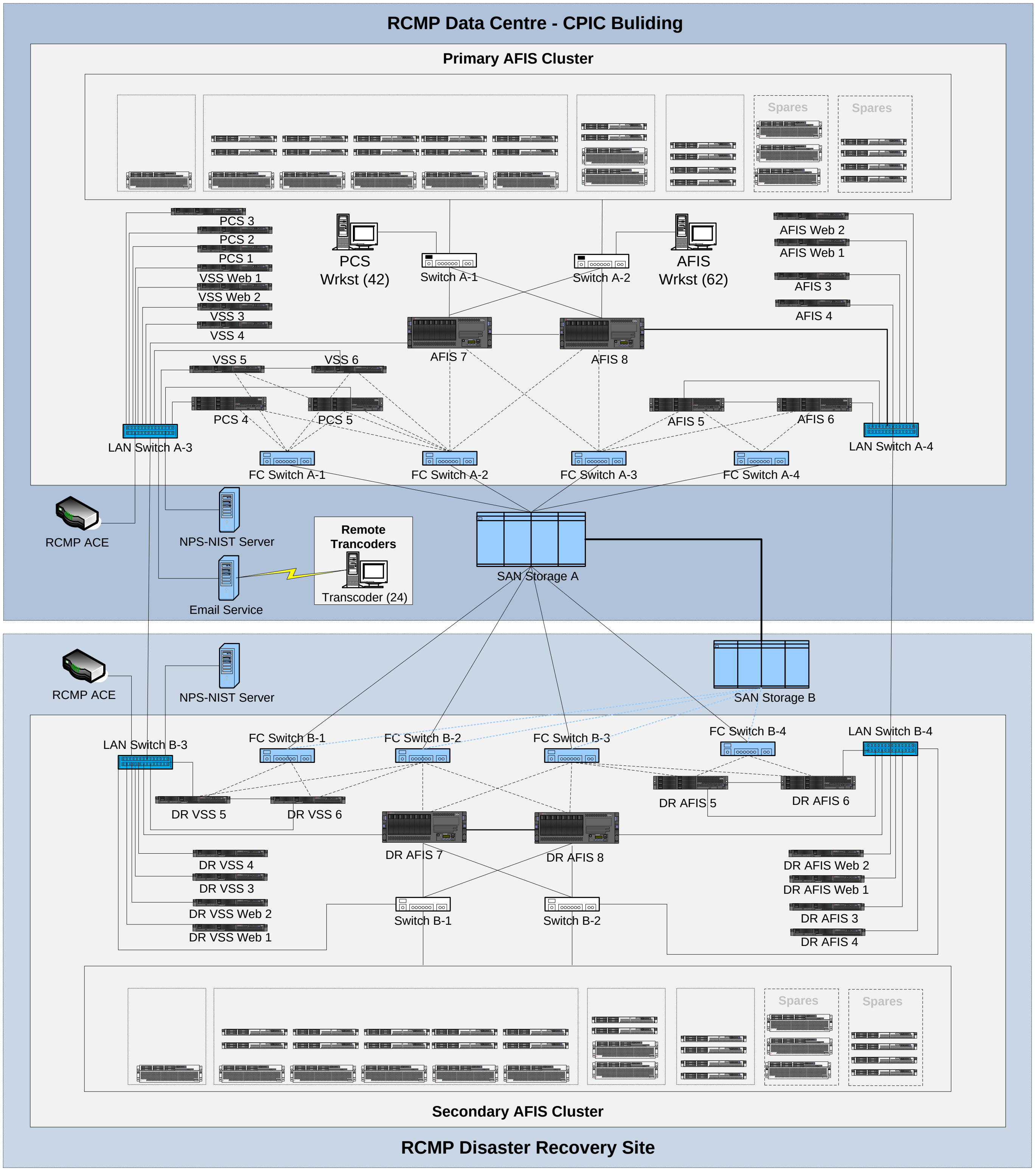

Figure 8: Production Architecture

2. All AFIS PR and DR matching components are fully utilized as part of normal operations. This creates a pseudo dual data center architecture where all matching components at both sites are utilized. The DR Web servers and the DR AFIS functional servers are only used if the PR fails and operations have to be re-established at the DR site with the SAN mirrored data. In case of a PR site failure, the DR Web and DR AFIS functional servers would use the fingerprint matching components at DR only.
3. VSS is a fully automated dual data center architecture that utilizes all servers at PR and DR and does not require any manual intervention to recover from a site failure. The integrated database exists at both the PR and DR sites enabling each site to work together or independently in case of a failure. The sites automatically resynchronize the integrated database once both sites are operational.

3.4.2 PRODUCTION PRIMARY (PR) SITE

1. The PR environment is used to support the production operational environment of AFIS and VSS. The PR/DR supports HA configurations that allow failover/redundancy capabilities within each site and between sites to ensure there is no single point of failure.
2. The interface between the NNS and RTID AFIS is load balanced through the ACE to the AFIS Web servers. The interface between the AFIS and NNS is load balanced through the ACE to the NNS Web servers
3. The two AFIS Web servers at the PR site provide HA capability. As well, all other AFIS functional servers are configured as pairs to provide HA capabilities within each site.
4. The PR site AFIS functional servers utilize all matching components (excluding live spares) at both the PR and DR site providing HA capabilities.
5. The RCMP/SSC's ACE provides a secure connection between CBSA and RCMP for the VSS. The ACE is also used to load balance and interface with the PR and DR VSS Web servers; and maintain a synchronous connection that provides results from the VSS Web server to CBSA. This VSS architecture is an automated dual data center configuration providing HA capabilities within a site and between sites.

3.4.3 DISASTER RECOVERY (DR)

1. The DR is configured with all the same servers as PR except for the PCS. As well, there are no workstations or other peripherals at the DR site. Workstations and other peripherals can easily be installed and configured to support DR only operations.

3.5 TEST AND PRODUCTION ENVIRONMENT RCMP/SSC INTEGRATION

3.5.1 GENERAL

1. The AFIS and VSS test and Production environments are integrated with RCMP/SSC maintenance and support capabilities. This integration is critical to the effective operation of AFIS and VSS within the RCMP/SSC infrastructure. The following subsections identify capabilities that the RCMP/SSC infrastructure supports for all AFIS and VSS test and Production environment components.

3.5.2 BACKUP AND RESTORE

1. RCMP/SSC has comprehensive backup and restore capabilities that are used by the AFIS and VSS databases and file system data. These capabilities include Tivoli Storage Management (TSM) and SAN mirroring.

3.5.3 SNMP REPORTING

1. All AFIS and VSS servers support SNMP reporting capabilities. Production and QCS environment servers have enabled reporting to RCMP/SSC's Spectrum/eHealth system monitoring solution. Additionally, some DEVTEST and MAINT servers also have enable reporting to RCMP/SSC's Spectrum/eHealth to ensure test servers are monitored allowing uninterrupted DEVTEST and MAINT environment services.
2. This SNMP reporting includes automated system level monitoring capabilities at the hardware and software application level, capable of producing SNMP traps/alerts when software or hardware faults are detected. The minimum SNMP reporting includes memory utilization, CPU utilization, disk utilization, key process failures and hardware faults.

3.5.4 MCAFEE ANTI VIRUS (AV) SCANNING

1. All AFIS and VSS servers and workstations, in all environments, receive automatic AV updates from the RCMP/SSC McAfee AV scanning through participation in ePo (ePolicy Orchestrator), with rare exceptions where the updates are completed manually in a manner approved by the RCMP with a configuration management documented history of the updates. These rare exceptions are for specialized components where the AV updates are verified in the QCS environment prior to updating the Production environment.

3.5.5 OS AND SOFTWARE UPGRADES

1. All AFIS and VSS Windows servers and workstations/transcoders, in all environments, receive Windows OS updates in an automated manner from RCMP/SSC Windows Server Update Services (WSUS). Workstation WSUS updates are forced within a specific timeframe if the user does not allow the updates to be completed prior to the time limit. Servers automatically receive the updates and AFIS and VSS support staff complete the updates during off hours.
2. For all non-Windows servers, RCMP/SSC provides approved patches and upgrades for the OS/ common software which is used to update the AFIS and VSS non-Windows servers. The AFIS and VSS support staff complete the updates during off hours.

3.5.6 DESIGNATED SPECIAL PORTS

1. The AFIS and VSS servers are also configured to use designated ports for various types of connectivity based on RCMP/SSC policy.

ANNEX A-1 - LIST OF DEFINITIONS

The purpose of this annex is to define the terminology used within this Statement of Requirements.

Table A-1.1: List of Definitions

Term	Definition
AFIS ICD	The AFIS ICD contains the NIST transactions that are used to communicate with the AFIS. This interface standard allows the RCMP to maintain independence from the proprietary AFIS yet communicate all of the necessary information required to request fingerprint searches.
AFIS Subject ID	A unique identifier assigned by the RTID AFIS system to a Subject (person) enabling the linkage of all fingerprints, regardless of file type, to the Subject.
Audit Log	A list of predetermined system related events for which the RCMP needs to record when, where and why, whatever happened and by whom, to ensure an historical record of those events are captured.
Auto Certification	An RTID AFIS configuration that allows for a Ten Print “lights out” or automatic confirmation of a fingerprint match of a candidate fingerprint to an existing subject on RTID AFIS.
Biographic Data	This term refers to alpha and numeric type data contained within a TR Submission. Examples include; Name, Date of Birth, Sex.
Configurable Parameter	Refers to a parameter that can be adjusted by a User who possesses the appropriate level of authorization. Configurable parameters typically refer to a system defined function, such as an SLA, retention period for files, etc.
Contributor	An authorized agency that submits requests for service to CCRTIS. Examples of requests for service include Criminal Retain (CAR-Y), Criminal Inquiry (CAR-N), Civil (MAP), Refugee (REF) and Temporary Resident (IMM) submissions.
CPIC (Query)	In the context of TRB, the only CPIC query transaction required is Q-CNI (Criminal Name Index). It is a CPIC transaction that can execute when the weekly CPIC maintenance data unload is running.
Fingerprint Biometric Data	This term refers to fingerprint images contained within a TR Submission.
IID Number (Immigration Identification Number)	The Immigration Identification File Number is the unique key generated by the RCMP under which Temporary Resident data is stored within the RCMP. • An IID Number, once purged, will never be reused.

Table A-1.1: List of Definitions

Term	Definition
Interface Control Document (ICD)	A specification for interfacing with a (legacy, internal or external) Subsystem, system or service. • ICDs and related documents that are relevant to the TRB project include: • Internal ICDs (e.g., AFIS ICD and IIS ICD); • External ICDs (e.g., NPS-NIST ICD for external contributors); and • ICD Transformation and FBI Conversion Specification.
NPS NIST ICD	The term National Police Services NPS NIST ICD is used to refer to the External NPS-NIST ICD version that includes the TR types of transactions and updates to existing transactions that will be used to support the TRB Project. The following new Transaction Types will be added: • TR Enrolment - IMM • TR Amend - IMA • TR Purge - IMP • TR Verification - VER • TR Purge Response - IMPR • TR Amend Response - IMAR • Search Response Verification – SRV • Verification Error Response - ERRV The following existing Transaction Types will be modified to support TR processing: • Search Response – SRE • Image Request – IRQ • Image Request Response - IRR • Ten Print Acknowledge Response – ACKT • Ten Print Error Response – ERRT
One to One (1:1) Verification	For purposes of verification at a CBSA Port of Entry, this term denotes the comparison of submitted fingerprints to the corresponding subject's enrolled fingerprints (referenced by the IID Number) stored on the TR Subject File and TR Subject Repository.
ORI	The Originating Agency Identifier (ORI) is a seven (7) digit alpha-numeric identifier used by the system to identify an agency that has submitted a submission to the RCMP.

Table A-1.1: List of Definitions

Term	Definition
Submission	A request for service initiated by an external contributor to add, retrieve, amend, remove or search for information held in the Royal Canadian Mounted Police (RCMP) National Fingerprint Repository. A submission may contain one or more transactions. For Example; an Enrolment contains the following transactions: • an IMM; • if applicable an ERRT; • an ACKT; and • an SRE.
System Availability	Availability is defined as the system's ability to receive and acknowledge a TR Submission. Availability is measured on a monthly basis. It does not apply to peripherals such as workstations or printers.
TR Subject	The applicant identified in an application for a Temporary Resident Visa and/or Temporary Resident Work/Study Permit.
TR Subject File	This term refers to the Temporary Resident biographic information created and retained in the RCMP biographic database for a TR Subject as well as the corresponding fingerprint image data on the TR Subject repository.
TR Subject Repository	This term refers to the Temporary Resident biometric fingerprint information created and retained in the RTID AFIS.
TR Submission	This term refers to a Temporary Resident transaction received by the system. Unless otherwise specified it is used to refer to the TR Enrolment (IMM), TR Amend (IMA), TR Purge (IMP) and TR Verification (VER) Submissions.
TR Submission Data	This term refers to the Temporary Resident information created as a result of processing each TR submission. Examples include; Activity Log Entries, Status Histories and Internal Transactions to RTID AFIS as well as other Subsystems etc…
TR Verification Repository	This term refers to the Temporary Resident biometric fingerprint encoding (minutiae) created and retained in the RTID AFIS for Verification purposes. It also includes the image data and biographical information.
Transaction	This term refers to a defined interaction within a submission. An exchange of information with the system or a sub system.

Table A-1.1: List of Definitions

Term	Definition
Type-14 ID Flats	The term Type-14 record is an NPS NIST ICD defined standard format that can be used to share fingerprint ID Flat images which are acquired by a subject placing their fingers on a fingerprint capture device without the need to roll the finger to capture a complete fingerprint image. These types of images are sometimes referred to as “slaps”. The RCMP definition or standard for “ID Flats” requires 1 to 3 of the following images. • Right Four Fingers • Left Four Fingers • Two Thumbs
User(s)	The term User or Users refers to CCRTIS Authorized User(s) that have been provided access to the function or User Interface referred to in these requirements.
Verification (Fingerprint)	Comparing a candidate set of fingerprints to one respondent matches in the RTID AFIS database.
Verification Subsystem	The term Verification Subsystem is defined as all the components required to fully support all Verification Subsystem requirements.
Work in Progress	The term Work in Progress (WIP) is defined as the time period from receipt of the submission to Completion of Service plus a buffer period. The Buffer Period is a system configurable number of days based on the submission type. For example a TR enrolment may be kept for 30 days after completion of service prior to data clean-up.
Work in Progress (WIP) Data	The term WIP Data is the data that is produced as a by product of TR related processing. Examples include; Name Search Iterations, Name Search Results, File Status Query Results, Activity Log entries etc…

ANNEX A-2 – LIST OF ACRONYMS

Table A-2.1: List of Acronyms

Acronym	Definition
ACKT	Acknowledgement Transaction
AFIS	Automated Fingerprint Identification System
ANSI	American National Standards Institute
ATP	Acceptance Test Plan
ATR	Acceptance Test Report
BSO	Border Services Officer
CBSA	Canada Border Services Agency
CCRTIS	Canadian Criminal Real Time Identification Services
CDRL	Contract Deliverables Requirement List
CIC	Citizenship and Immigration Canada
CIO	Chief Information Officer
COG	the Contractor Change Request
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf System
CPIC	Canadian Police Information Center
CSR	Contractor Status Report
DID	Deliverable Item Description
DCN	Document Control Number
EFCD	Electronic Fingerprint Capture Device
ERRIN	Internal Error Transaction
ERRT	Error Transaction
ERRV	Error on Verification Transaction
FBI	Federal Bureau of Investigation
ICD	Interface Control Document
IID	Immigration File Number
ILRI	Image List Retrieval
IMA	Temporary Resident Amend Transaction
IMAR	Temporary Resident Amend Response
IMM	Temporary Resident Enrolment Transaction

Table A-2.1: List of Acronyms

Acronym	Definition
IMP	Temporary Resident Purge Transaction
IMPR	Temporary Resident Purge Response
IRQ	Fingerprint Image Request
IRR	Image Request Response
MCS	Master Contract Schedule
NNS ICD	NPS-NIST External ICD
NPS	National Police Service
NIST	National Institute of Standards and Technology
ORI	Originator
PMA	Programmable Matching Accelerator
POE	Port of Entry
PRM	Progress Review Meetings
RCMP	Royal Canadian Mounted Police
RTID	Real Time Identification (system)
SDD	System Design Documentation
SIP	Site Installation Plan
SIR	RCMP Software/Solution Incident Report
SATP	Site Acceptance Test Plan
SATR	Site Acceptance Test Report
SLA	Service Level Agreement
SOW	Statement of Work
SRE	Search Response
SRV	Verification Search Response
STI	Status Transaction
TBD	To Be Determined
TCN	Transaction Control Number
TPAI	Ten Print Amend
TPCNI	Ten Print Consolidation transaction
TPCNRI	Ten Print Consolidation Response
TPDI	Ten-Print Delete Request

Table A-2.1: List of Acronyms

Acronym	Definition
TPQCI	Ten Print Quality Control Response
TPREI	Ten Print Request Response
TPRI	Ten Print Search Request
TR	Temporary Resident
TRB	Temporary Resident Biometrics
UI	User Interface
VER	Temporary Resident Verification Transaction
WI	RCMP Work Item replaces the term SIR; however, sometimes used interchangeably
WIP	Work in Progress