SRS (PRTTDCIS-3037)

~~SRS-279~~ Pooled Portable Rugged Spectrum Analyser shall be suited to all TDCIS Transmission Systems specifications to perform trouble shooting activities.

SRS (PRTTDCIS-4640)

~~SRS-280~~ Pooled Portable Rugged Spectrum Analyzer elements shall be composed of software and hardware components supporting physical troubleshooting on all Transmission Systems hardware components in base band and in Radio Frequency (RF) band.

SRS (PRTTDCIS-4641)

~~SRS-281~~ All Sys Admin Tent shall support the installation of a Pooled Tent ECU.

SRS (PRTTDCIS-4390)

~~SRS-282~~ All TDCIS Shelters shall support the installation of a Pooled Lifting Jacks Kit.

SRS (PRTTDCIS-4391)

~~SRS-283~~ The Pooled Maintenance Platforms shall be compatible with all PRT Shelters variants.

3.6 Implementation Constraints

SRS (PRTTDCIS-1222)

~~SRS-284~~ The TDCIS node design shall be modular and generic, built in common building blocks.

SRS (PRTTDCIS-1223)

~~SRS-285~~ Nodes shall be fitted only with those elements that are required.

SRS (PRTTDCIS-1840)

~~SRS-286~~ The Voice End User PFE baseline is composed of following models:

- Cisco 7942; and,
- Cisco 8865; and,
- Cisco 7861 (SIP); and,
- Cisco 8821 (Wireless IP Phone).

SRS (PRTTDCIS-4270)

~~SRS-287~~ The Contractor shall implement CAS variants as per following table:

Node	Security Domain	CAS Variant
AN	xU	Single Server
AN	xR	Software Defined
AN	xS	Software Defined
BCC	xU	Single Server
BCC	xR	SAN Based
BCC	xS	SAN Based
CCC	xU	Single Server
CCC	xR	Single Server
RAP	xU	Single Server
RAP	xR	Single Server
NS Kit	NS	Single Server

Table 24 - CAS variant per Node and Security Domain

SRS (PRTTDCIS-4515)

~~SRS-288~~ There shall be no DRS-xU implemented in RAP.

SRS (PRTTDCIS-3016)

~~SRS-289~~ On top of all services identified in the Contractor Design, the Contractor shall include the following PFE workload for COI Services to the CAS Subsystem design:

Node	Security Domain	vCPU	vRAM (GB)	Storage (GB)
AN	xU	20	56	1300
AN	xR	108	284	6800
AN	xS	112	292	7000
BCC	xU	20	56	1300
BCC	xR	108	284	6800
BCC	xS	112	292	7000
CCC	xU	12	24	300
CCC	xR	12	24	300
RAP	xU	12	40	1100
RAP	xR	20	56	1300

Table 25 - PFE Payload per Node and Security Domain

NOTE (PRTTDCIS-4269)

~~[102]~~ The PFE workload to the CAS Subsystem does not include oversubscription nor provision for growth.

SRS (PRTTDCIS-4404)

~~SRS-290~~ The Contractor shall implement LMM as per following table:

Node	Security Domain	LMM as an ISM Workload	LMM as a Sys Admin Workstation Workload
AN	BLK	-	Yes
AN	xU	Yes	Yes
AN	xR	Yes	Yes
AN	xS	Yes	Yes
BCC	BLK	-	Yes
BCC	xU	Yes	Yes
BCC	xR	Yes	Yes
BCC	xS	Yes	Yes
CCC	BLK	-	Yes
CCC	xU	Yes	Yes
CCC	xR	Yes	Yes
RAP	BLK	-	Yes
RAP	xU	Yes	Yes
RAP	xR	Yes	Yes
TN	BLK	-	Yes
TN	xU	-	Yes
RL	BLK	-	Yes
RL	xU	-	Yes
NS Kit	NS	Yes	Yes

Table 26 - CAS variant per Node and Security Domain

SRS (PRTTDCIS-4512)

~~SRS-291~~ Any TCE621 integration in rack shall include an opaque plate hiding the front panel of the TCE621 making any screen, LED, etc. invisible.

SRS (PRTTDCIS-4541)

~~SRS-292~~ TDCIS shall not implement TEMPEST inline power filters on BLK, xU and xR security domains.

3.7 Performance Targets

3.7.1 General

SRS (PRTTDCIS-2627)

~~SRS-293~~ Unless stated otherwise, all Performance Targets shall be met with TWO (02) trained System Administrators per Shelter.

SRS (PRTTDCIS-4090)

~~SRS-294~~ All TDCIS Elements shall survive a hard shut-down.

3.7.2 Deployability

SRS (PRTTDCIS-1947)

~~SRS-295~~ Any Node shall be teared-down in less than 30 minutes.

SRS (PRTTDCIS-2628)

~~SRS-296~~ Node Tear-down status shall be understood as all services and Transmission links properly shutdown.

SRS (PRTTDCIS-1948)

~~SRS-297~~ Any Node shall re-deploy in less than 90 minutes.

SRS (PRTTDCIS-2629)

~~SRS-298~~ Node re-deploy status shall be understood as ready for departure: all components are properly packed and stored for transport, Shelter is closed and securely mounted on the Vehicle, trailer is attached to the vehicle, vehicle motor running and people sitting in the cabin ready to take the road.

SRS (PRTTDCIS-1949)

~~SRS-299~~ Any Node shall be self-sustainable during 72 hours of regular operations without Logistic Supply Run.

SRS (PRTTDCIS-2622)

~~SRS-300~~ Radio Based xR Voice service shall be operational in less than 15 minutes after arrival on site.

SRS (PRTTDCIS-2623)

~~SRS-301~~ All services locally hosted in the Node shall be operational in less than 30 minutes after arrival on site.

SRS (PRTTDCIS-2625)

~~SRS-302~~ All Radio and SATCOM links (including mast and antenna raising) shall be operational in less than 45 minutes after arrival on site.

SRS (PRTTDCIS-2081)

~~SRS-303~~ The Military SATCOM Terminal shall deploy in no more than 15 minutes.

SRS (PRTTDCIS-4460)

~~SRS-304~~ Military SATCOM Terminal deployment time shall start from the moment antenna started to move from stowed position within line of sight of the satellite.

SRS (PRTTDCIS-2624)

~~SRS-305~~ All Inter-Node services (e.g. those hosted in or interconnecting with other nodes) shall be operational in less than 60 minutes after arrival on site.

SRS (PRTTDCIS-2626)

~~SRS-306~~ Any node shall have reached Full Operational Capability in less than 75 minutes after arrival on site.

3.7.3 Interoperability

SRS (PRTTDCIS-1215)

~~SRS-307~~ The TDCIS shall be compliant with the FMN Spiral 3 specification.

3.7.4 Power Supply

SRS (PRTTDCIS-2814)

~~SRS-308~~ The shelter UPS shall implement ability for all housed Elements in all security domains to continue to operate through:

1) Mains or generator power blackout for at least 30 minutes;
2) Mains or generator power brownouts indefinitely.

SRS (PRTTDCIS-2795)

~~SRS-309~~ The UPS in the NS Kit shall implement ability for the Core Node lite to continue to operate through:

1) Mains or generator power blackout for at least 20 minutes; and,
2) Mains or generator power brownouts indefinitely.

SRS (PRTTDCIS-4372)

~~SRS-310~~ The UPS in the NS Kit shall implement ability for the Remote Node lite to continue to operate through:

1) Mains or generator power blackout for at least 20 minutes; and,
2) Mains or generator power brownouts indefinitely.

SRS (PRTTDCIS-2282)

~~SRS-311~~ The GAR-T HCLOS relay variant UPS battery system shall be capable of providing sufficient power to operate all the equipment (i.e. radio system, masts, lighting, auxiliary equipment, etc.) for a period of 12 hours.

SRS (PRTTDCIS-2276)

~~SRS-312~~ The GAR-T HCLOS relay variant PGU shall be capable of providing sufficient power to all the GAR-T HCLOS relay variant systems including the electrical generator starter battery and GAR-T UPS battery banks for a minimum period of up to 24 hours on one full fuel tank.

3.7.5 Modularity

SRS (PRTTDCIS-1444)

~~SRS-313~~ The TDCIS shall be modular to allow the PRT Army to choose the operating capability for the deployment they are undertaking, by identify and configuring only the assets required for the specific mission.

SRS (PRTTDCIS-4239)

~~SRS-314~~ The CCC shall support conversion into a CCC Plus, hosting the full scale of services like in an AN and a BCC (only on xU and xR) though hardware augmentation from Pooled Elements and through configuration.

3.7.6 Environmental

SRS (PRTTDCIS-1366)

~~SRS-315~~ All TDCIS outdoor assemblies and sub-assemblies; such as, but not limited to, Housing Elements, CIS Elements (e.g. Antenna, Mast, ODU...)...; under full operational configuration, shall be capable of withstanding climatic and environmental conditions, without suffering degradation of system performance (gain, pattern type, sensitivity) and without suffering permanent mechanical damages, as stipulated operate under in TN-1078 for OPE-1a environmental conditions.

SRS (PRTTDCIS-2379)

~~SRS-316~~ All Access Breakout Box (BoB) shall operate in OPE-1c conditions.

SRS (PRTTDCIS-4642)

~~SRS-317~~ All Wireless Access Points shall operate in OPE-1a conditions.

SRS (PRTTDCIS-4268)

~~SRS-318~~ NS Kit shall operate in OPE-1c conditions.

NOTE (PRTTDCIS-3219)

~~[103]~~ All indoor PFE components (Radio, Amplifier...) to be integrated in Housing Elements are OPE-3 compliant and all outdoor PFE components (Antennas...) are OPE-1a compliant.

SRS (PRTTDCIS-4465)

~~SRS-319~~ End User Devices shall operate in OPE-1c conditions.

SRS (PRTTDCIS-4543)

~~SRS-320~~ System Administrator Helpdesk tool kit shall operate in OPE-1c conditions.

3.7.7 Security

SRS (PRTTDCIS-1149)

~~SRS-321~~ All CIS Nodes and Modules including electronic components processing classified information at SECRET level shall, as a minimum, be certified to TEMPEST Level B.

SRS (PRTTDCIS-1805)

~~SRS-322~~ TDCIS Elements shall, as a minimum, comply with TEMPEST requirements as per following table.

	Minimum TEMPEST
NS Kit - Core Node Lite	Level B
NS Kit - Remote Node Lite	Level B
Access BoB-xS	Level B
EUD - xS	Level B

Table 27 - TDCIS Elements TEMPEST levels

SRS (PRTTDCIS-4643)

~~SRS-323~~ Contractor shall privilege commonality of hardware in all Security Domains. Therefore, TEMPEST performances shall be met through the housing solution (Racks in Shelter and Transit Case).

SRS (PRTTDCIS-4644)

~~SRS-324~~ At the exception of AN, BCC and CCC, all Nodes marked as *Enabled* for xS Elements shall be delivered with standard racks (i.e. not providing required protection to meet TEMPEST performances).

NOTE (PRTTDCIS-4645)

~~[104]~~ Customer will take care of installing appropriate racks in those Nodes if they decide to install xS Elements in the future.

4 Services

4.1 Business Support Services

4.1.1 General

SRS (PRTTDCIS-1231)

~~SRS-325~~ The contractor shall design, implement, configure and deliver all necessary Network (e.g. DHCP, etc.), Infrastructure (e.g. AD, DC, DNS, etc.) and Platform (e.g. hypervisor, etc.) services necessary to support Business Support Services in line with industry best practices and compliant with security measures.

SRS (PRTTDCIS-2700)

~~SRS-326~~ Multiple services are linked to the Unified Communication and Collaboration (UCC) solution. The exact product reference to fulfill the role of the UCC tool which is interfacing to the user, here after named the *Collaboration Application*, is design driven.

SRS (PRTTDCIS-2887)

~~SRS-327~~ The *Collaboration Application* shall be a single software providing all functionalities specified for the services it supports.

SRS (PRTTDCIS-4646)

~~SRS-328~~ The Contractor shall deliver all necessary components (including licenses if any) for the *Collaboration Application* to be installed on every End User Workstation, for all Nodes and in all Security Domains applicable.

SRS (PRTTDCIS-2876)

~~SRS-329~~ Following Services shall rely on a common Global Address List (GAL) of users:

- Email Service; and,
- Collaboration Information Portal Service; and,
- Printing and Scanning Services; and,
- Video Teleconference Service; and,
- Voice Collaboration Service.

4.1.2 Email

SRS (PRTTDCIS-2897)

~~SRS-330~~ The Email Service design shall adhere to the implementation concept illustrated on the following figure for service instances hosted in a TDCIS Node and the NS Kit.

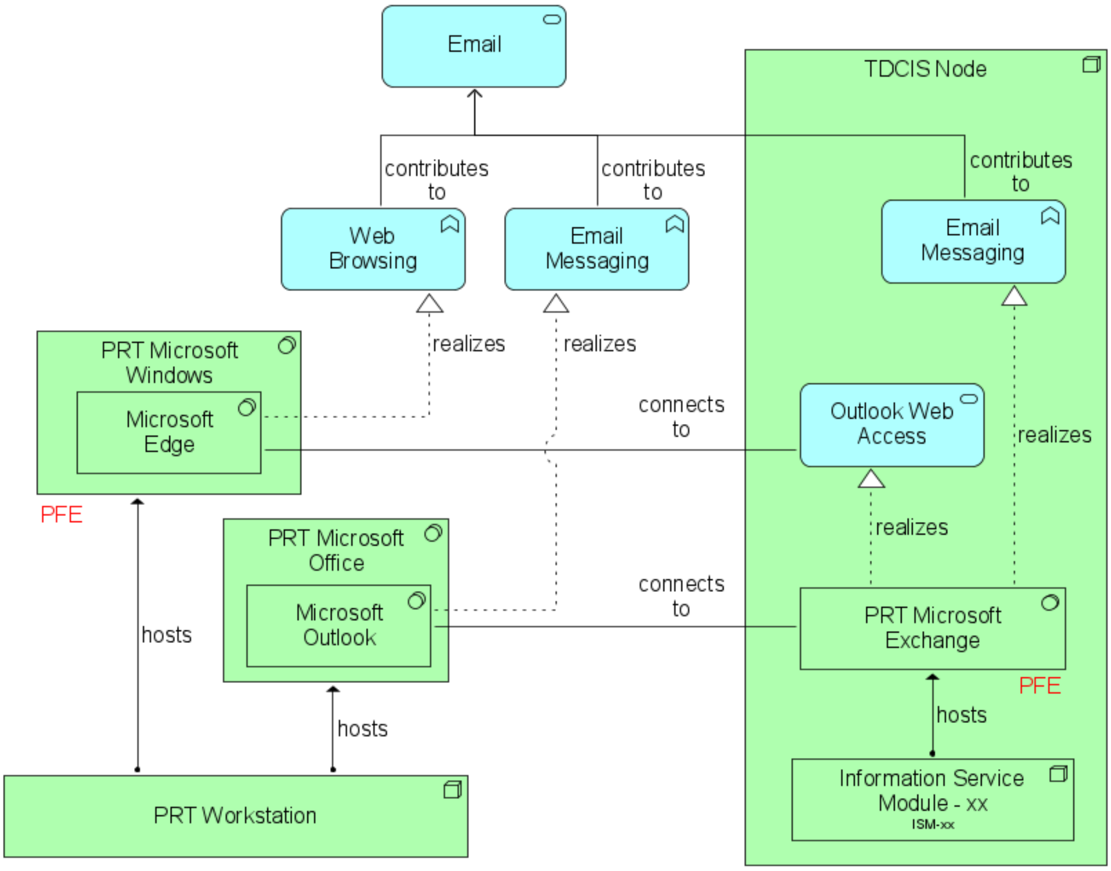

Figure 21 - Email Service implementation concept (TDCIS Node hosted)

SRS (PRTTDCIS-4272)

~~SRS-331~~ The Email Service design shall adhere to the implementation concept illustrated on the following figure for service instances hosted in PRT NDN.

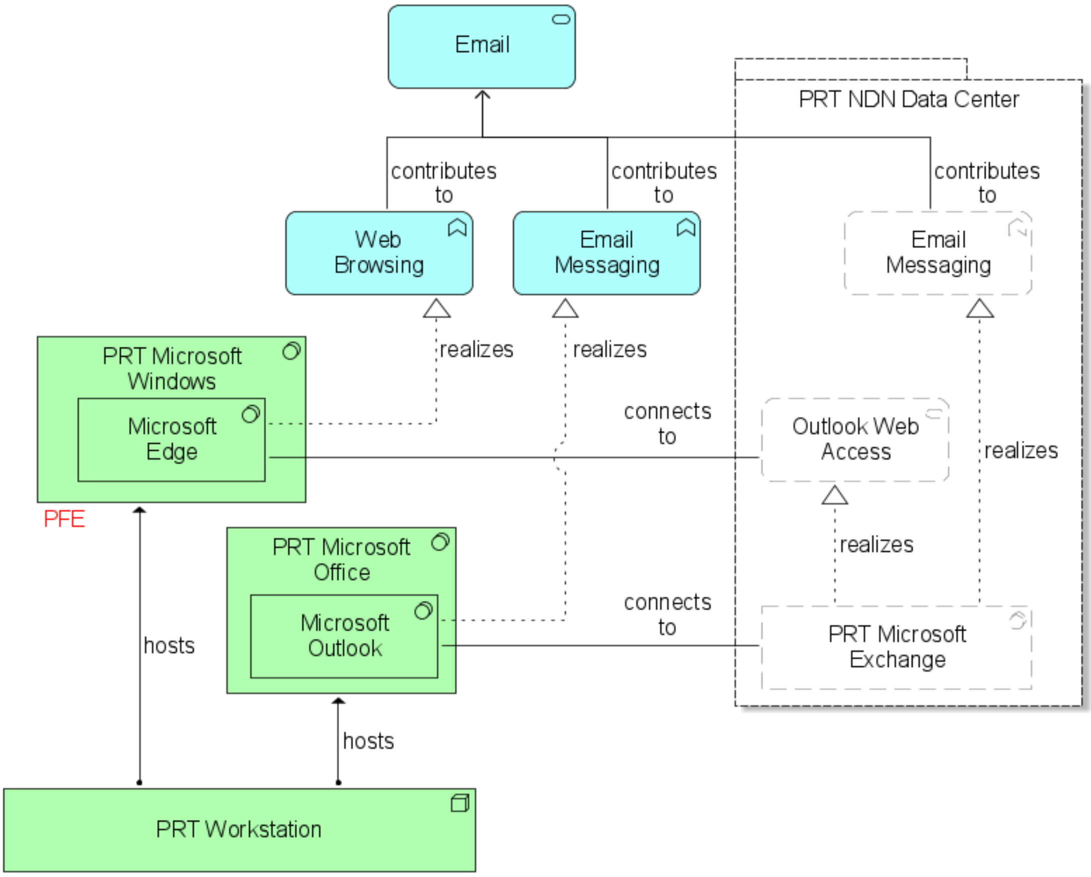

Figure 22 - Email Service implementation concept (PRT NDN hosted)

SRS (PRTTDCIS-4273)

~~SRS-332~~ Email Service shall be implemented using Microsoft Email solution as follow:

- Email Server implemented by Microsoft Exchange with Outlook Web Access; and,
- Email Client implemented by Microsoft Outlook.

NOTE (PRTTDCIS-4274)

~~[105]~~ Microsoft Exchange Licenses for TDCIS Nodes implementation are PFE.

SRS (PRTTDCIS-2911)

~~SRS-333~~ Each node user shall have a personal mailbox in each security domain present in the Node.

SRS (PRTTDCIS-2912)

~~SRS-334~~ Each TDCIS Nodes shall support up to 10 functional mailboxes per security domain present in the Node.

SRS (PRTTDCIS-2913)

~~SRS-335~~ Each Mailbox shall support up to 2.5GB of storage with an additional 10% of reserve.

4.1.3 Collaboration Information Portal Service

SRS (PRTTDCIS-2894)

~~SRS-336~~ The Collaborative Information Portal Service design shall adhere to the implementation concept illustrated on the following figure for service instances hosted in a TDCIS Node.

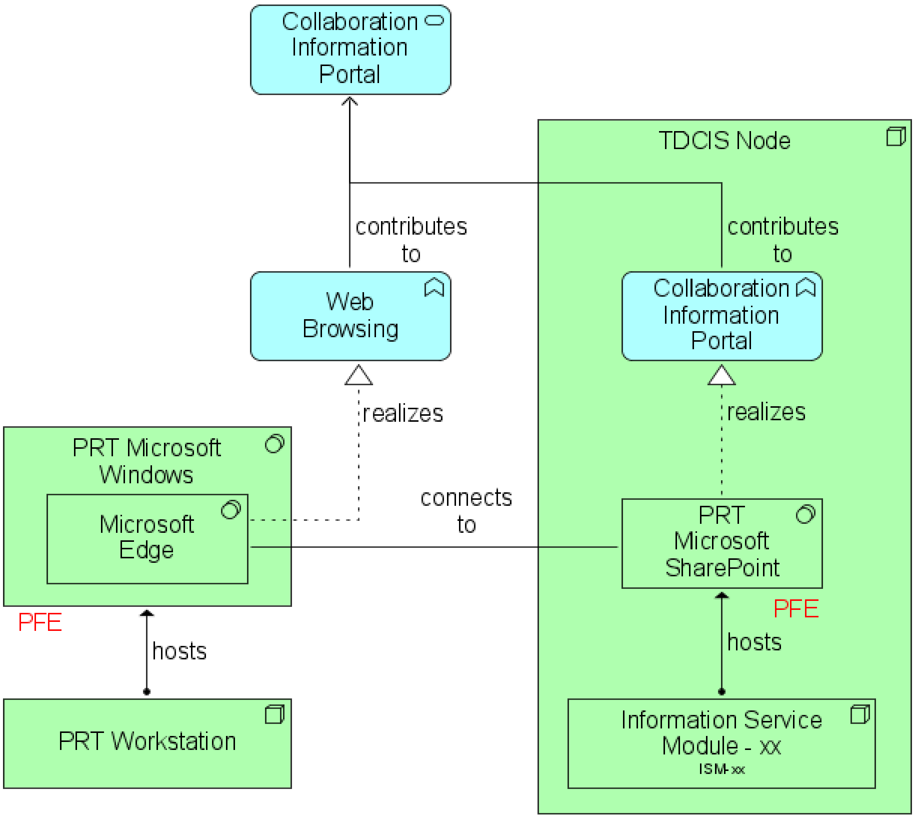

Figure 23 - Collaborative Information Portal Service implementation concept (TDCIS Node hosted)

SRS (PRTTDCIS-4275)

~~SRS-337~~ The Collaborative Information Portal Service design shall adhere to the implementation concept illustrated on the following figure for service instances hosted in PRT NDN.

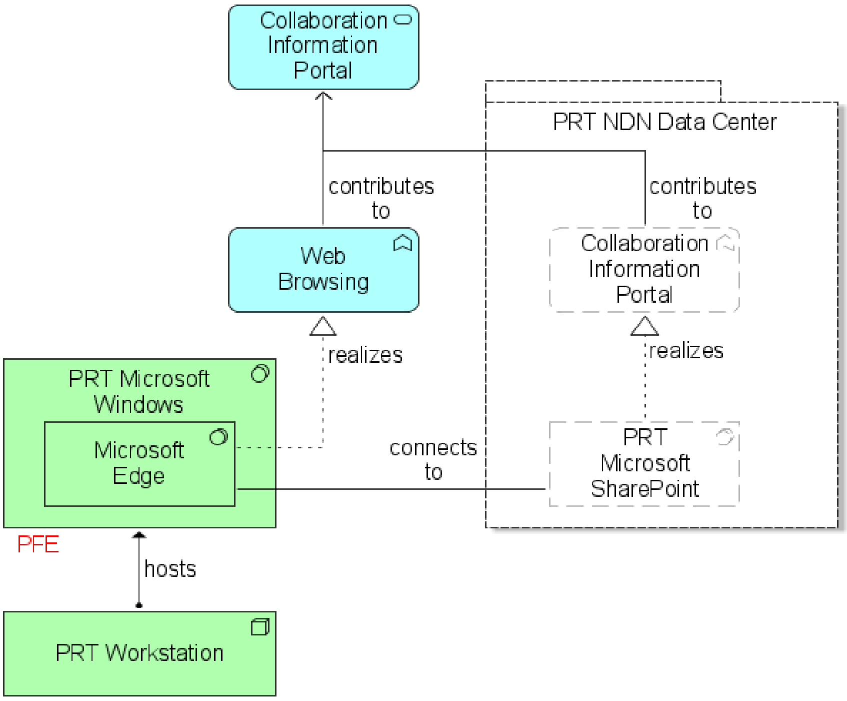

Figure 24 - Collaborative Information Portal Service implementation concept (PRT NDN hosted)

SRS (PRTTDCIS-4276)

~~SRS-338~~ The Collaborative Information Portal Service shall be implemented using Microsoft SharePoint.

NOTE (PRTTDCIS-4277)

~~[106]~~ Microsoft SharePoint Licenses for TDCIS Nodes implementation are PFE.

NOTE (PRTTDCIS-4278)

~~[107]~~ Microsoft SQL Licenses for TDCIS Nodes implementation are not PFE.

SRS (PRTTDCIS-2905)

~~SRS-339~~ The Collaboration Information Portal Service shall provide:

- 1TB of common storage; and,
- 2GB of personal storage for each user; and,
- 10% of reserve on the total.

4.1.4 Printing and Scanning Service

SRS (PRTTDCIS-2895)

~~SRS-340~~ The Printing and Scanning Service design shall adhere to the implementation concept illustrated on the following figure.

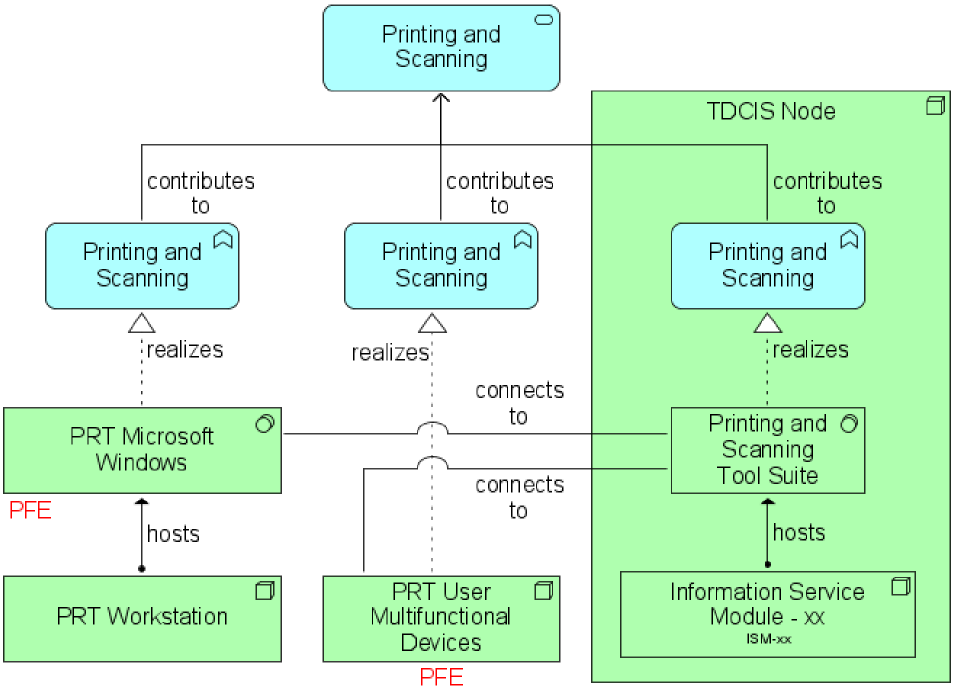

Figure 25 - Printing and Scanning Service implementation concept

SRS (PRTTDCIS-2907)

~~SRS-341~~ The Printing and Scanning Tool Suite shall allow users to:

- Print to paper hard copies on PFE Multifunctional Devices (MFD); and,
- Print to PDF file format; and,
- Scan from PFE Multifunctional Devices (MFD); and,
  - Send the scanned document via email to any user listed in the GAL; and,
  - Store the scanned document in a library provided by the Collaborative Information Portal Service.

4.1.5 Voice Collaboration Service

SRS (PRTTDCIS-2885)

~~SRS-342~~ The IP Voice Collaboration Service design shall adhere to the implementation concept illustrated on the following figure.

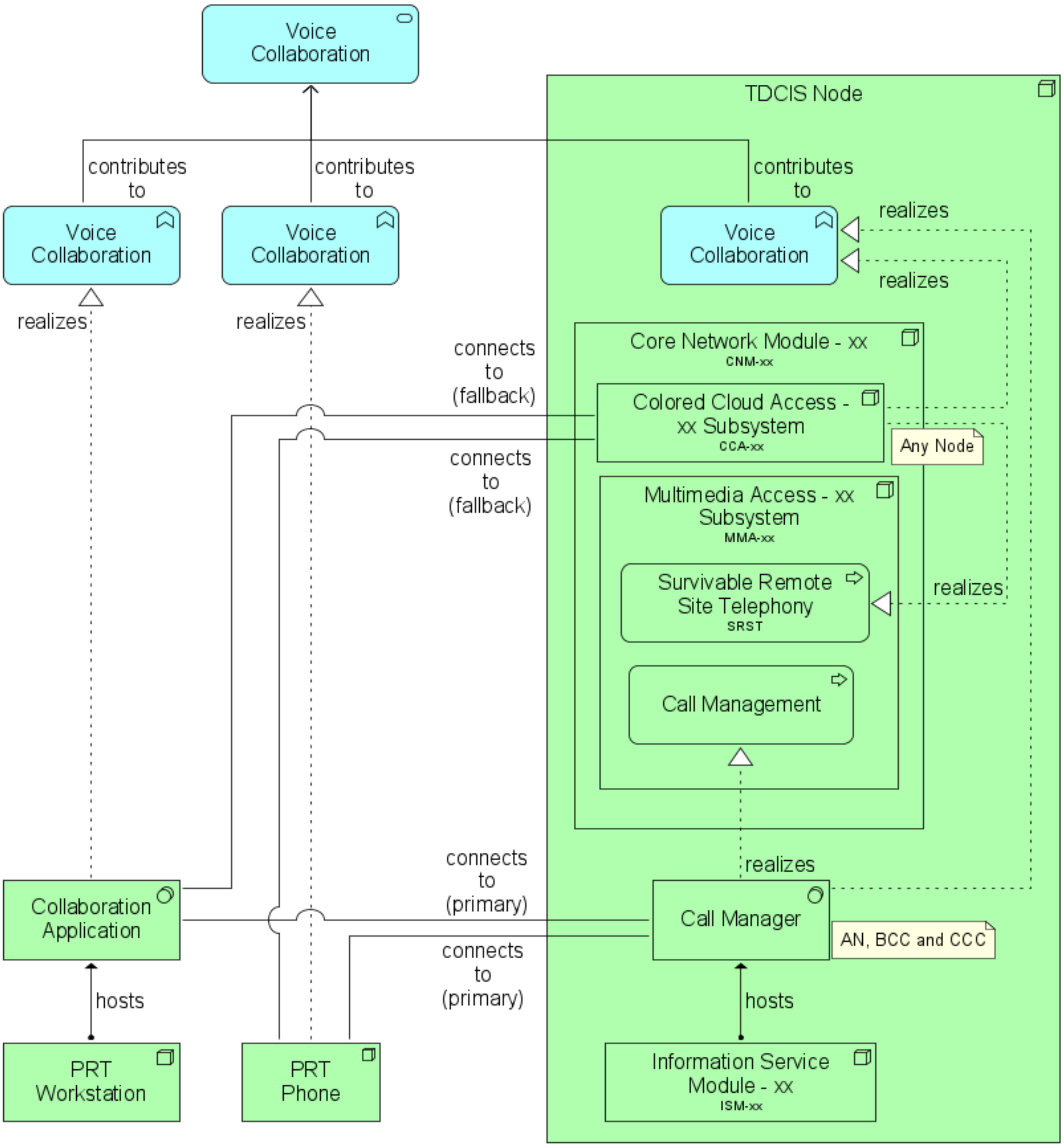

Figure 26 – IP Voice Collaboration Service implementation concept.

SRS (PRTTDCIS-4304)

~~SRS-343~~ The IP Voice Collaboration Service federation with mission partners design shall adhere to the implementation concept illustrated on the following figure.

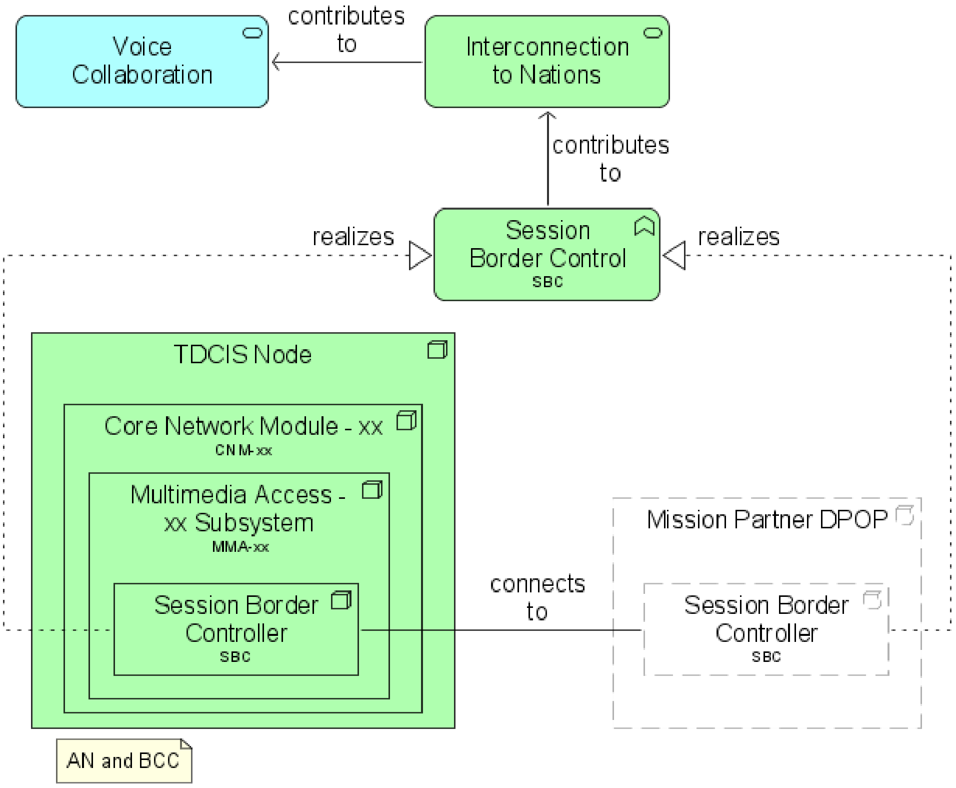

Figure 27 – IP Voice Collaboration Service federation implementation concept.

SRS (PRTTDCIS-2888)

~~SRS-344~~ Each user shall be associated with one physical (hardware) and one virtual (software) IP phone, both configured on the collaboration solution.

SRS (PRTTDCIS-2889)

~~SRS-345~~ The virtual (software) IP phone shall be realized by the Collaboration Application.

SRS (PRTTDCIS-2901)

~~SRS-346~~ On top of the user community based dimensioning constraint, the Contractor shall include an additional 10% provision of IP phones capacity.

SRS (PRTTDCIS-1266)

~~SRS-347~~ IP Voice service shall be provided in xU and xS security domains, in accordance to FMN specifications.

SRS (PRTTDCIS-4585)

~~SRS-348~~ The Analogue Voice Collaboration Service design shall adhere to the implementation concept illustrated on the following figure.

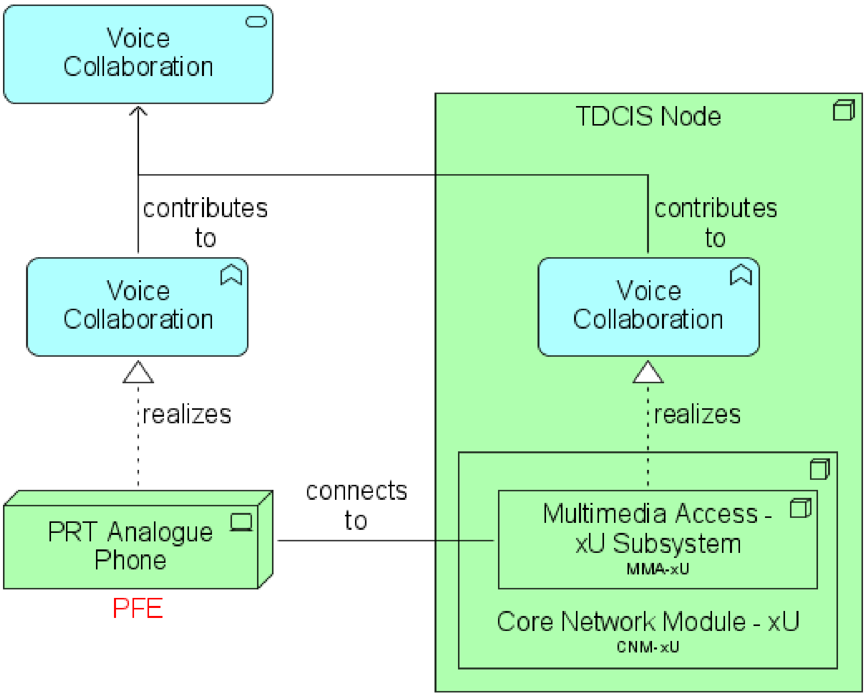

Figure 28 – Analogue Voice Collaboration Service federation implementation concept.

4.1.6 Video Teleconference Service

SRS (PRTTDCIS-2893)

~~SRS-349~~ The Video Teleconference Service design shall adhere to the implementation concept illustrated on the following figure for service instances hosted in a TDCIS Node.

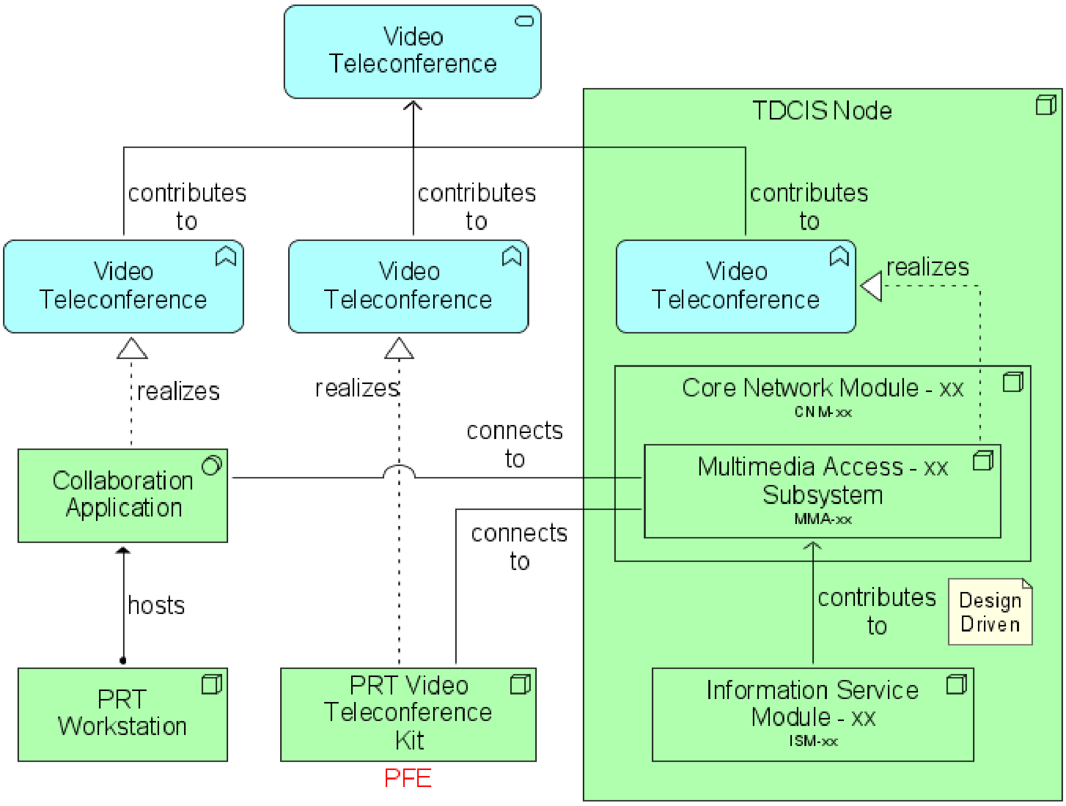

Figure 29 - Video Teleconference Service implementation concept (TDCIS Node hosted).

SRS (PRTTDCIS-4308)

~~SRS-350~~ The Video Teleconference Service design shall adhere to the implementation concept illustrated on the following figure for service instances hosted in PRT NDN.

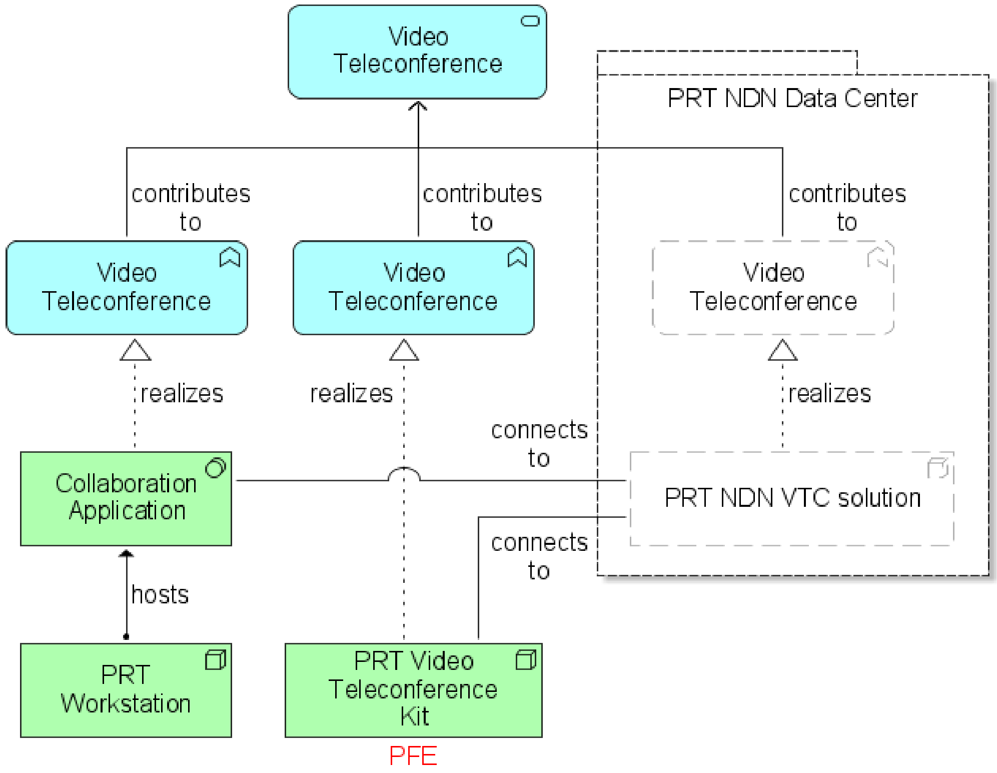

Figure 30 - Video Teleconference Service implementation concept (PRT NDN hosted).

SRS (PRTTDCIS-4305)

~~SRS-351~~ The Video Teleconference Service federation with mission partners design shall adhere to the implementation concept illustrated in the following figure.

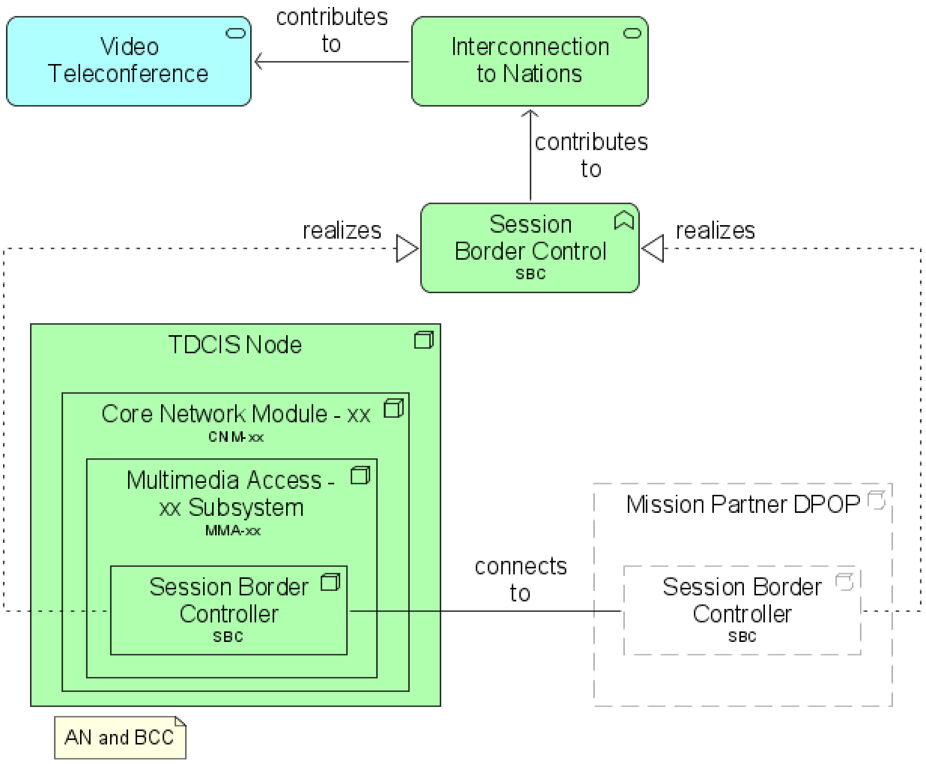

Figure 31 - Video Teleconference Service federation implementation concept.

SRS (PRTTDCIS-2899)

~~SRS-352~~ The Video Teleconference Service shall support:

- ONE (01) Video Teleconference Kit for each AN; and,
- ONE (01) Video Teleconference Kit for each BCC.

SRS (PRTTDCIS-2902)

~~SRS-353~~ Each user shall have a soft-VTC client realized by the Collaboration Application.

SRS (PRTTDCIS-4463)

~~SRS-354~~ The VTC Service shall provide Content Sharing allowing the users to share their Desktop or Applications (e.g. Microsoft PowerPoint, etc.).

SRS (PRTTDCIS-2900)

~~SRS-355~~ On top of the user community based dimensioning constraint, the Contractor shall include an additional 10% provision.

SRS (PRTTDCIS-2903)

~~SRS-356~~ The exact PFE product reference to fulfill the role of the *VTC Kit* is design driven. The Contractor shall provide the exact brand and model to the Purchaser for provisioning of this PFE.

SRS (PRTTDCIS-4107)

~~SRS-357~~ VTC Service shall be provided in xU and xS security domains, in accordance to FMN specifications.

NOTE (PRTTDCIS-4576)

~~[108]~~ VTC Solution implemented in PRT NDN is Cisco Meeting Server.

4.2 Community of Interest Services

SRS (PRTTDCIS-2882)

~~SRS-358~~ The Community of Interest Service design shall adhere to the implementation concept illustrated on the following figure.

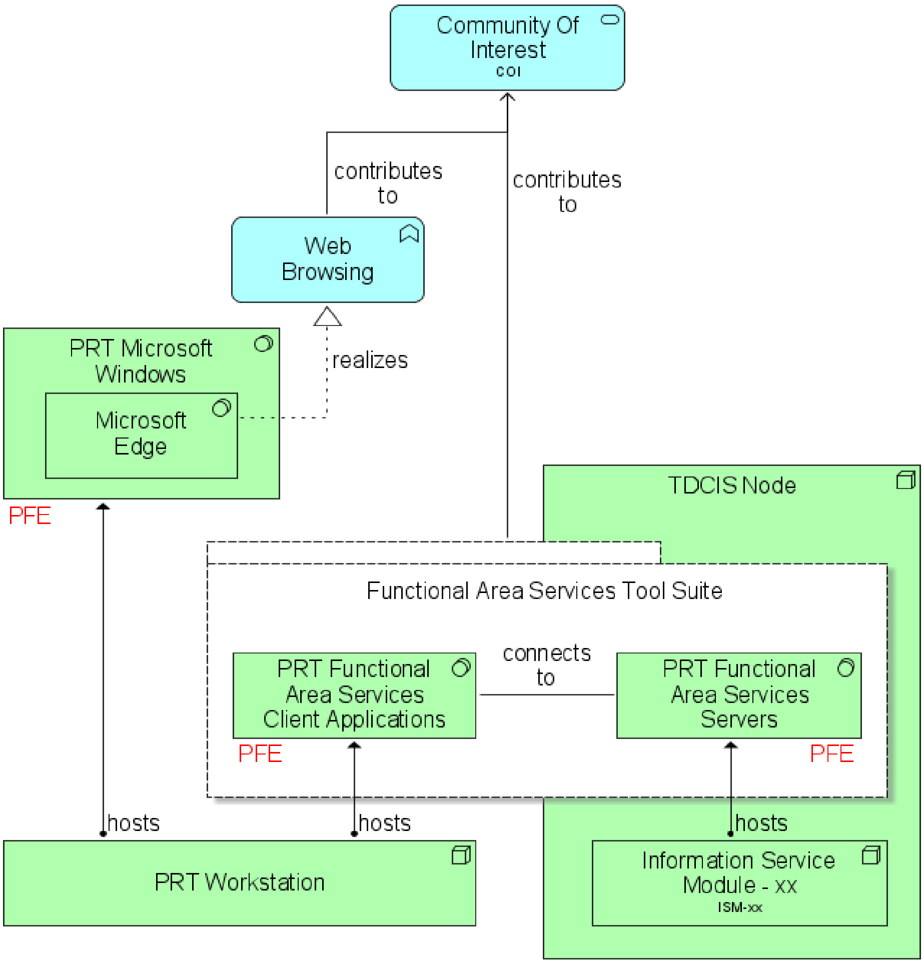

Figure 32 - Community of Interest Service implementation concept.

NOTE (PRTTDCIS-1233)

~~[109]~~ TDCIS is designed to be a tactical deployable CIS system. Over this system, PRT Army is intending to run their own Mission-specific Software (known as Functional Area Services) which composes the PFE workload to the CAS subsystem.

NOTE (PRTTDCIS-2881)

~~[110]~~ The Functional Area Services (FAS) Tool Suite is PFE.

SRS (PRTTDCIS-2883)

~~SRS-359~~ The Contractor shall create and configure the Virtual Machine (VM) as instructed by the Purchaser.

NOTE (PRTTDCIS-2884)

~~[111]~~ FAS software will be installed and configured by the Purchaser on the VM provided by the Contractor.

4.3 CIS Security Services

4.3.1 Antivirus Service

SRS (PRTTDCIS-2875)

~~SRS-360~~ The Antivirus Service design shall adhere to the implementation concept illustrated on the following figure.

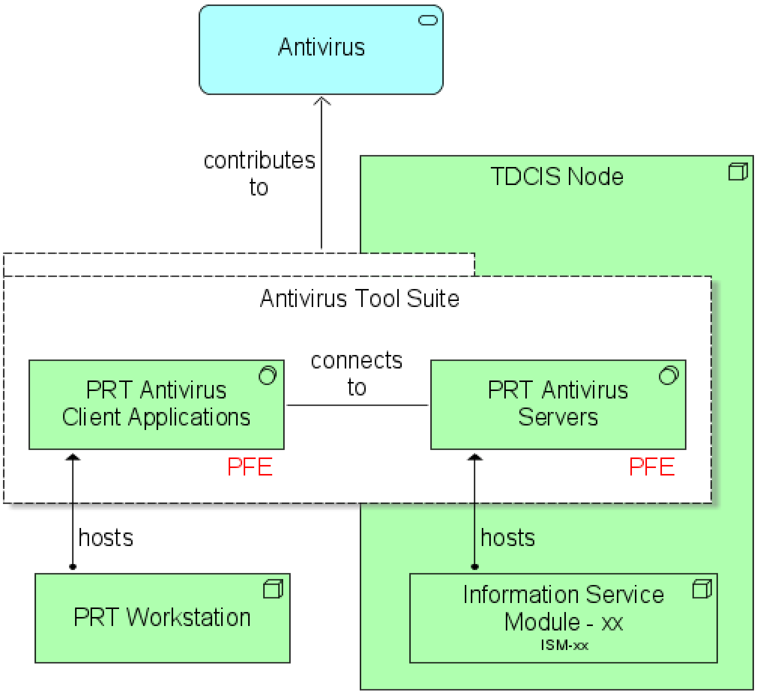

Figure 33 - Antivirus Service implementation concept.

NOTE (PRTTDCIS-2873)

~~[112]~~ The Antivirus Service provides CIS Security Service.

NOTE (PRTTDCIS-2874)

~~[113]~~ The Antivirus Tool Suite is PFE and is:

- a BitDefender product on xU and xR; and,
- McAfee ePO solution on xS.

SRS (PRTTDCIS-2877)

~~SRS-361~~ Applicable Antivirus Tool Suite components shall be installed and configured by the Contractor on all servers.

SRS (PRTTDCIS-2886)

~~SRS-362~~ Applicable Antivirus Tool Suite components shall be installed and configured by the Contractor on all System Administrator Workstations.

4.3.2 Network Access Control

SRS (PRTTDCIS-4242)

~~SRS-363~~ The Network Access Control (NAC) Service design in TDCIS Nodes shall adhere to the concept illustrated on following diagram.

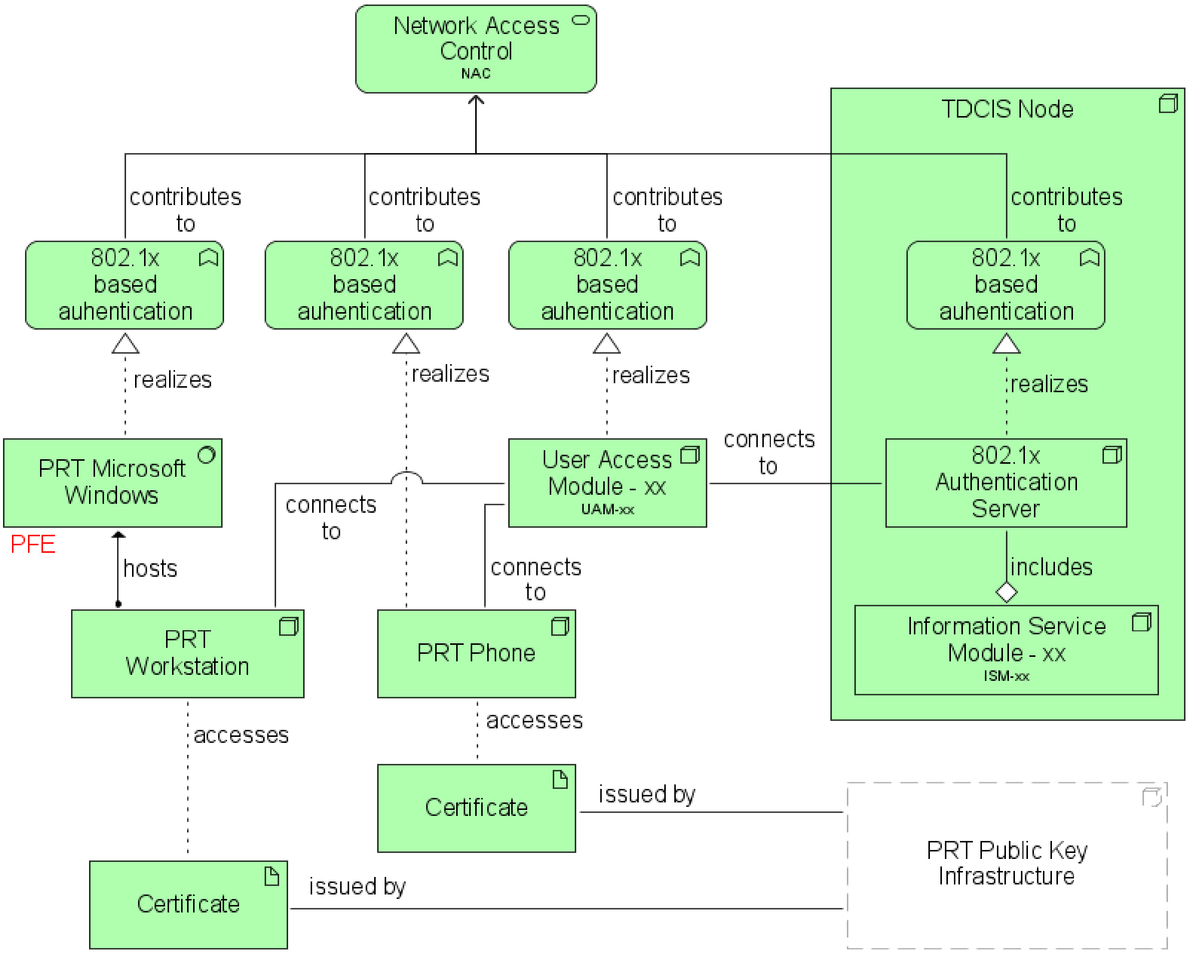

Figure 34- NAC service implementation concept in TDCIS Nodes

SRS (PRTTDCIS-4316)

~~SRS-364~~ The Network Access Control (NAC) Service design in the NS Kit shall adhere to the concept illustrated on following diagram.

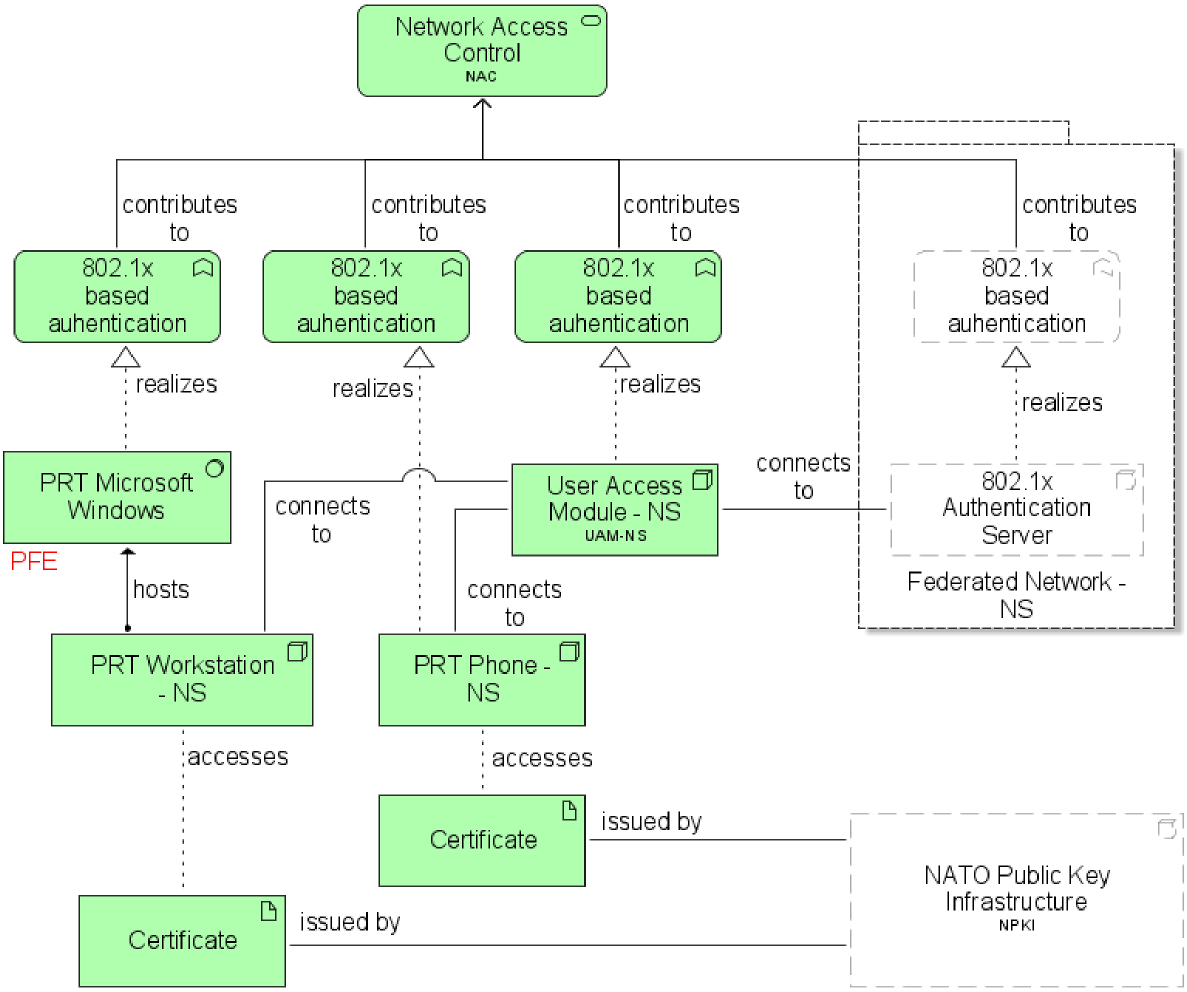

Figure 35 - NAC service implementation concept in the NS Kit

SRS (PRTTDCIS-4243)

~~SRS-365~~ The NAC Service shall be implemented with IEEE 802.1x protocol

SRS (PRTTDCIS-4244)

~~SRS-366~~ The NAC Service shall be implemented over wired and wireless connectivity between EUD and UAM.

SRS (PRTTDCIS-4245)

~~SRS-367~~ The NAC Service for TDCIS Nodes shall be implemented with certificates delivered by the PRT Public Key Infrastructure.

SRS (PRTTDCIS-4317)

~~SRS-368~~ The NAC Service for the NS Kit shall be implemented with certificates delivered by the NATO Public Key Infrastructure (NPKI).

4.3.3 Encryption

4.3.3.1 General

NOTE (PRTTDCIS-4246)

~~[114]~~ The Encryption Service variants are illustrated on following diagram.

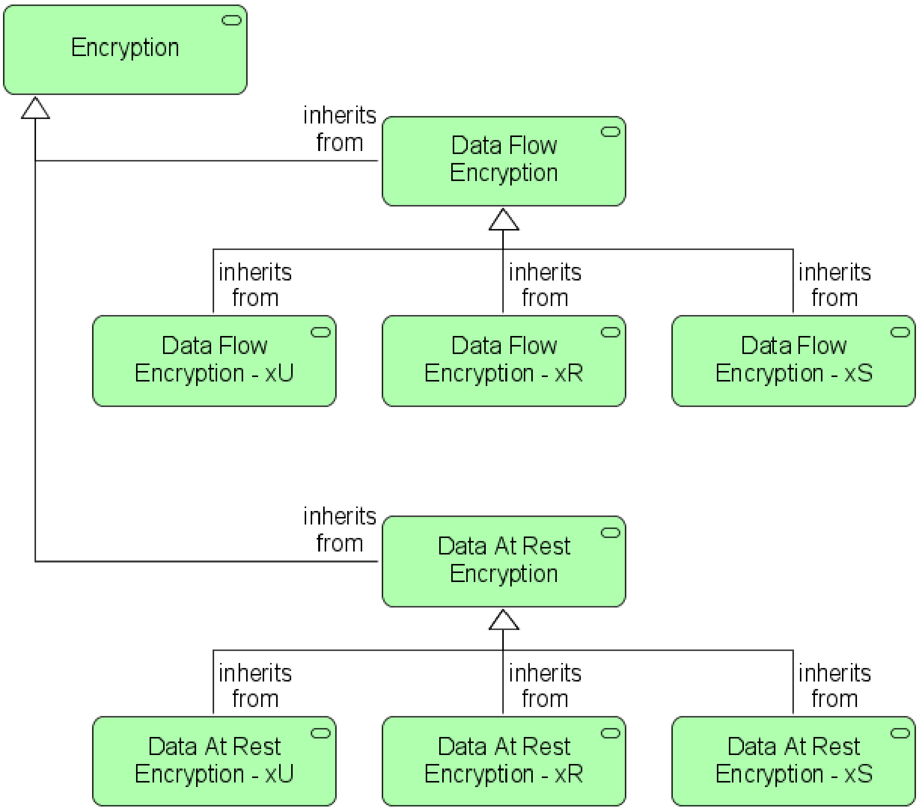
Encryption
inherits from
Data Flow Encryption
inherits from
inherits from
inherits from
Data Flow Encryption - xU
Data Flow Encryption - xR
Data Flow Encryption - xS
inherits from
Data At Rest Encryption
inherits from
inherits from
inherits from
Data At Rest Encryption - xU
Data At Rest Encryption - xR
Data At Rest Encryption - xS

Figure 36 - Encryption service variants

4.3.3.2 Data Flow Encryption

SRS (PRTTDCIS-4247)

~~SRS-369~~ The Data Flow Encryption Service design shall adhere to the concept illustrated on following diagram.

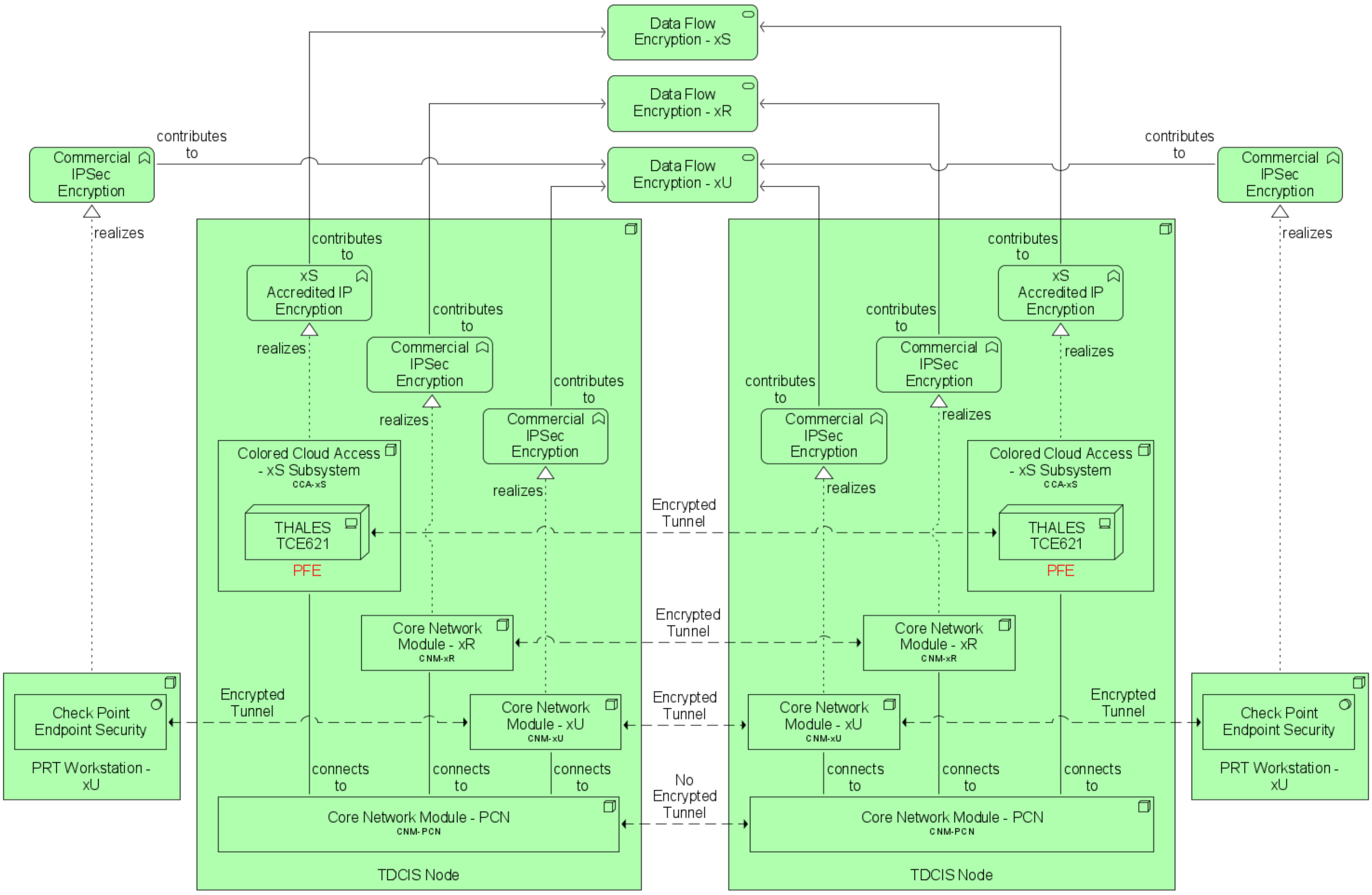
Data Flow Encryption - xS
Data Flow Encryption - xR
Data Flow Encryption - xU
contributes to
Commercial IPSec Encryption
realizes
xS Accredited IP Encryption
Colored Cloud Access - xS Subsystem
CCA-xS
THALES TCE621
PFE
Encrypted Tunnel
Core Network Module - xR
CNM-xR
Core Network Module - xU
CNM-xU
Check Point Endpoint Security
PRT Workstation - xU
connects to
Core Network Module - PCN
CNM-PCN
No Encrypted Tunnel
TDCIS Node

Figure 37 - Data Flow Encryption service implementation concept

SRS (PRTTDCIS-4248)

~~SRS-370~~ The TDCIS Nodes Data Flow Encryption Service on xS shall be implemented with THALES TCE621B IP cryptos.

SRS (PRTTDCIS-4249)

~~SRS-371~~ The NS Kit Data Flow Encryption Service on NS shall be implemented with THALES TCE621M IP cryptos.

SRS (PRTTDCIS-4310)

~~SRS-372~~ The Data Flow Encryption Service on xR shall be implemented with Commercial IPSec encryption embedded in the CCA-xR.

SRS (PRTTDCIS-4250)

~~SRS-373~~ The Data Flow Encryption Service on xU shall be implemented with Commercial IPSec encryption embedded in the CCA-xU.

NOTE (PRTTDCIS-4251)

~~[115]~~ No encrypted tunnels will be implemented at PCN level.

SRS (PRTTDCIS-4312)

~~SRS-374~~ The Data Flow Encryption Service on xU shall be implemented with Check Point Endpoint Security software between the PRT Workstation and the CCA-xU.

SRS (PRTTDCIS-4313)

~~SRS-375~~ The CCA-xU shall act as the VPN concentrator for all users of the TDCIS Node.

4.3.3.3 Data At Rest Encryption

SRS (PRTTDCIS-4253)

~~SRS-376~~ The Data At Rest Encryption Service design shall adhere to the concept illustrated on following diagram.

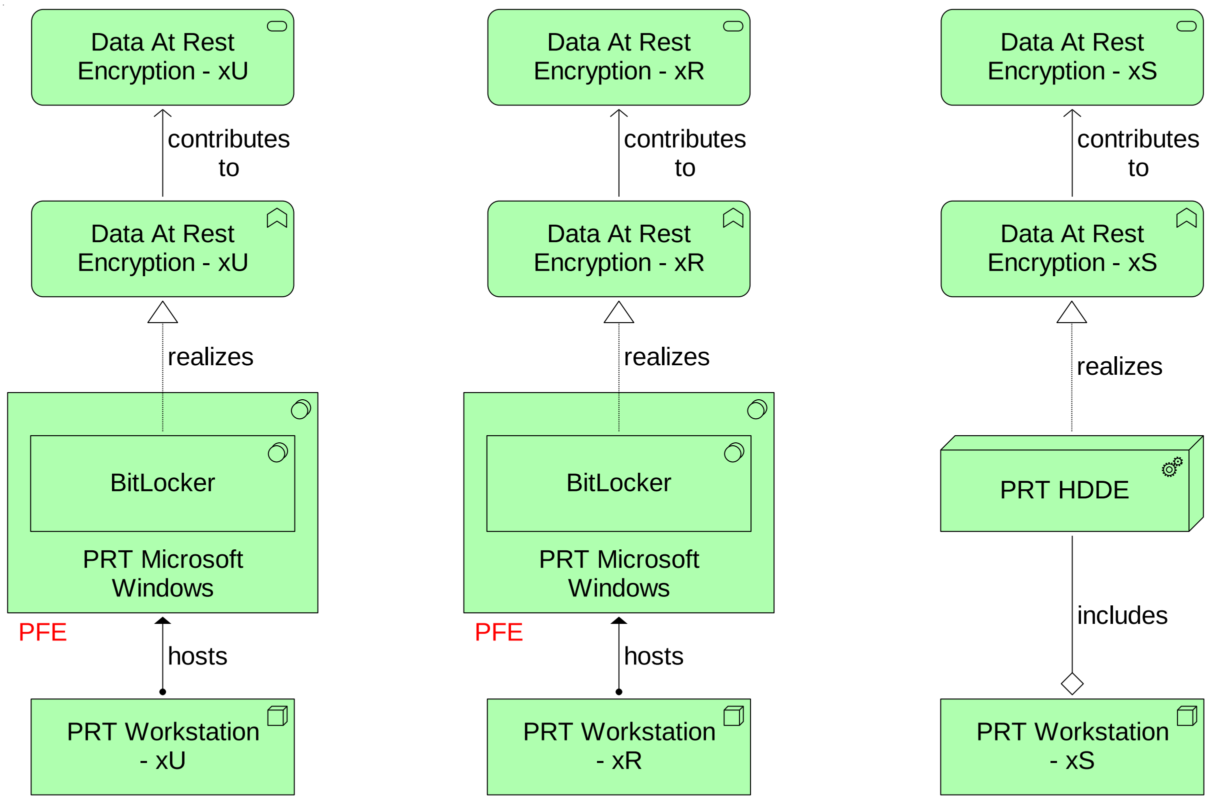

Figure 38 - Data At Rest Encryption service implementation concept

SRS (PRTTDCIS-4254)

~~SRS-377~~ The TDCIS Data At Rest Encryption Service on xS shall be implemented with HDDE sourced from non-archived appliances listed in the NIAPC and certified for SECRET.

SRS (PRTTDCIS-4311)

~~SRS-378~~ The TDCIS Node Data At Rest Encryption Service on xR shall be implemented with the BitLocker functionality embedded in Microsoft Windows Operating System.

SRS (PRTTDCIS-4255)

~~SRS-379~~ The TDCIS Node Data At Rest Encryption Service on xU shall be implemented with the BitLocker functionality embedded in Microsoft Windows Operating System.

4.3.4 Log Aggregation

SRS (PRTTDCIS-4257)

~~SRS-380~~ TDCIS Nodes shall support future integration in a Log Aggregation Services as illustrated on following picture.

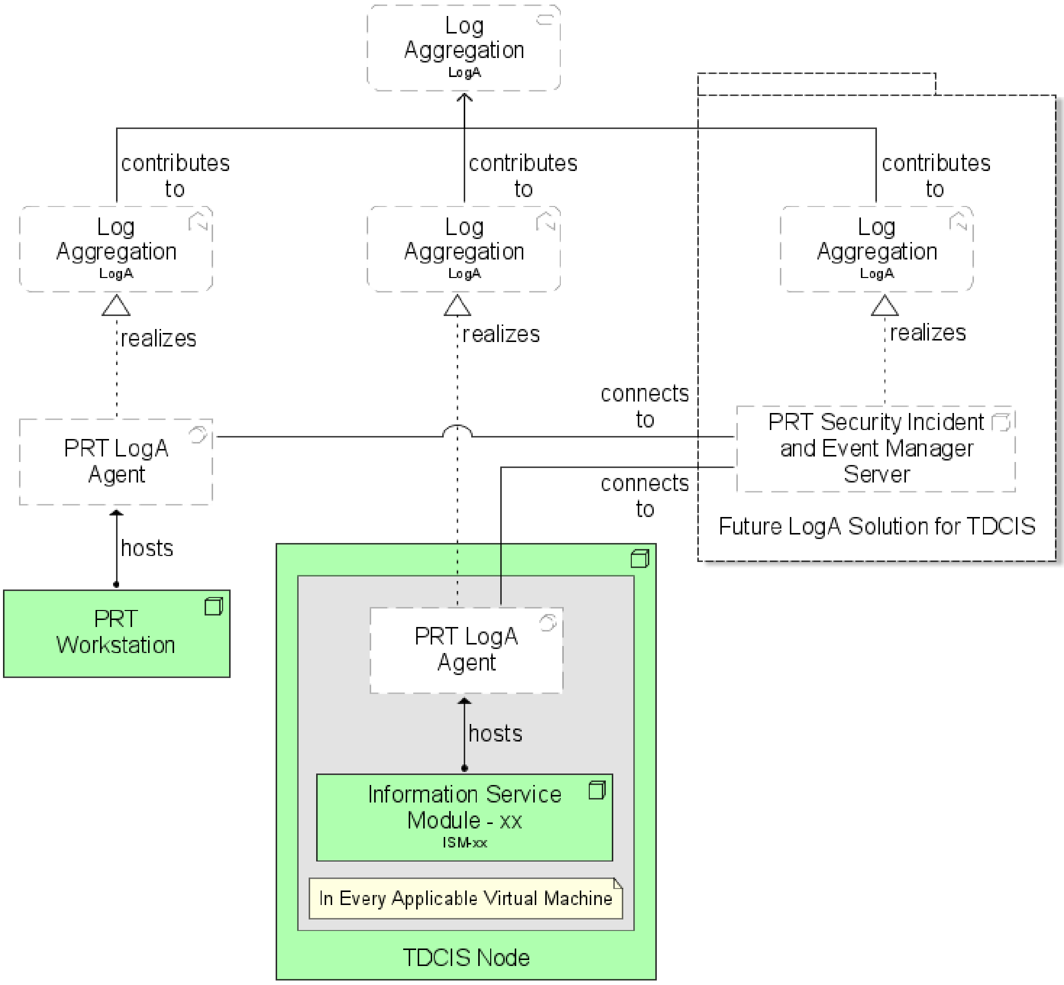

Figure 39 - LogA service integration concept

SRS (PRTTDCIS-4314)

~~SRS-381~~ The Log Aggregation (LogA) Service design in the NS Kit shall adhere to the concept illustrated on following diagram.

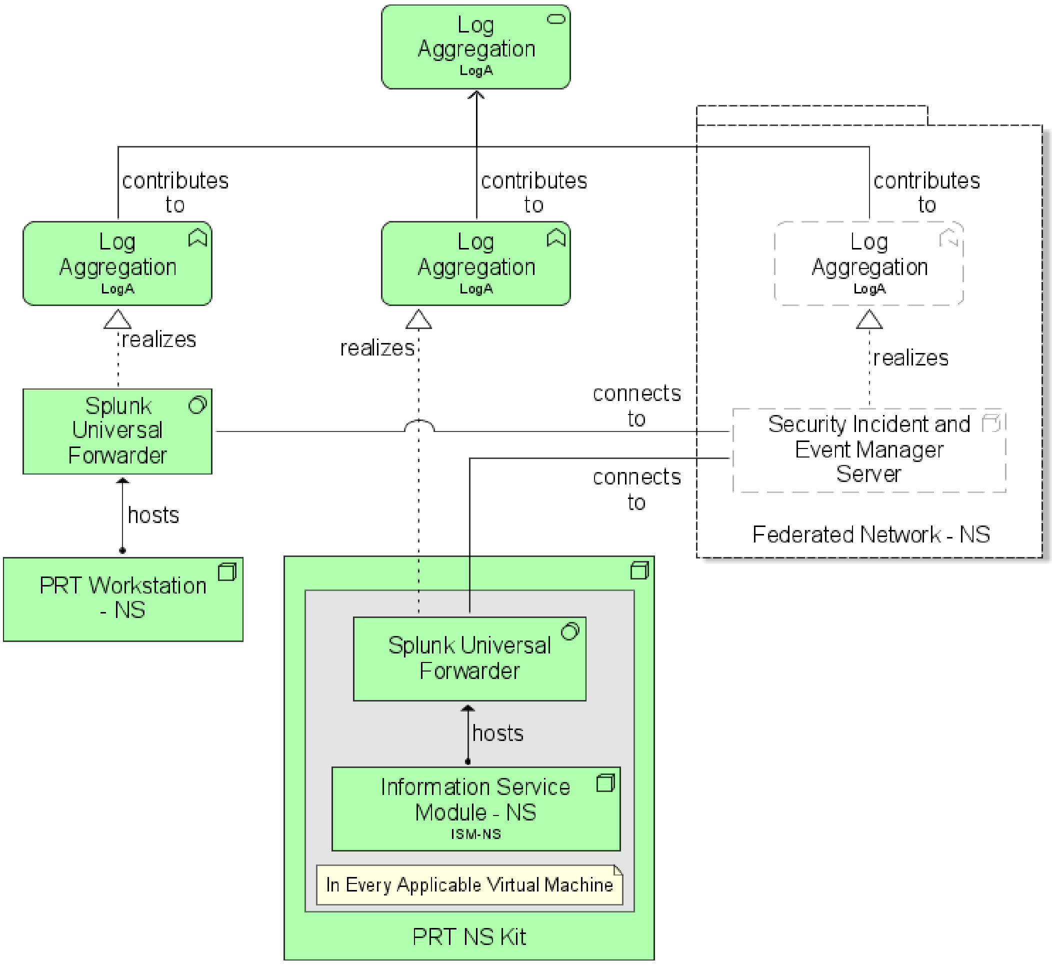

Figure 40 - LogA service implementation concept in NS Kit

SRS (PRTTDCIS-4258)

~~SRS-382~~ The LogA Service in the NS Kit shall be implemented with Splunk Universal Forwarder application installed on the Workstation.

4.3.5 Online Vulnerability Assessment

SRS (PRTTDCIS-4260)

~~SRS-383~~ TDCIS Nodes shall support future integration in an Online Vulnerability Assessment Services as illustrated on following picture.

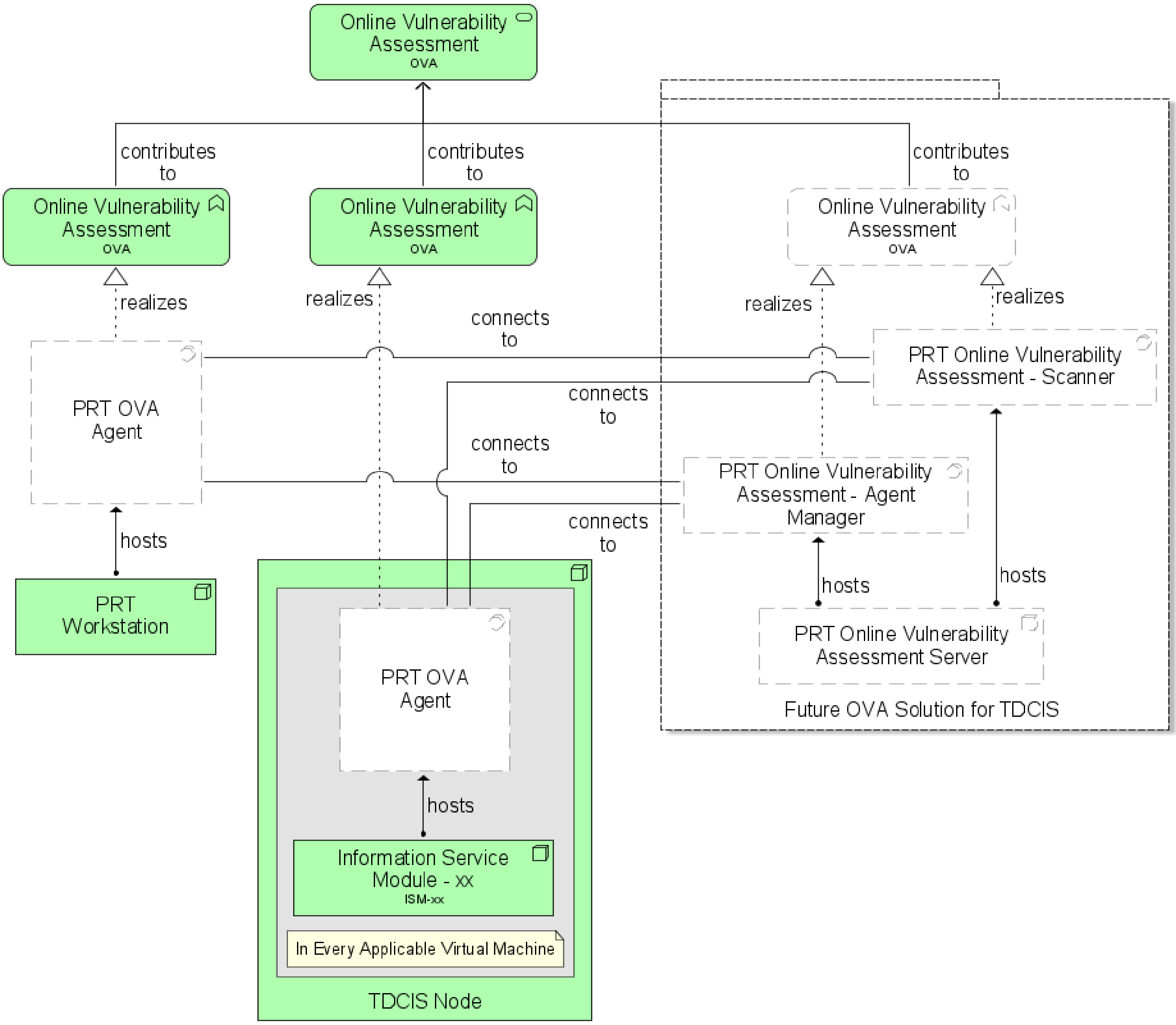
Online Vulnerability Assessment
OVA
contributes to
contributes to
contributes to
Online Vulnerability Assessment
OVA
Online Vulnerability Assessment
OVA
Online Vulnerability Assessment
OVA
realizes
realizes
realizes
realizes
connects to
connects to
connects to
connects to
PRT OVA Agent
PRT Online Vulnerability Assessment - Scanner
PRT Online Vulnerability Assessment - Agent Manager
hosts
hosts
hosts
hosts
PRT Workstation
PRT OVA Agent
PRT Online Vulnerability Assessment Server
Future OVA Solution for TDCIS
Information Service Module - xx
ISM-xx
In Every Applicable Virtual Machine
TDCIS Node

Figure 41 - OVA service integration concept for TDCIS Nodes

SRS (PRTTDCIS-4315)

~~SRS-384~~ The Online Vulnerability Assessment (OVA) Service design in the NS Kit shall adhere to the concept illustrated on following diagram.

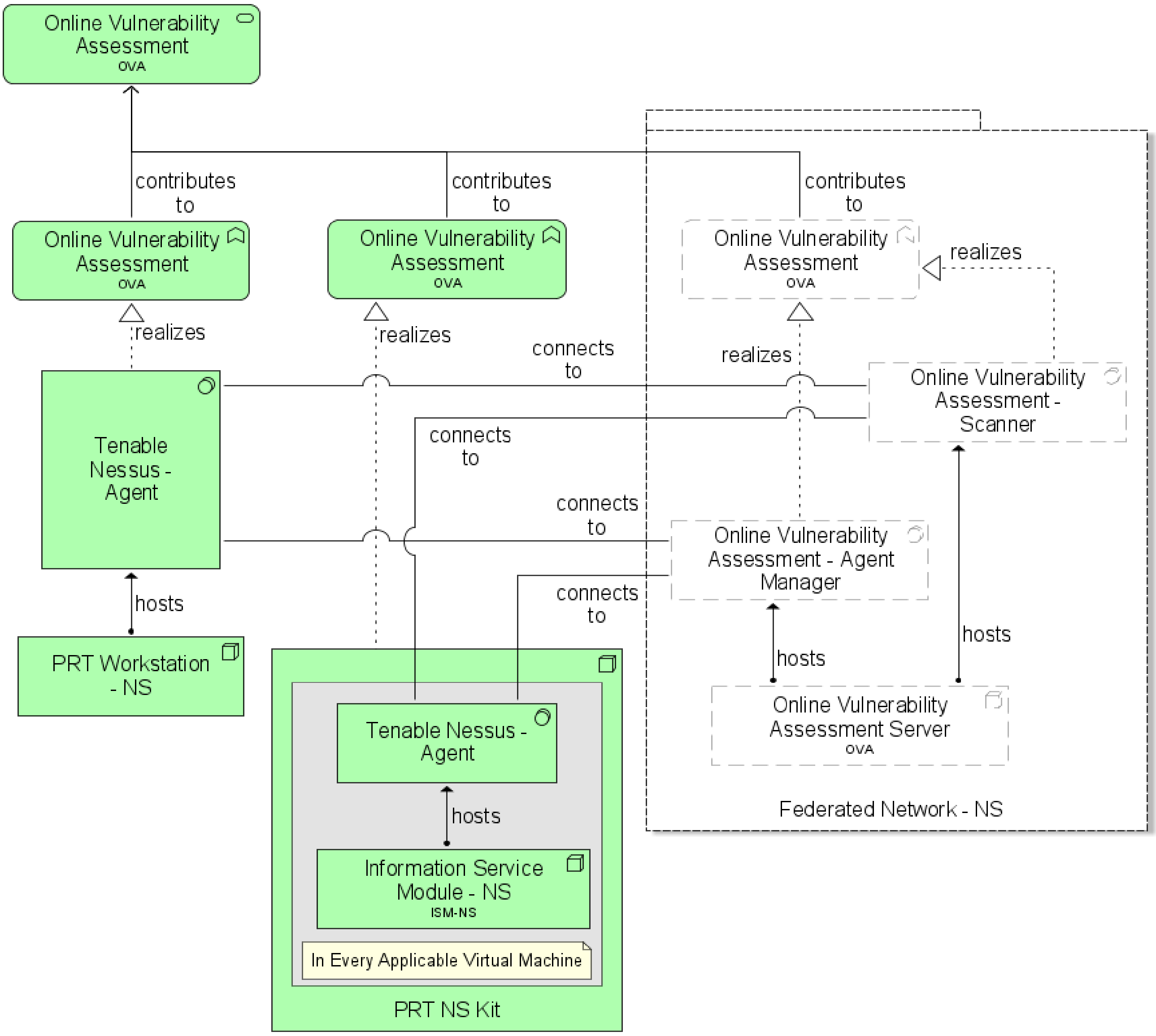
Online Vulnerability Assessment
OVA
contributes to
contributes to
contributes to
Online Vulnerability Assessment
OVA
Online Vulnerability Assessment
OVA
Online Vulnerability Assessment
OVA
realizes
realizes
realizes
realizes
connects to
Online Vulnerability Assessment - Scanner
Tenable Nessus - Agent
connects to
connects to
Online Vulnerability Assessment - Agent Manager
hosts
connects to
hosts
hosts
PRT Workstation - NS
Tenable Nessus - Agent
Online Vulnerability Assessment Server
OVA
hosts
Federated Network - NS
Information Service Module - NS
ISM-NS
In Every Applicable Virtual Machine
PRT NS Kit

Figure 42 - OVA service implementation concept in the NS Kit

SRS (PRTTDCIS-4261)

~~SRS-385~~ The OVA Service in the NS Kit shall be implemented with Tenable Nexus Agent application installed on the Workstation.

4.3.6 Cross Domain

NOTE (PRTTDCIS-4360)

~~[116]~~ The Cross Domain Service variants are illustrated on following diagram.

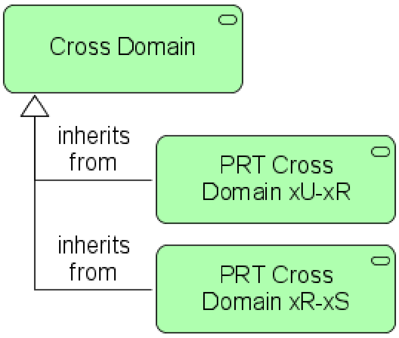

Figure 43 - Cross Domain service variants

SRS (PRTTDCIS-4361)

~~SRS-386~~ The xU-xR Cross Domain Service design shall adhere to the concept illustrated on following diagram.

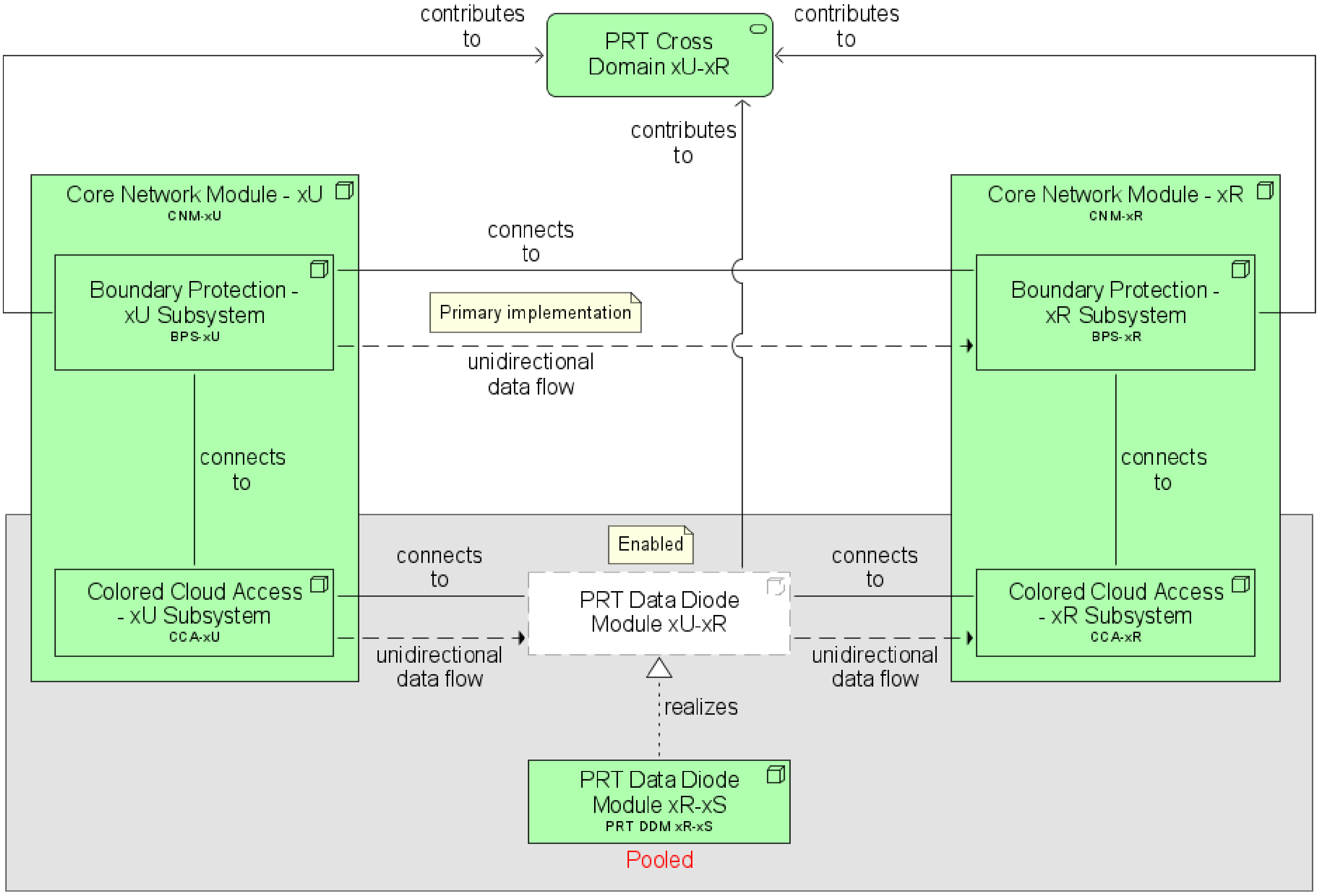

Figure 44 - xU-xR Cross Domain service implementation concept

SRS (PRTTDCIS-4363)

~~SRS-387~~ The xU-xR Cross Domain Service shall be implemented through a direct link between BPS-xU and BPS-xR.

SRS (PRTTDCIS-4367)

~~SRS-388~~ The xU-xR Cross Domain Service realized through BPS-xU and xR shall meet the same functional and technical requirements as the DDM xR-xS.

SRS (PRTTDCIS-4365)

~~SRS-389~~ The xU-xR Cross Domain Service shall support to be realized by re-purposing pooled DDM xR-xS to this purpose. This realization shall only require physical installation of hardware in racks and configuration.

SRS (PRTTDCIS-4362)

~~SRS-390~~ The xR-xS Cross Domain Service design shall adhere to the concept illustrated on following diagram.

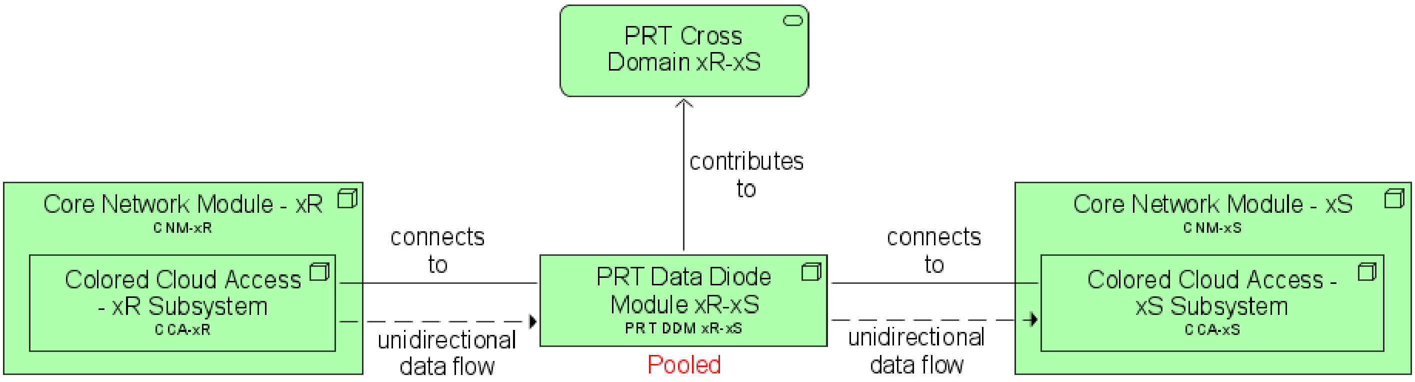

Figure 45 - xR-xS Cross Domain service implementation concept

SRS (PRTTDCIS-4364)

~~SRS-391~~ The xR-xS Cross Domain Service shall be implemented by the DDM xR-xS.

4.4 Interconnection to Nations

NOTE (PRTTDCIS-2977)

~~[117]~~ The Interconnection to Nations Service is composed by elements belonging to other Services in order to enable federation with Mission Partners under the FMN Framework.

SRS (PRTTDCIS-2978)

~~SRS-392~~ The Interconnection to Nations Service design shall adhere to the implementation concept illustrated on the following figure.

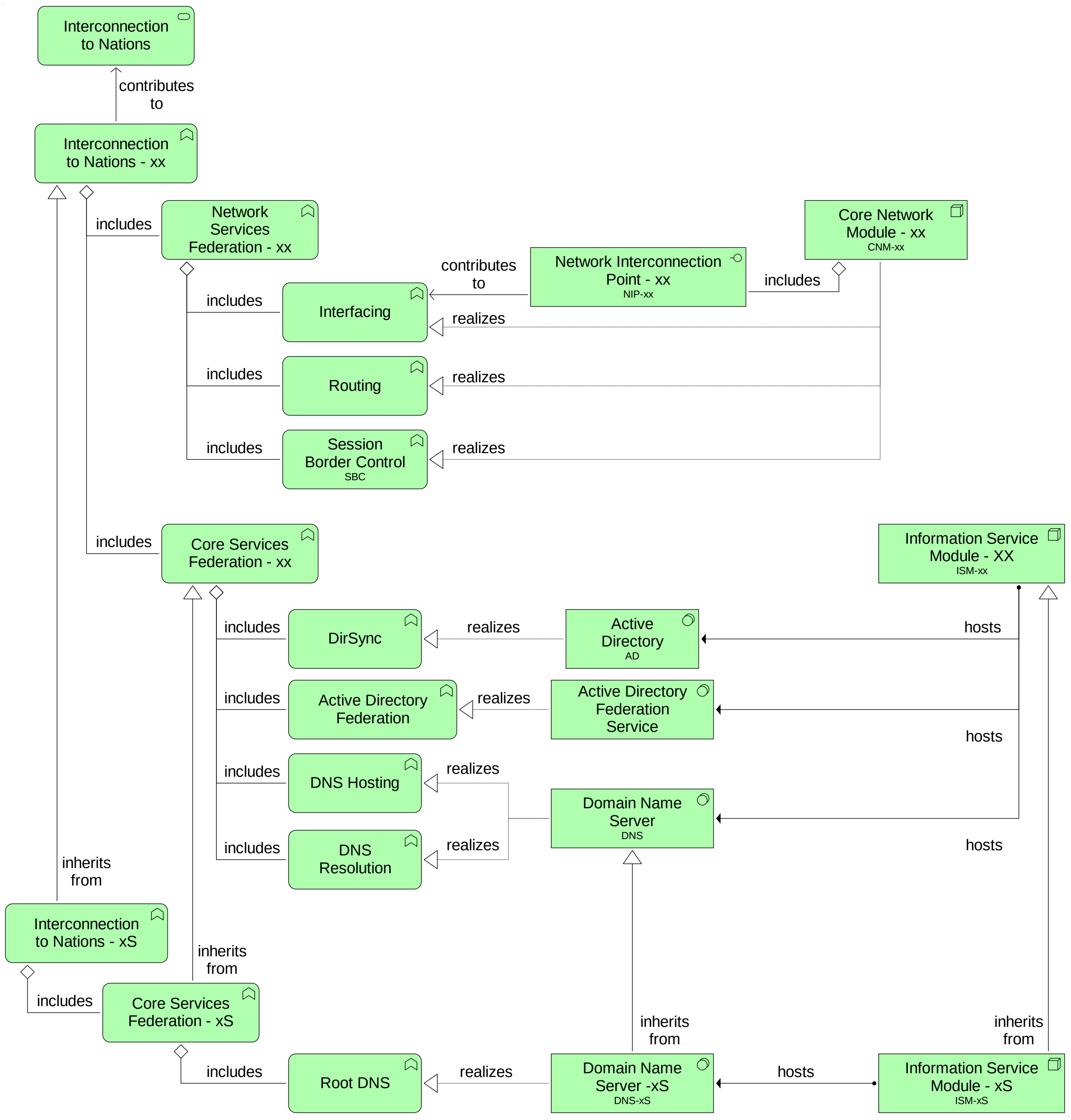

Figure 46 - Interconnection to Nations Service implementation concept.

NOTE (PRTTDCIS-2979)

~~[118]~~ The Interconnection to Nations Services relies on the Interconnection to Nations Function which contains:

- **Network Services Federation** which combines Network and Communication Services; and
- **Core Services Federation** which combines Infrastructure and Business Support Services.

SRS (PRTTDCIS-2980)

~~SRS-393~~ The Interconnection to Nations Service shall rely on following elements:

- From the CNM:
  - The Network Interconnection Point (NIP) interface which physically and logically connects Mission Partners; and
  - Routing functions to federate at network layer; and,
  - Session Border Control (SBC) functions to federate Communication Services; and
- From the ISM:
  - The Active Directory (AD) for DirSync to enable the federation; and
  - The Email software to federate Informal Messaging Service (IMS); and
  - The Active Directory Federation Service (ADFS); and
  - The Domain Name Server (DNS) to enable DNS hosting and Resolver for the federation.

SRS (PRTTDCIS-2981)

~~SRS-394~~ The DNS Server for the xS implementation of the Interconnection to Nations Service shall also enable Root DNS.

4.5 Service Management and Control

4.5.1 General

NOTE (PRTTDCIS-2937)

~~[119]~~ Service Management and Control (SMC) is divided in following levels:

1) **Enterprise** level SMC is the level providing Management and Monitoring at the highest level possible within an organization (e.g. TDCIS as a whole or a mission or exercise specific TDCIS subset, PRT NDN, etc.) and their associated processes; and,
2) **Domain** level SMC is the level providing Management and Monitoring over a certain community or subset (e.g. Network elements, a TDCIS Node, etc.) and their associated specialization of the Enterprise level processes; and,
3) **Element** level SMC is the lowest level and contains all tools and instructions to perform layer-, technology- or even product-centric Management and Configuration activities (e.g. SCCM, Cisco Prime, etc.).

SRS (PRTTDCIS-2938)

~~SRS-395~~ This project shall implement TDCIS Node-centric (i.e. providing SMC for the Node and its composing elements only) Element and Domain SMC.

SRS (PRTTDCIS-2939)

~~SRS-396~~ The integration of TDCIS SMC at mission or exercise layer (e.g. Monitoring of all nodes from a Theatre Operation Center, etc.) or with PRT NDN at Enterprise level is not in scope of this project. However, the Contractor shall aim to provide a TDCIS SMC solution which supports these integrations in the future.

SRS (PRTTDCIS-4398)

~~SRS-397~~ The TDCIS SMC shall provide following functions:

- **Capture and Manage Configurations:** Capture, manage and control the configuration, status, and relationships of services, service components, and service resources; and,
- **Discovery:** The automatic finding, identification, and relationship mapping of service components. Used to automatically feed a Configuration Management Data Base (CMDB); and,
- **Monitor:** Automatically observe and record the consumption and performance of services, service components and related resources within the context of an agreed scope and set of constraints. Includes the ability to provide awareness (alerts, notifications, triggers) when predefined thresholds may be, or are being, breached; and,
- **Manage Systems:** Respond to changes in a system's operating state. Perform configuration changes on one or more systems with the intention to change the existing operating configuration; and,
- **Report:** Consume raw data, aggregate, transform, analyse, and provide useful summary and detailed output based on a point in time or specified timeframe view of service related metrics.

SRS (PRTTDCIS-4525)

~~SRS-398~~ When referring to "Configuration" in the SMC context, it shall include and implement its two dimensions in support of the Configuration Management process:

1) Visibility of configurations from the view of a set of service elements (with attributes) and the relationships between service elements of the same service and different services; and,
2) The contents of key configuration files, e.g. the configuration of a switch or router.

SRS (PRTTDCIS-4399)

~~SRS-399~~ TDCIS SMC Capture and Manage Configurations function shall:

- Enable the identification, configuration, control and location of every Configuration Item (CI) over the management network.
- Automatically capture CI configurations; and,
- Backup configurations to support configuration Recovery; and,
- Support Configurations Import from and Export to files.

SRS (PRTTDCIS-4401)

~~SRS-400~~ TDCIS SMC Report function shall:

- Present Node Elements Status using the format of maps and dashboards; and,
- Support export to common Office file formats (e.g. Microsoft Word, Microsoft Excel, PDF, etc.) and Picture file formats (e.g. JPEG, PNG, etc.).

SRS (PRTTDCIS-1235)

~~SRS-401~~ The TDCIS SMC shall consist of a set of computer tools to provide across all layers of the TDCIS architecture:

- **Element Management:** Element level of SMC which provides:
  - Management and Configuration of Elements; and,
  - Discovery and Inventory to support populating the Node CMDB with CIs; and,
  - Events to the Node Monitoring layer; and,
- **Node Monitoring:** Domain level of SMC which:
  - Collects Events to report the impacted services status; and,
  - Monitor Service performances; and,
  - Report Service Situation Awareness (including all Service Subsets).

SRS (PRTTDCIS-2940)

~~SRS-402~~ The following picture illustrates the relationships between Element Management and Node Monitoring layers and with which their associated Tool Suites shall comply. Flow relationships illustrate the logical flow of information between the different elements. e.g. nothing prevents the Node Monitoring Tool Suite to interact directly with Configuration Items (radio, router, server, etc.) to populate the Node CMDB.

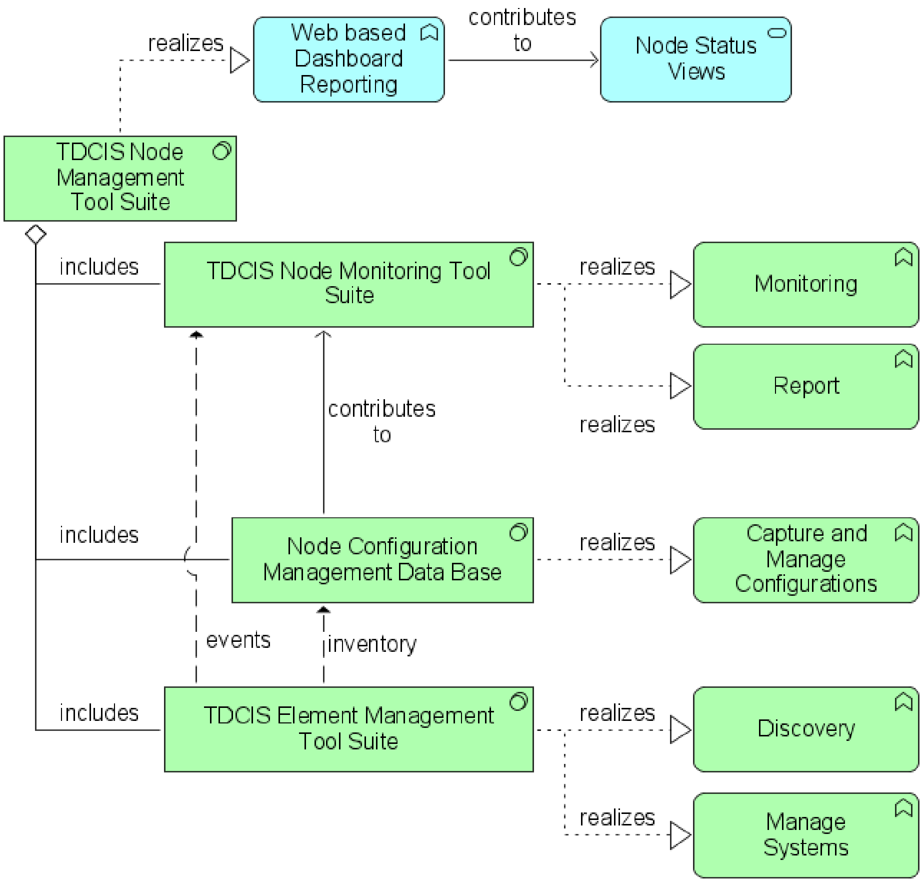
realizes
Web based Dashboard Reporting
contributes to
Node Status Views
TDCIS Node Management Tool Suite
includes
TDCIS Node Monitoring Tool Suite
realizes
Monitoring
Report
realizes
contributes to
includes
Node Configuration Management Data Base
realizes
Capture and Manage Configurations
events
inventory
includes
TDCIS Element Management Tool Suite
realizes
Discovery
realizes
Manage Systems

Figure 47 - SMC Tool Suites in Context

NOTE (PRTTDCIS-2934)

~~[120]~~ The existing Monitoring Tool in use in PRT NDN is Zabbix.

SRS (PRTTDCIS-2935)

~~SRS-403~~ The TDCIS SMC shall encompass the provision of the following:

1) Deployable management Account Administration tooling, running locally on the ISM, synchronized with the extant centralized account management capability when TDCIS is configured as NDN extension (Nat-x security domains variants); and
2) The implementation of Virtual Machines as required, to run local instances of the SMC tools; and
3) The ability to perform all SMC functions for all Node subsystems locally.

SRS (PRTTDCIS-2933)

~~SRS-404~~ SMC elements implemented as part of the DPOP, shall support Role Based Access Control via integration with Active Directory.

SRS (PRTTDCIS-1357)

~~SRS-405~~ The Role Based Access Control shall log all action carried out within the scope of the management of TDCIS to enable audits and forensics.

SRS (PRTTDCIS-1356)

~~SRS-406~~ The Role Based Access Control shall enable application of access policies to management platforms. To this end, it shall include functionalities for creation, removal and control of users, together with their associated level of management services. It shall also include the distribution of relevant security information.

SRS (PRTTDCIS-2967)

~~SRS-407~~ Every TDCIS component shall be managed via a dedicated physical or logical Management Interface.

SRS (PRTTDCIS-2966)

~~SRS-408~~ TDCIS Components (with the exception of PFE items) Management Interface shall be managed using:

- As a minimum:
  - Simple Network Management Protocol version 3 (SNMP v3) (IETF RFC 3410 – 3418, 2002); and,
  - RESTful API based configuration; and,
- Additionally one or multiple of the following:
  - HTTPS, TLS (as a minimum version 1.2 and 1.3):
    - RFC2616:1999, Hypertext Transfer Protocol – HTTP/1.1; and,
    - RFC2818:2000, HTTP Over TLS; and,
    - RFC5246:2008, the Transport Layer Security (TLS) Protocol Version 1.2; and,
    - RFC8446:2018, the Transport Layer Security (TLS) Protocol Version 1.3; and,
  - HyperText Transport Protocol (HTTP)(IETF RFC 7230, 2014); and,
  - Secure Shell Protocol (SSH) (IETF RFC 4251, 2006); and,
  - Windows Remote Management (WinRM); and,
  - Remote Desktop Protocol (RDP); and,
  - Keyboard, Video and Mouse (KVM) over Ethernet.

SRS (PRTTDCIS-3040)

~~SRS-409~~ Should it be required, use of SNMPv1 shall be solely limited to the integration of some PFE elements.

SRS (PRTTDCIS-1358)

~~SRS-410~~ TDCIS SMC shall include an Automatic system for startup and shut down functions to allow the coordinated start up, reboot or shut down of the system.

SRS (PRTTDCIS-2968)

~~SRS-411~~ The command signals for the automatic system startup, shut down and reboot actions shall be triggered whether by the System Administrator or automatically from other elements (e.g. Element Management Tool Suite for UPS, ECU, etc.).

SRS (PRTTDCIS-1349)

~~SRS-412~~ The TDCIS SMC shall monitor and control the temperature of all elements of the system and trigger a graceful system shutdown when the temperature is above the maximum acceptable system limit and the ECU is not providing enough cooling capacity.

SRS (PRTTDCIS-4400)

~~SRS-413~~ It shall be possible for the System Administrator to disable independently any TDCIS SMC automated graceful system shutdown feature.

SRS (PRTTDCIS-1351)

~~SRS-414~~ The TDCIS SMC shall implement logically separated management networks isolated from the operational data network.

SRS (PRTTDCIS-1353)

~~SRS-415~~ The TDCIS SMC shall allow the detection, analysis, isolation and the possibility to perform correction measures of faulty or malfunctioning components, modules or services.

4.5.2 Element Management

SRS (PRTTDCIS-2942)

~~SRS-416~~ The following figure illustrates the Element Management Tool Suite in context with which it shall comply.

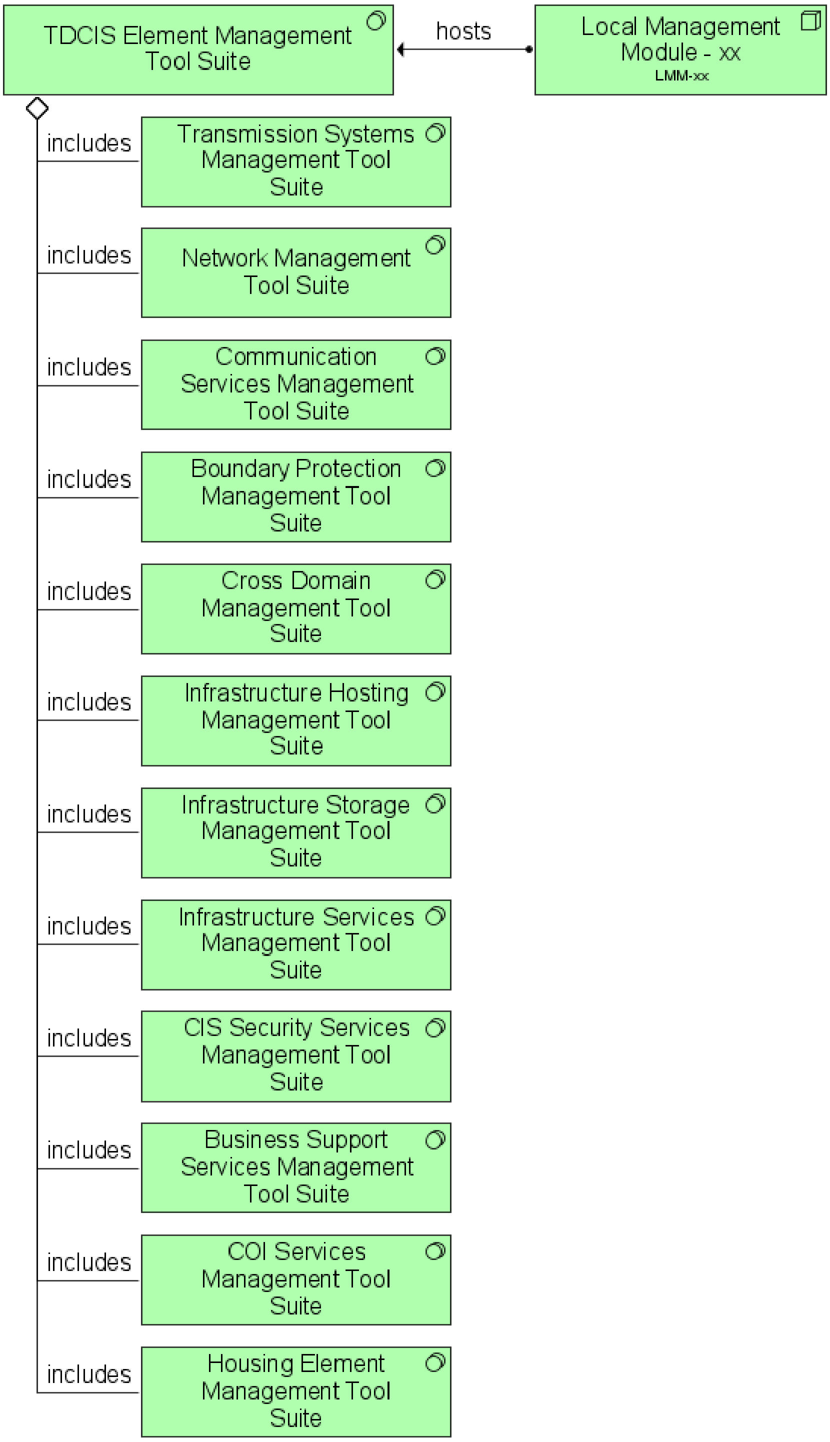
TDCIS Element Management Tool Suite
hosts
Local Management Module - xx
LMM-xx
includes
Transmission Systems Management Tool Suite
includes
Network Management Tool Suite
includes
Communication Services Management Tool Suite
includes
Boundary Protection Management Tool Suite
includes
Cross Domain Management Tool Suite
includes
Infrastructure Hosting Management Tool Suite
includes
Infrastructure Storage Management Tool Suite
includes
Infrastructure Services Management Tool Suite
includes
CIS Security Services Management Tool Suite
includes
Business Support Services Management Tool Suite
includes
COI Services Management Tool Suite
includes
Housing Element Management Tool Suite

Figure 48 - Element Management Tool Suite in context

SRS (PRTTDCIS-2943)

~~SRS-417~~ The Element Management Tool Suite shall contain all tools and software to Manage, Monitor and Configure:

1) Transmission System Elements; and
2) Network Elements; and
3) Communication Services Elements; and
4) Boundary Protection Elements; and
5) Cross Domain Elements; and
6) Infrastructure Hosting Elements; and
7) Infrastructure Storage Elements; and
8) Infrastructure Services Elements; and
9) CIS Security Services Elements; and,
10) Business Support Services Elements; and,
11) COI Services Elements; and,
12) Housing Elements.

SRS (PRTTDCIS-2944)

~~SRS-418~~ The Element Management Tool Suite shall integrate PFE Management and Configuration tools related to PFE components.

SRS (PRTTDCIS-2945)

~~SRS-419~~ The Local Management Module (LMM) shall host security domain specific components of the Element Management Tool Suite.

SRS (PRTTDCIS-2947)

~~SRS-420~~ Access to Element Management Tool Suite components (with the exception PFE elements) shall preferably be implemented as a web-based service, accessed through a standard web browser, as a minimum Microsoft Edge (latest version in use in PRT MOD) without the need of special browser add-ons. Any special functionality shall be provided through HTML5.

SRS (PRTTDCIS-2960)

~~SRS-421~~ The LMM-BLK shall host Element Management Tool Suite components related to TDCIS elements as illustrated on following picture.

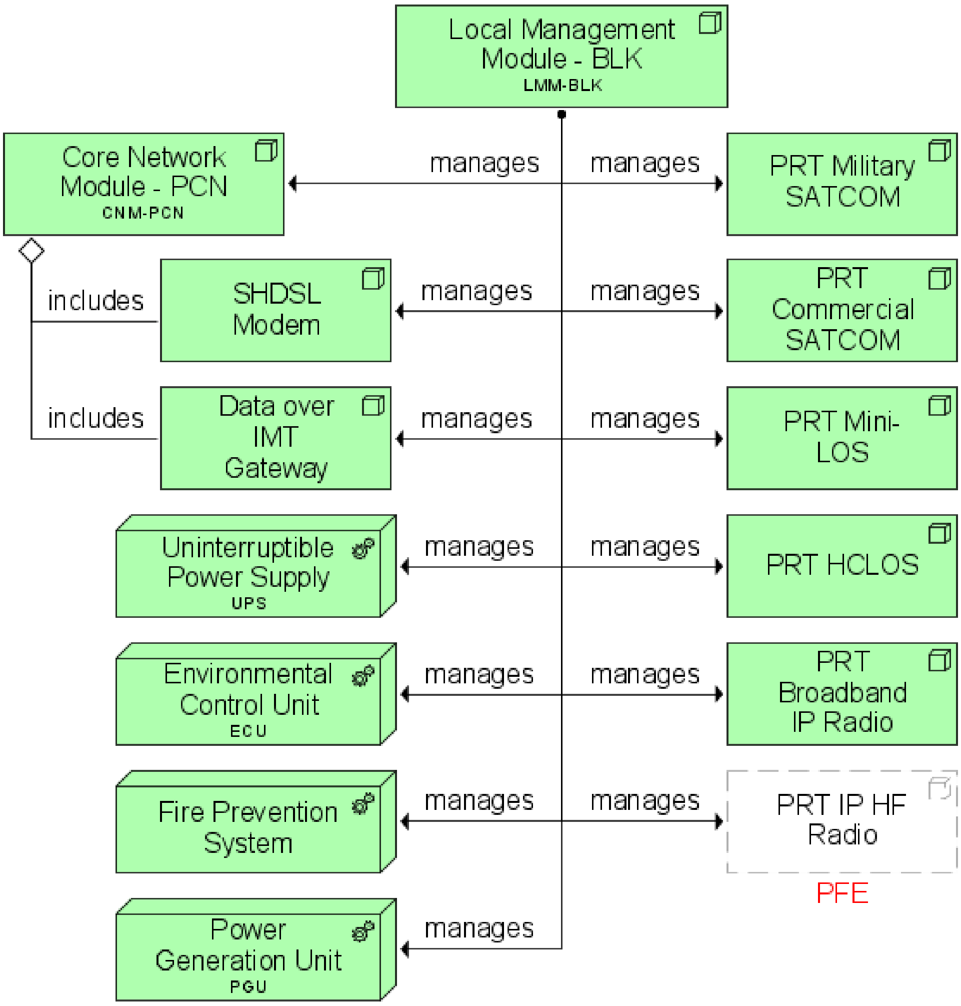

Figure 49 - LMM-BLK Element Management scope.

SRS (PRTTDCIS-2963)

~~SRS-422~~ The LMM-xU shall host Element Management Tool Suite components related to TDCIS elements as illustrated on following picture.

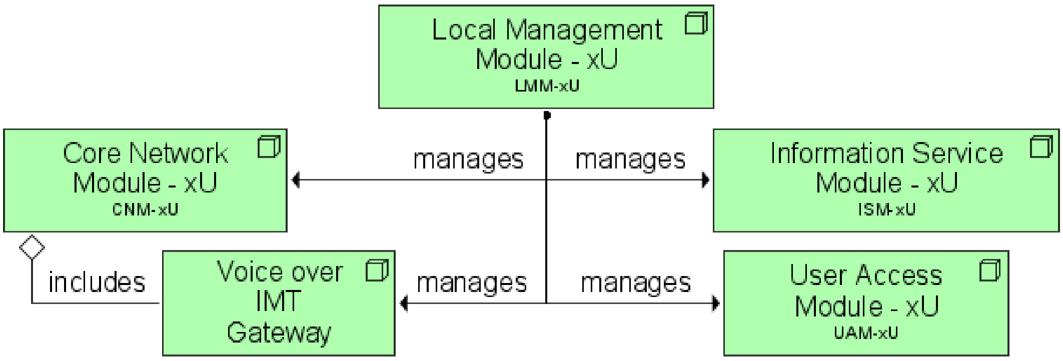

Figure 50 - LMM-xU Element Management scope.

SRS (PRTTDCIS-2964)

~~SRS-423~~ The LMM-xR shall host Element Management Tool Suite components related to TDCIS elements as illustrated on following picture.

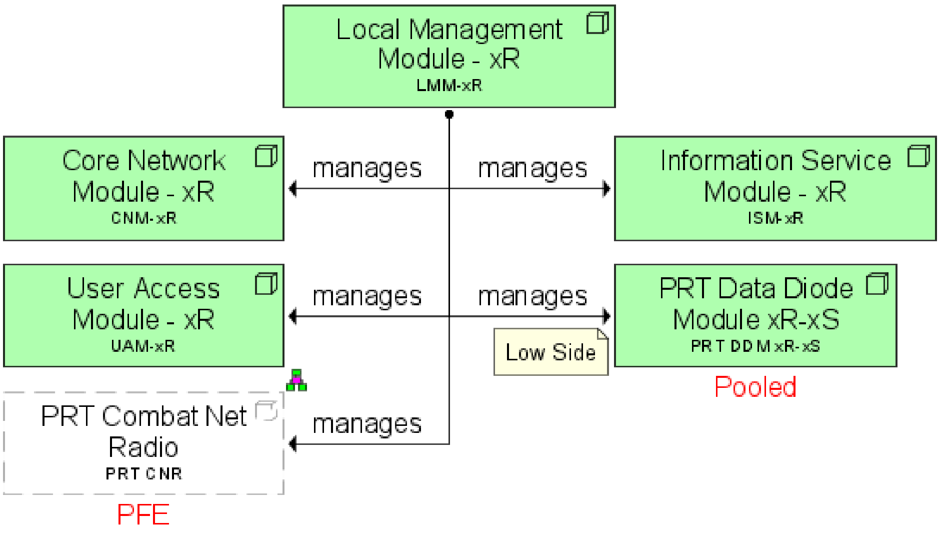

Figure 51 - LMM-xR Element Management scope.

SRS (PRTTDCIS-2965)

~~SRS-424~~ The LMM-xS shall host Element Management Tool Suite components related to TDCIS elements as illustrated on following picture.

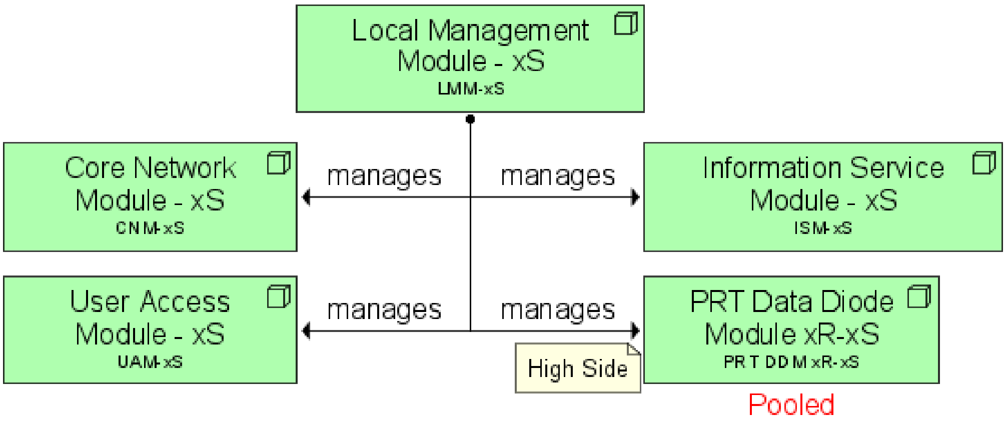

Figure 52 - LMM-xS Element Management scope.

SRS (PRTTDCIS-2972)

~~SRS-425~~ The LMM-NS shall host Element Management Tool Suite components related to TDCIS elements as illustrated on following picture.

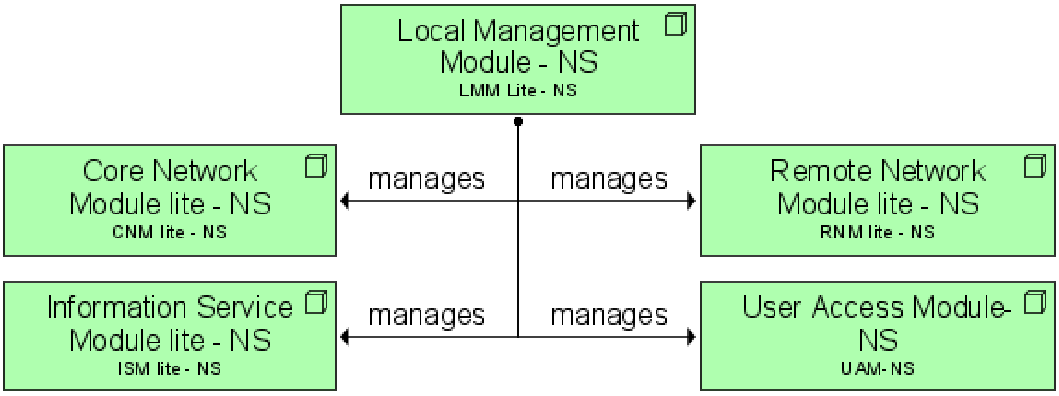
Local Management Module - NS
LMM Lite - NS
Core Network Module lite - NS
CNM lite - NS
manages
manages
Remote Network Module lite - NS
RNM lite - NS
Information Service Module lite - NS
ISM lite - NS
manages
manages
User Access Module- NS
UAM- NS

Figure 53 - LMM-NS Element Management scope.

SRS (PRTTDCIS-3036)

~~SRS-426~~ Element Management Tool Suite shall support integration with the pooled Portable Rugged Spectrum Analyzer.

SRS (PRTTDCIS-4647)

~~SRS-427~~ Element Management Tool Suite shall integrate with the Military SATCOM Terminal Embedded Spectrum Analyser.

SRS (PRTTDCIS-2974)

~~SRS-428~~ The Element Management Tool suite implementation in a Node shall be limited to the sole components and services hosted in this Node.

4.5.3 Node Monitoring

SRS (PRTTDCIS-2955)

~~SRS-429~~ The following figure illustrates the Node Monitoring Tool Suite per security domains in context with which it shall comply.

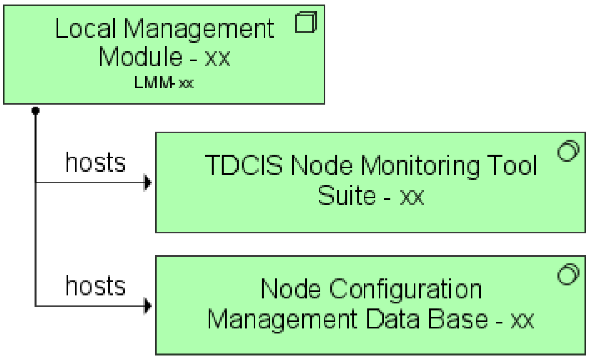
Local Management Module - xx
LMM-xx
hosts
TDCIS Node Monitoring Tool Suite - xx
hosts
Node Configuration Management Data Base - xx

Figure 54 - Node Monitoring Tool Suite in context

SRS (PRTTDCIS-2956)

~~SRS-430~~ The Node Monitoring Tool Suite shall contain all tools and software to:

1) Visualize all services health status for the Node; and
2) Alert System Administrator of Service outages; and
3) Allow System administrator to Identify and Isolate Service outage root cause; and
4) Report Service Performance live (i.e. near real-time) and using time filtered reports based on stored historical data.

SRS (PRTTDCIS-2958)

~~SRS-431~~ The Node Monitoring Tool Suite shall automatically pre-populate a set of views based on the information available in the CMDB.

SRS (PRTTDCIS-2959)

~~SRS-432~~ The Node Monitoring Tool Suite shall allow System Administrator to create custom views.

SRS (PRTTDCIS-2961)

~~SRS-433~~ Where and when possible, the Node Monitoring Tool Suite shall integrate with the Element Management Tool Suite, without any custom development other than software configuration, to quickly and easily access component-specific tools and software.

SRS (PRTTDCIS-1360)

~~SRS-434~~ Node Monitoring Tool Suite shall inform about the actual State of Charge (SOC) of the battery, the Estimated Time to Empty (ETE) of the battery and other relevant data of the Shelter UPS.

SRS (PRTTDCIS-2950)

~~SRS-435~~ Access to Node Monitoring Tool Suite components shall be implemented as a web-based service, accessed through a standard web browser, as a minimum Microsoft Edge (latest version in use in PRT MOD) without the need of special browser add-ons. Any special functionality shall be provided through HTML5.

SRS (PRTTDCIS-2975)

~~SRS-436~~ The Node Monitoring Tool Suite implementation in a Node shall be limited to the sole components and services hosted in this Node.

5 Modules

5.1 General

NOTE (PRTTDCIS-2560)

~~[121]~~ Where not specified explicitly, xU, xR and xS variants of modules will be fiber-based wired.

SRS (PRTTDCIS-2561)

~~SRS-437~~ xU, xR and xS variants of modules connections to EUD shall be Eth-Cu

SRS (PRTTDCIS-2559)

~~SRS-438~~ NS Kit modules shall be fiber-based wired, including the connections to EUD.

SRS (PRTTDCIS-2698)

~~SRS-439~~ All module components storage media (e.g. Hard Drives, Flash Drives...) shall be easily accessible and quickly removable from their hosting parent without having to remove or dismount any asset.

5.2 Core Network Module

5.2.1 Functional Requirements

SRS (PRTTDCIS-1666)

~~SRS-440~~ Each Core Network Module (CNM) shall provide wide area network connectivity to:

1) The PRT static infrastructure, via terrestrial lines or over Military SATCOM (from RL), anchoring the links at the PRT Satellite Ground Stations (SGS); and simultaneously,
2) The Core Network Modules of other TDCIS Nodes.

SRS (PRTTDCIS-1665)

~~SRS-441~~ Each Core Network Module shall provide local area and Metro-Area Network (MAN) connectivity to:

1) Information Services Module (ISM); and,
2) Data Diode Module (DDM) connecting two CNM-xx from two different security domains; and,
3) User Access Module (UAM), where local users connect; and,
4) Points of Presence (PoP) of collocated Mission Partner nations in the mission network environment as per FMN framework; and,
5) Protected Core Network (PCN) connectivity to other PCN participants.

NOTE (PRTTDCIS-1529)

~~[122]~~ The CNM implements the following functions in support of deployable instances of Communications Services:

1) Protected Core Access function; and,
2) Coloured Cloud Access function; and,
3) Multimedia Access function; and,
4) Boundary Protection function.

SRS (PRTTDCIS-1639)

~~SRS-442~~ The detailed system design of the CNM shall map each of the functions specified into subsystems (or functional building blocks) by the same name (i.e. PCA, CCA, MMA and BPS) and adhere to the subsystems breakdown presented on the following picture:

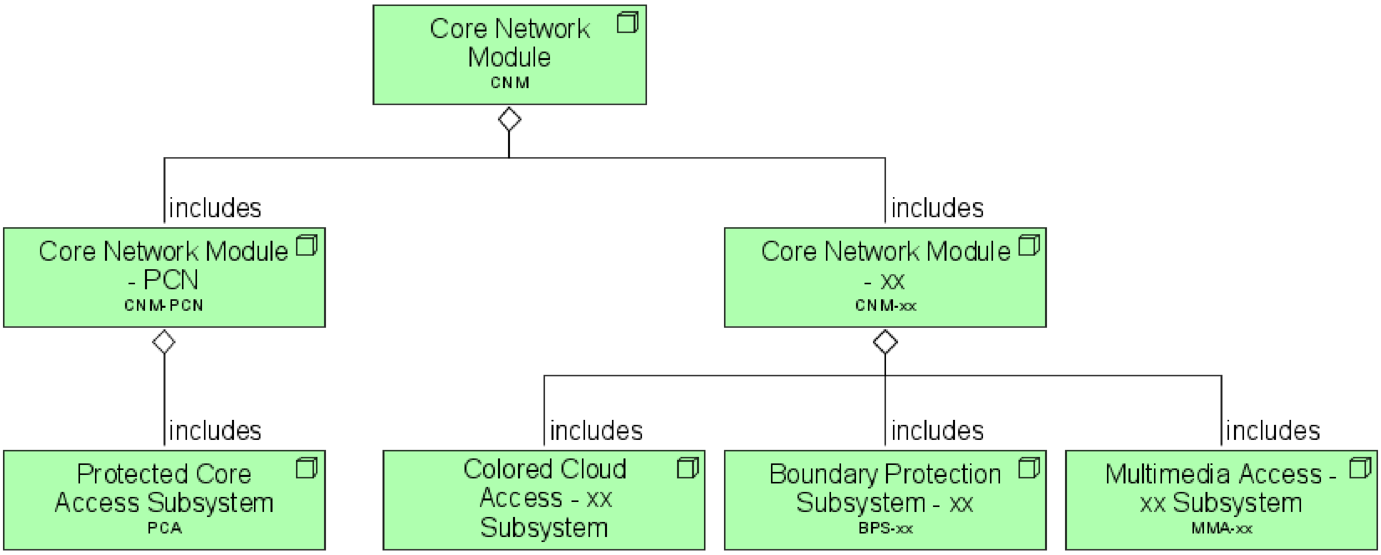
Core Network Module
CNM
includes
includes
Core Network Module - PCN
CNM-PCN
Core Network Module - xx
CNM-xx
includes
includes
includes
includes
Protected Core Access Subsystem
PCA
Colored Cloud Access - xx Subsystem
Boundary Protection Subsystem - xx
BPS-xx
Multimedia Access - xx Subsystem
MMA-xx

Figure 55 - CNM breakdown

SRS (PRTTDCIS-3121)

~~SRS-443~~ Colour Clouds encrypted traffic shall be transported by the Protected Core Network (PCN).

NOTE (PRTTDCIS-4091)

~~[123]~~ PCN is a specific implementation of the BLK Network.

SRS (PRTTDCIS-1530)

~~SRS-444~~ The **Protected Core Access (PCA)** function of the CNM shall:

1) Aggregate and distribute traffic across the diverse Transmission Systems on the DCIS Protected Core (e.g. SATCOM, HCLOS radio, fiber, etc. where available), using IP unicast and IP multicast routing; and,
2) Implement the DCIS Protected Core, providing wide-area transport services in support of the Coloured Cloud Access (CCA) function, both intra-theatre towards other TDCIS Nodes, as well as into the PRT static infrastructure (via the RL); and,
3) Implement Multiprotocol Label Switching - Traffic Engineering (MPLS-TE) in order to assure end-to-end Quality and Class of Service across the WAN, for the flows of CCA functions of different classifications, and for the flows within each CCA function and security classification.

SRS (PRTTDCIS-1531)

~~SRS-445~~ The **Coloured Cloud Access (CCA)** function of the CNM shall, for each security domain:

1) Connect to the PCA function using a Security accredited commercial grade IPSec function (for the CCA-xU and CCA-xR); and,
2) Connect to the PCA function using a PRT Nationally accredited high-grade IP Crypto function (for the CCA-Nat-S); and,
3) Connect to the PCA function using a NATO accredited high-grade IP Crypto function (for the CCA-MS and CCA-NS); and,
4) Provide the core switching capability, acting as a hub for the MMA, DDM and BPS functions; and,
5) Provide the HDS function for the ISMs; and,
6) Use an Interior Gateway Protocol (IGP) to converge routing information within the Coloured Cloud; and,
7) Provide IP access (LAN) and IP transport (WAN) to the Multimedia Access function of the CNM, Information Services modules (ISM) and User Access Modules (UAM) within the TDCIS Node; and,
8) Provide IP access (LAN) to the Boundary Protection function in the CNM, such that IP flows from/to the local ISM, UAM and MMA, as well as the flows from/to the WAN (other TDCIS Nodes) can be routed through it and protected accordingly; and,
9) Implement traffic classification and marking, traffic conditioning and dynamic IP routing at the edges of the network; and,
10) Support IP interworking with collocated Mission Network Participants (MNP), over a Network Interconnection Point (NIP), compliant with FMN framework.

SRS (PRTTDCIS-1532)

~~SRS-446~~ The **Multimedia Access (MMA)** function of the CNM shall, for each security domain:

1) Provide local users with multimedia access for IP Telephony, voice mail and secure voice conferencing support, at xU, xR and xS levels, using the CCA function for transport; and,
2) Implement an IP telephony service that enables users at a TDCIS Node to intercommunicate with other users in other TDCIS Nodes, MNP nodes, or in the PRT static infrastructure, within the same security domain; and,
3) Support multi-protocol signaling (i.e. SIP, H.323) and media (i.e. DTMF, fax) interworking, codec transcoding, voice and video conferencing; and,
4) Terminate and relay media streams, address and port translations (Topology Hiding); and,
5) Feature a Session Border Controller (SBC) capability to enable voice and video (V2) services federation with third party V2 network at xU and xS levels, over the NIP of the CCA function; and,
6) Use Call Admission Control (CAC) to prevent oversubscription of bandwidth across the WAN trunks that would degrade voice quality; and,
7) Support Multi-Level Precedence Pre-emption (MLPP) across the WAN trunks to ensure best use of the available bandwidth, with four levels of priority (Flash Override, Flash, Intermediate, Priority, Routine); and,
8) Support user-initiated subscriber extension mobility; and,
9) Implement a Gateway for IMT networks Voice service integration with IP Telephony service in the xU security domain; and,
10) Implement a Gateway for IRIDIUM Push To Talk integration in the xU security domain; and,
11) Implement a Gateway for Radio over IP integration, enabling Push To Talk (PTT) analogue audio communication through the VoIP network in the xU security domain; and,
12) Implement a Gateway for Radio over IP integration, enabling PTT communication through the xR-VoIP network and the CNR Voice network in the xR security domain; and,
13) Implement an Analogue Telephony service integrated with the TDCIS IP Telephony service in the xU security domain; and,
14) Federation to MNP according to FMN framework; and,
15) Unified Communication and Collaboration (UCC) capabilities in the form of integrated Video, Audio and Content Sharing; and,
16) Provide Auto attendant and contact center features with multiple greetings and structured menu functionality; and,
17) Provide Call Detail Record (CDR) reports; and,
18) Provide survivable remote node IP telephony service in case the main call processing device; i.e. Communication server is not reachable or down.

SRS (PRTTDCIS-1533)

~~SRS-447~~ The **Boundary Protection (BPS)** function of the CNM shall, for each security domain:

1) Implement the Self-protecting Node principle and protect the following LAN, WAN and MAN traffic flows using port-based or/and AppID inspection on the flows:
    1) UAM to local ISM (LAN); and,
    2) UAM to local MMA function (LAN); and,
    3) ISM to remote ISM or to PRT static infrastructure, over the CCA and PCA functions (WAN); and,
    4) UAM to remote ISM, over the CCA and PCA functions (WAN); and,
    5) NIP to ISM; and,
    6) ISM to DDM (LAN); and,
2) Be able to detect malicious activity by implementing a Network Intrusion Detection System (NIDS) functionality; and,
3) Implement the cross domain service between xU and xR.

NOTE (PRTTDCIS-3330)

~~[124]~~ As defined in D48Rev3 , a Self-Protecting CIS is to be understood as each CIS treating other CIS as un-trusted and implementing protection measures to control the exchange of information with other CIS.

5.2.2 Technical Requirements

5.2.2.1 PCA subsystem

5.2.2.1.1 General

NOTE (PRTTDCIS-3049)

~~[125]~~ The following picture illustrates the PCA in context.

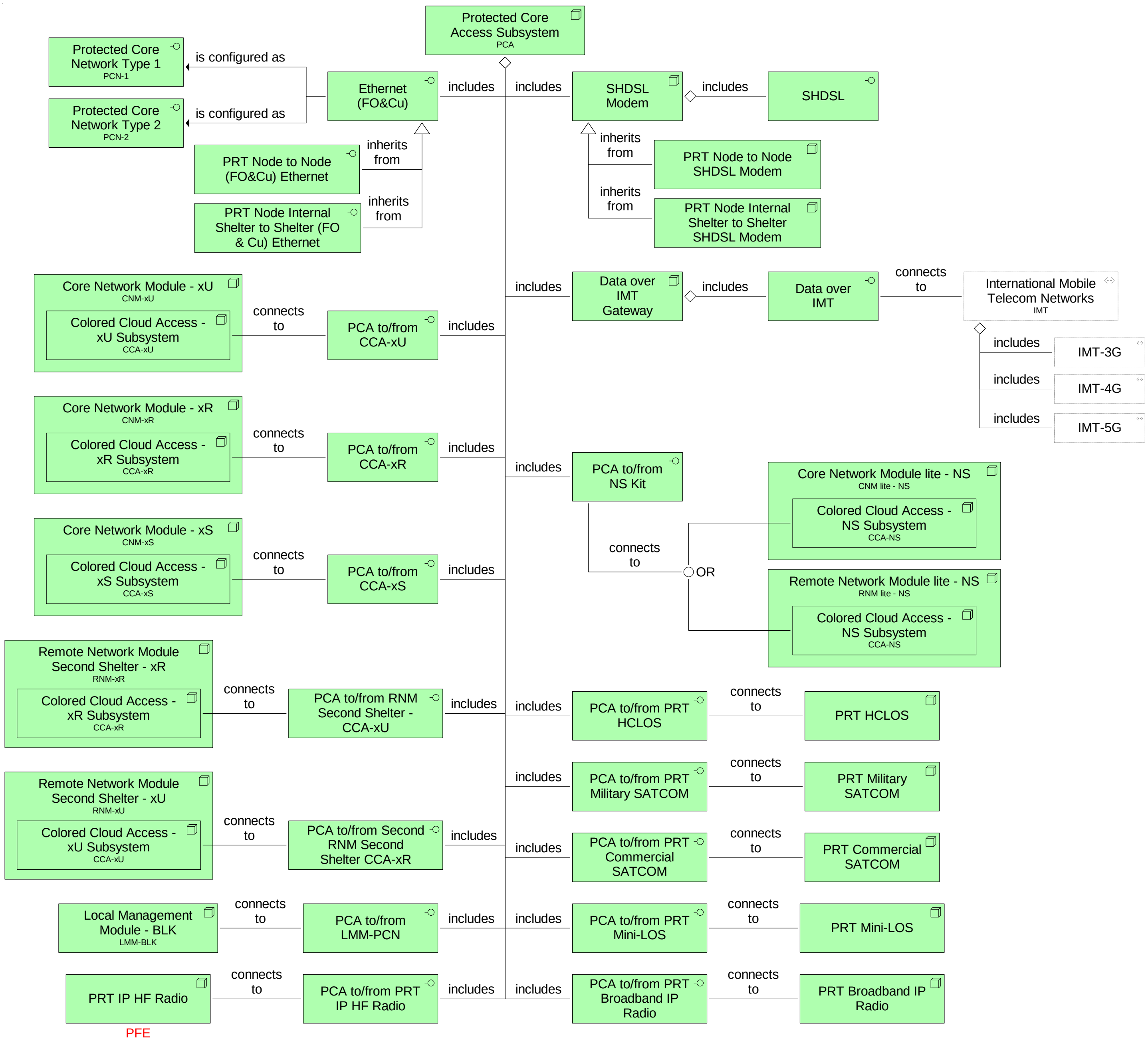

Figure 56 - PCA in context

SRS (PRTTDCIS-1535)

~~SRS-448~~ The PCA subsystem shall implement the PCA functions.

SRS (PRTTDCIS-1289)

~~SRS-449~~ The PCA shall include a data gateway to International Mobile Telecommunication (IMT) Networks.

SRS (PRTTDCIS-2097)

~~SRS-450~~ The PCA shall include Symmetric High speed Digital Subscriber Line (SHDSL) modems that enable high speed communications over single unloaded and unconditioned twisted copper pairs, of the type used in the local telephone distribution plant.

SRS (PRTTDCIS-2098)

~~SRS-451~~ The SHDSL shall be compliant with ITU-T G.991.2 Annexes B, F and G.

SRS (PRTTDCIS-1536)

~~SRS-452~~ The PCA subsystem shall deliver MPLS-based IP transport services to the xS, xR and xU IP routed security domains (implemented by the respective CCA subsystems).

SRS (PRTTDCIS-1537)

~~SRS-453~~ The PCA subsystem shall perform the Provider Edge (PE) function of the MPLS WAN, and support MP-BGP.

SRS (PRTTDCIS-1538)

~~SRS-454~~ The PCA subsystem shall forward packets to and from each CCA subsystems based on labels.

SRS (PRTTDCIS-1539)

~~SRS-455~~ The PCA subsystem shall use MPLS to implement Traffic Engineering through Label-Switched Paths (LSP). LSP are logical paths established over multiple transmission media. A given logical path may involve one or more Transmission Systems.

SRS (PRTTDCIS-1540)

~~SRS-456~~ The PCA subsystem shall use an internal routing protocol which shall be configured in all WAN interfaces in support of the exchange of control-plane information. This includes:

1) IP reachability information; and,
2) MPLS traffic engineering metrics; and,
3) BGP next-hop reach ability.

SRS (PRTTDCIS-1542)

~~SRS-457~~ Label Distribution Protocol (LDP) shall be used within the MPLS core to facilitate MPLS VPN services.

SRS (PRTTDCIS-1543)

~~SRS-458~~ The PCA subsystem shall use its IGP to carry topology information for the WAN links, its loopback interfaces (which are the end-points for MPLS LSPs), its physical interfaces, used for the IPSec tunnels for the xU, xR and xS access networks (e.g. the interfaces facing the black IP port of the TCE-621B).

SRS (PRTTDCIS-1544)

~~SRS-459~~ The PCA subsystem shall implement different LSPs to carry traffic internal, amongst TDCIS Nodes and towards the PRT static infrastructure, and FMN traffic transiting between NIPs.

SRS (PRTTDCIS-1545)

~~SRS-460~~ The PCA subsystem interfaces for IPSec tunnel end-points shall be set as "passive" in the IGP as they are Protected Core Edge connections.

SRS (PRTTDCIS-2312)

~~SRS-461~~ There shall be no IP routing exchange between the Protected Core and the xU, xR and xS networks.

SRS (PRTTDCIS-1546)

~~SRS-462~~ The PCA subsystem shall implement IPv4 and IPv6 multicast routing through PIM-SM, PIM-SSM and MLDv2.

SRS (PRTTDCIS-1547)

~~SRS-463~~ Rendezvous points shall be anycasted in accordance with RFC4610. Geographically RP redundancy shall be implemented.

SRS (PRTTDCIS-1548)

~~SRS-464~~ For IPv4 multicast, the anycasted rendezvous points shall use Multicast Source Discovery Protocol (MSDP).

SRS (PRTTDCIS-1549)

~~SRS-465~~ For IPv4 multicast, when BGP-4 is used across interoperability interfaces, MSDP shall peer using the same source and destination addresses as the external BGP peering session.

SRS (PRTTDCIS-1550)

~~SRS-466~~ For IPv4 multicast, MSDP shall be configured to source from the loopback addresses on internal BGP peering sessions.

SRS (PRTTDCIS-1551)

~~SRS-467~~ The PCA subsystem shall support IP throughput performances up to 1 Gbps and 5 Gbps, with and without IPSec encryption, respectively.

SRS (PRTTDCIS-1552)

~~SRS-468~~ The PCA subsystem shall be able to simultaneously connect to all the Transmission Systems.

SRS (PRTTDCIS-1555)

~~SRS-469~~ The PCA subsystem shall, as a minimum, implement interfaces to the WAN/MAN and to other subsystems within the CNM, as per the table below. The need for additional interfaces, or interfaces different from those listed below, including internal interfaces within the PCA subsystem, if required, as well as their specification, shall be design-driven and shall be justified, based on component selection and functionality sought.

Interface Name	Qty.	Interface Type	Interface Speed	Remarks
SHDSL	2	N/A	N/A	Same interface can be used for Node to Node as well as for Shelter to Shelter (internal to a dual Shelter Node) connectivity.
Data over IMT	1	N/A	N/A	N/A
Ethernet (FO and Cu)	4	Eth-Cu Eth-FO-LR	100/1000Mbps 1Gbps	SFP based supporting both RJ45 and fibre for 100/1000Mbps Interface is either configured as PCN-1 or PCN-2 Same interface can be used for Node to Node as well as for Shelter to Shelter (internal to a dual Shelter Node) connectivity.
PCA to/from PRT Mini LOS	3	Design Driven	Design Driven	N/A
PCA to/from PRT HCLOS	4	Design Driven	Design Driven	N/A
PCA to/from PRT Broadband IP Radio	1	Design Driven	Design Driven	N/A
PCA to/from PRT Commercial SATCOM	1	Design Driven	Design Driven	N/A

Interface Name	Qty.	Interface Type	Interface Speed	Remarks
PCA to/from PRT Military SATCOM	1	Design Driven	Design Driven	N/A
PCA to/from PRT IP HF Radio	1	Eth-Cu	10BaseT	N/A
PCA to/from CCA-xS	1	Eth-FO-SR	10/100/1000Mbps	Interface to TCE-621B
PCA to/from CCA-xR	1	Eth-FO-SR	1Gbps	N/A
PCA to/from CCA-xU	1	Eth-FO-SR	1Gbps	N/A
PCA to/from RNM Second Shelter -CCA-xU	1	Eth-FO-SR	1Gbps	This Interface may use the same physical port as the PCA to/from CCA-xU
PCA to/from Second RNM Second Shelter CCA-xR	1	Eth-FO-SR	1Gbps	This Interface may use the same physical port as the PCA to/from CCA-xR
PCA to/from NS Kit	2	Eth-FO-LR	1Gbps	Interface can be connected to the TCE621M of the CCA-NS of a Core Node Lite or of a Remote Node Lite
PCA to/from LMM-PCN	N	Eth-Cu	1Gbps	N is Design Driven with a minimum of 2 interfaces to connect Sys Admin Workstations.

Table 28 - PCA subsystem interfaces

SRS (PRTTDCIS-1668)

~~SRS-470~~ All PCA across TDCIS Nodes shall be identical, therefore, the computation of interface quantities have taken into consideration the largest connections possible.

SRS (PRTTDCIS-1556)

~~SRS-471~~ The PCA subsystem shall implement additional interfaces, as required and as driven by the design, in support of service management and control functionalities.

NOTE (PRTTDCIS-1557)

~~[126]~~ Additional interfaces may be implemented to accommodate other connections and end-points resulting from the detailed design.

SRS (PRTTDCIS-1558)

~~SRS-472~~ Any routers and switches in the PCA subsystem shall be duly sized and licensed in order to meet the functional and technical requirements above.

SRS (PRTTDCIS-1248)

~~SRS-473~~ The PCA shall support the E-Node functionality in support of the Protected Core Network (PCN) specification, in accordance with STANAG-5637.

SRS (PRTTDCIS-1244)

~~SRS-474~~ In order to be an E-Node in the PCN context, the PCA shall support following services and their federation with other affiliates of the PCN:

- Domain Name Server (DNS); and,
- Authentication, Authorisation & Accounting (AAA); and,
- Network Time Protocol (NTP); and,
- Public Key Infrastructure (PKI); and,
- Interface to the Network Management / Cyber Defence System.

5.2.2.1.2 Data over IMT Gateway

NOTE (PRTTDCIS-4111)

~~[127]~~ The PCA Data IMT Gateway is an IMT-UE.

NOTE (PRTTDCIS-4112)

~~[128]~~ The purpose of the PCA Data IMT Gateway, along with the underlying IMT Network Access Service, is to interconnect the TDCIS with the PRT NDN Infrastructure, primarily via public IMT networks.

NOTE (PRTTDCIS-4144)

~~[129]~~ The IMT Network Access Service (i.e. SIM cards and subscription) is not a project deliverable.

SRS (PRTTDCIS-4113)

~~SRS-475~~ The PCA Data IMT Gateway shall consist of Outdoor Elements and Indoor Elements.

SRS (PRTTDCIS-4114)

~~SRS-476~~ The PCA Data IMT Gateway shall support Public and Private IMT networks.

SRS (PRTTDCIS-4115)

~~SRS-477~~ The PCA Data IMT Gateway shall be compatible with IMT Network Access Service implementing Private Access Point Name (APN).

SRS (PRTTDCIS-4135)

~~SRS-478~~ The PCA Data IMT Gateway shall implement Multiple Input Multiple Output (MIMO) techniques.

SRS (PRTTDCIS-4136)

~~SRS-479~~ The PCA Data IMT Gateway shall support a minimum of TWO (02) MIMO layers.

SRS (PRTTDCIS-4116)

~~SRS-480~~ The PCA Data IMT Gateway shall support a minimum of TWO (02) independent antenna elements.

SRS (PRTTDCIS-4117)

~~SRS-481~~ The antenna shall be able to operate across all frequency bands specified.

SRS (PRTTDCIS-4118)

~~SRS-482~~ The antenna elements shall be detachable and replaceable by a System Administrator.

SRS (PRTTDCIS-4119)

~~SRS-483~~ The PCA Data IMT Gateway antenna shall be mounted outside, on the Shelter.

SRS (PRTTDCIS-4123)

~~SRS-484~~ The PCA Data IMT Gateway shall support Dual Subscriber Identity Module (SIM) Card.

SRS (PRTTDCIS-4124)

~~SRS-485~~ SIM-based carrier selection shall be automatic without requiring any System Administrator action.

SRS (PRTTDCIS-4125)

~~SRS-486~~ The PCA Data IMT Gateway shall support IPv4 and IPv6 dual stack.

SRS (PRTTDCIS-4126)

~~SRS-487~~ The PCA Data IMT Gateway shall implement 3G/IMT2000 and 4G/IMT-Advanced compliant Radio Access Technology (RAT) including, as a minimum:

- 3GPP's UMTS Release 7 (HSPA+); and,
- 3GPP's LTE Release 11 (LTE Advanced); and,
- LTE IMT-UE Category 11.

SRS (PRTTDCIS-4620)

~~SRS-488~~ The PCA Data IMT Gateway shall implement 5G/IMT-2020 compliant RAT including, as a minimum:

- 3GPP's LTE Release 13 (LTE Advanced Pro); and,
- 3GPP's 5G Release 15 (5G NR) in Frequency Range 1 (FR1); and,
- 5G+LTE dual connectivity.

SRS (PRTTDCIS-4128)

~~SRS-489~~ The PCA Data IMT Gateway shall primarily operate with LTE technology and fall back automatically to UMTS technology.

SRS (PRTTDCIS-4129)

~~SRS-490~~ The fall back to UMTS technology shall depend on the RAN technology propagation and coverage conditions, without requiring any System Administrator action.

SRS (PRTTDCIS-4622)

~~SRS-491~~ The PCA Data IMT Gateway shall primarily operate with LTE technology and switch automatically to 5G technology when in coverage.

SRS (PRTTDCIS-4623)

~~SRS-492~~ The switch to 5G technology shall depend on the RAN technology propagation and coverage conditions, without requiring any operator action.

SRS (PRTTDCIS-4132)

~~SRS-493~~ The PCA Data IMT Gateway shall implement Roaming techniques.

SRS (PRTTDCIS-4133)

~~SRS-494~~ Any kind of Roaming shall be automatic without requiring any System Administrator action.

SRS (PRTTDCIS-4134)

~~SRS-495~~ The PCA Data IMT Gateway shall implement Carrier Aggregation (CA) techniques.

SRS (PRTTDCIS-4137)

~~SRS-496~~ The PCA Data IMT Gateway shall implement global coverage, supporting the adopted bands in the regions of Europe, Africa/Middle East, Asia and Pacific.

SRS (PRTTDCIS-4138)

~~SRS-497~~ The PCA Data IMT Gateway shall implement a minimum of ONE (01) 3GPP UMTS band per region.

SRS (PRTTDCIS-4139)

~~SRS-498~~ The PCA Data IMT Gateway shall implement a minimum of TWO (02) 3GPP LTE bands per region.

SRS (PRTTDCIS-4626)

~~SRS-499~~ The PCA Data IMT Gateway shall implement a minimum of ONE (01) 3GPP 5G NR FR1 band per region.

SRS (PRTTDCIS-4142)

~~SRS-500~~ The PCA Data IMT Gateway shall implement a Human Machine Interface (HMI) interface that allows monitoring and control of the PCA Data IMT Gateway by a System Administrator.

SRS (PRTTDCIS-4143)

~~SRS-501~~ The PCA Data IMT Gateway HMI shall provide the minimum following functionalities to System Administrators:

- A clock driven by the IMT Network; and,
- Enabling IMT Gateway parameters configuration; and,
- Collecting, Logging and Reporting Errors, Warnings and Alarms in a Human comprehensive format; and,
- Monitoring and reporting of the IMT Gateway operational status; and,
- MNO currently connected; and,
- Estimated uplink and downlink data rates; and,
- Signal strength.

5.2.2.2 CCA subsystem

NOTE (PRTTDCIS-3050)

~~[130]~~ The following picture illustrates the CCA in context.

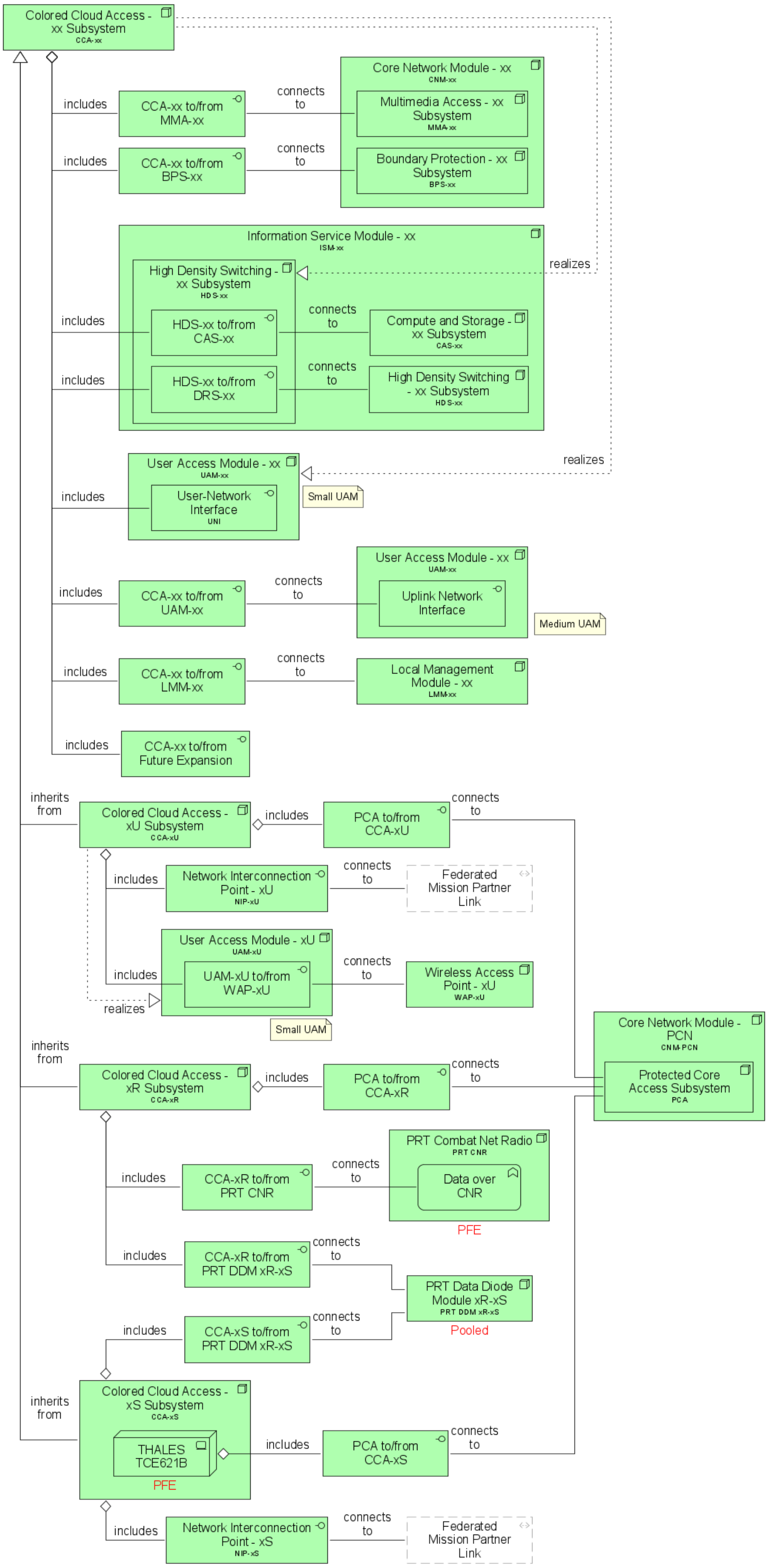

Figure 57 - CCA in context

NOTE (PRTTDCIS-1559)

~~[131]~~ The CCA subsystem exists in three different variants: CCA-xU, CCA-xR and CCA-xS. The xU and xR variants are different from the other one in the sense that the corresponding module will not require dedicated crypto equipment.

SRS (PRTTDCIS-1560)

~~SRS-502~~ The CCA subsystem shall implement the CCA functions.

SRS (PRTTDCIS-1561)

~~SRS-503~~ The CCA subsystem shall implement IPv4/IPv6 dual stack.

SRS (PRTTDCIS-1563)

~~SRS-504~~ All CCA subsystems shall be built and licensed the same, irrespective of the security domain.

SRS (PRTTDCIS-1564)

~~SRS-505~~ The CCA subsystem shall use OSPFv2 as the IGP for IPv4 and OSPFv3 as the IGP for IPv6.

SRS (PRTTDCIS-1575)

~~SRS-506~~ The CCA subsystem shall use BGP4 as the EGP to interconnect interior routing domains (iBGP) and to dynamically advertise IP information over the NIP (eBGP).

SRS (PRTTDCIS-1565)

~~SRS-507~~ The CCA subsystem shall support IP multicast and fulfil all multicast-related requirements stated for the PCA subsystem.

SRS (PRTTDCIS-1566)

~~SRS-508~~ The CCA subsystem shall implement a tunneling architecture for transporting xS data between TDCIS Nodes. Tunnels shall provide point-to-point IP transport at a given QoS level, in turn determined by the link attributes of the underlying MPLS-TE tunnels (LSP) between the PCA subsystems.

SRS (PRTTDCIS-1567)

~~SRS-509~~ To allow dynamic routing updates between two connected TDCIS Nodes, a main End-to-End tunnel shall be created between CCAs.

SRS (PRTTDCIS-1568)

~~SRS-510~~ This tunnel acts as a logical interface to BGP and OSPF, and as the point-to-point transport interface connecting to other networks. All dynamic routing updates shall be sent and received through this tunnel.

NOTE (PRTTDCIS-1569)

~~[132]~~ Quality of Service (QoS) and Anti-Replay methods are performed inside the End-to-End tunnel and are transparent to the dynamic routing protocols. The per-QoS Encapsulating Security Protocol (ESP) between IP crypto equipment correspond to separate Virtual Crypto Units (VCU).

SRS (PRTTDCIS-1570)

~~SRS-511~~ For each End-to-End (E2E) Generic Routing Encapsulation (GRE) tunnel and for QoS purposes, five additional GRE tunnels shall be configured within the CCA subsystem, one for each QoS class. The routing design shall be implemented as follows:

1) QoS tunnels shall be established between CCA subsystem instances; and,
2) Traffic shall be first routed into the correct E2E tunnel by the dynamic routing protocol; and,
3) Once in the correct E2E tunnel, traffic shall then be routed into one of the associated five QoS-based GRE tunnels via static configuration. As this routing decision is based upon Differentiated Services Code Point (DSCP) and destination IP (with the destination being the tunnel endpoint of the chosen E2E GRE), Policy-Based Routing (PBR) and a separate Virtual Routing and Forwarding (VRF) instances are required; and,
4) Each QoS tunnel (mapped to a VCU) shall be associated with one or more (more in case of load balancing across cryptos) cryptographic tunnels and routed across the Protected Core Network accounting for the QoS requirements.

NOTE (PRTTDCIS-1571)

~~[133]~~ Cryptographic tunnels are established:

- between IP encryption equipment of the different CCA-xS; and,
- between Commercial grade crypto instances of the different CCA-xU; and,
- between Commercial grade crypto instances of the different CCA-xR.

SRS (PRTTDCIS-1576)

~~SRS-512~~ Over the NIP, each CCA subsystem shall transit multicast traffic on behalf of all Mission Network Participants (MNP).

SRS (PRTTDCIS-1578)

~~SRS-513~~ In order to fulfil end-to-end QoS for higher level services, IP performance within the CCA Subsystem shall be expressed as a maximum IP packet loss rate (IPLR), a maximum IP transfer delay (IPTD) and a maximum jitter (IPDV) and shall comply with parameters are as follows for the Real Time (RT) Voice and Video (V2) traffic:

- Latency ≤ 150 ms one-way; and,
- Jitter ≤ 30 ms; and,
- Loss ≤ 1%.

SRS (PRTTDCIS-1579)

~~SRS-514~~ The following QoS parameters for Inter-domain Multicast Source Discovery over the CCA subsystem shall be observed or tailored to fit mission-specific requirements: Application Type: Router (multicast source discovery).

SRS (PRTTDCIS-1580)

~~SRS-515~~ The following QoS parameters for Inter-domain Routing over the CCA subsystem shall be observed or tailored to fit mission-specific requirements: Application Type: Router (inter-domain routing).

SRS (PRTTDCIS-1581)

~~SRS-516~~ The following QoS parameters for Inter-domain Multicast Signaling over the CCA subsystem shall be observed or tailored to fit mission-specific requirements: Application Type: Router (multicast signaling).

SRS (PRTTDCIS-1582)

~~SRS-517~~ The following QoS parameters for Key negotiation and keepalives over the CCA subsystem shall be observed or tailored to fit mission-specific requirements: Application Type: Router (IPSec authentication and tunnel management).

SRS (PRTTDCIS-1583)

~~SRS-518~~ Over the NIP, the CCA subsystem shall provide multicast infrastructure based on PIMv2 Sparse-Mode signaling and Rendezvous points within each MN Communications Services Provider.

SRS (PRTTDCIS-1586)

~~SRS-519~~ Each individual CCA subsystem shall implement a core switching capability with buffers of minimum 16 MB, in order to prevent frame drops resulting from micro-bursts of traffic.

SRS (PRTTDCIS-1587)

~~SRS-520~~ Each individual CCA subsystem shall, as a minimum, implement interfaces to other subsystems within the Core Network Module as well as to external elements, as per the table below. The need for additional interfaces, or interfaces different from those listed below, as well as their specification, shall be design-driven and shall be justified, based on component selection and functionality sought.

Interface Name	Qty.	Interface Type	Interface Speed	Remarks
CCA-xx to/from MMA-xx	N	Design Driven	Design Driven	N is Design Driven
CCA-xx to/from BPS-xx	M	Design Driven	Design Driven	M is Design Driven through CCA switching core

Interface Name	Qty.	Interface Type	Interface Speed	Remarks
HDS-xx to/from CAS-xx	—	—	—	See HDS specifications
HDS-xx to/from DRS-xx	—	—	—	See HDS specifications
User Network Interface	2	—	—	To realize the small UAM See UAM section for specifications
CCA-xx to UAM-xx	2	Eth-FO-LR	Minimum 2Gbps	To connect to Medium UAM
CCA-xx to LMM-xx	Q	Design Driven	Design Driven	Q is Design Driven with a minimum of 2 interfaces to connect Sys Admin Workstations.
CCA-xx to Future Expansion	4	Eth-Cu Eth-FO-SR	100/1000Mbps 1Gbps	SFP based supporting both RJ45 and fibre for 100/1000Mbps
PCA to/from CCA-xU	1	Eth-FO-SR	1Gbps	only in CCA-xU direct interface on CCA routing platform
UAM-xU to/from WAP-xU	1	—	—	To realize the small UAM See UAM section for specifications
NIP-xU	1	Eth-FO-LR	1Gbps	only in CCA-xU direct interface on CCA routing platform
PCA to/from CCA-xR	1	Eth-FO-SR	1Gbps	only in CCA-xS direct interface on CCA routing platform
CCA-xR to/from PRT CNR	T	Design Driven	Design Driven	T is Design Driven For Data over CNR direct interface on CCA routing platform
CCA-xR to/from PRT DDM xR-xS	R	Design Driven	Minimum 1Gbps	R is Design Driven
PCA to/from CCA-xS	1	Eth-FO-SR	10/100/1000Mbps	Interface to TCE-621B only in CCA-xS direct interface on CCA routing platform
NIP-xS	1	Eth-FO-LR	1Gbps	only in CCA-xU direct interface on CCA routing platform
CCA-xS to/from PRT DDM xR-xS	S	Design Driven	Minimum 1Gbps	S is Design Driven

Table 29 - CCA subsystem interfaces

SRS (PRTTDCIS-1669)

~~SRS-521~~ All CCA across TDCIS Nodes shall be identical, therefore, the computation of interface quantities have taken into consideration the largest connections possible.

SRS (PRTTDCIS-1588)

~~SRS-522~~ Each CCA subsystem shall implement additional interfaces, as required and as driven by the design, in support of service management and control functionalities.

NOTE (PRTTDCIS-1590)

~~[134]~~ Additional interfaces may be implemented to accommodate other connections and end-points resulting from the detailed design.

SRS (PRTTDCIS-1591)

~~SRS-523~~ Any routers and switches in each CCA subsystem shall be duly sized and licensed in order to meet the functional and technical requirements above.

SRS (PRTTDCIS-1584)

~~SRS-524~~ Each individual CCA subsystem shall implement IP throughput performances of minimum 1 Gbps with IPSec encryption enabled.

SRS (PRTTDCIS-1585)

~~SRS-525~~ Each individual CCA subsystem shall support IP throughput performances of minimum 10 Gbps without IPSec encryption enabled.

SRS (PRTTDCIS-1562)

~~SRS-526~~ The CCA subsystem shall implement a minimum of 10Gbps switching core.

SRS (PRTTDCIS-1644)

~~SRS-527~~ Core switches in the CCA Subsystem shall implement a minimum of 2 Gbps uplinks towards each UAM Access BoB.

SRS (PRTTDCIS-2869)

~~SRS-528~~ Crypto devices shall be removable from the racks of the CCA, for storage and transport.

SRS (PRTTDCIS-3864)

~~SRS-529~~ The removal of the crypto devices shall be compatible with the implementation of TEMPEST requirements in the racks.

NOTE (PRTTDCIS-2870)

~~[135]~~ Foam-padded transport cases able to carry one TCE-621/B will be used for that purpose.

NOTE (PRTTDCIS-3865)

~~[136]~~ TCE-621/B transport cases are PFE and will be transported separately from the Node.

SRS (PRTTDCIS-4103)

~~SRS-530~~ Core switching function of the CCA in the CNM shall realize the HDS function of the ISM.

5.2.2.3 MMA subsystem

5.2.2.3.1 General

NOTE (PRTTDCIS-3051)

~~[137]~~ The following picture illustrates the Multi Media Access (MMA) in context.

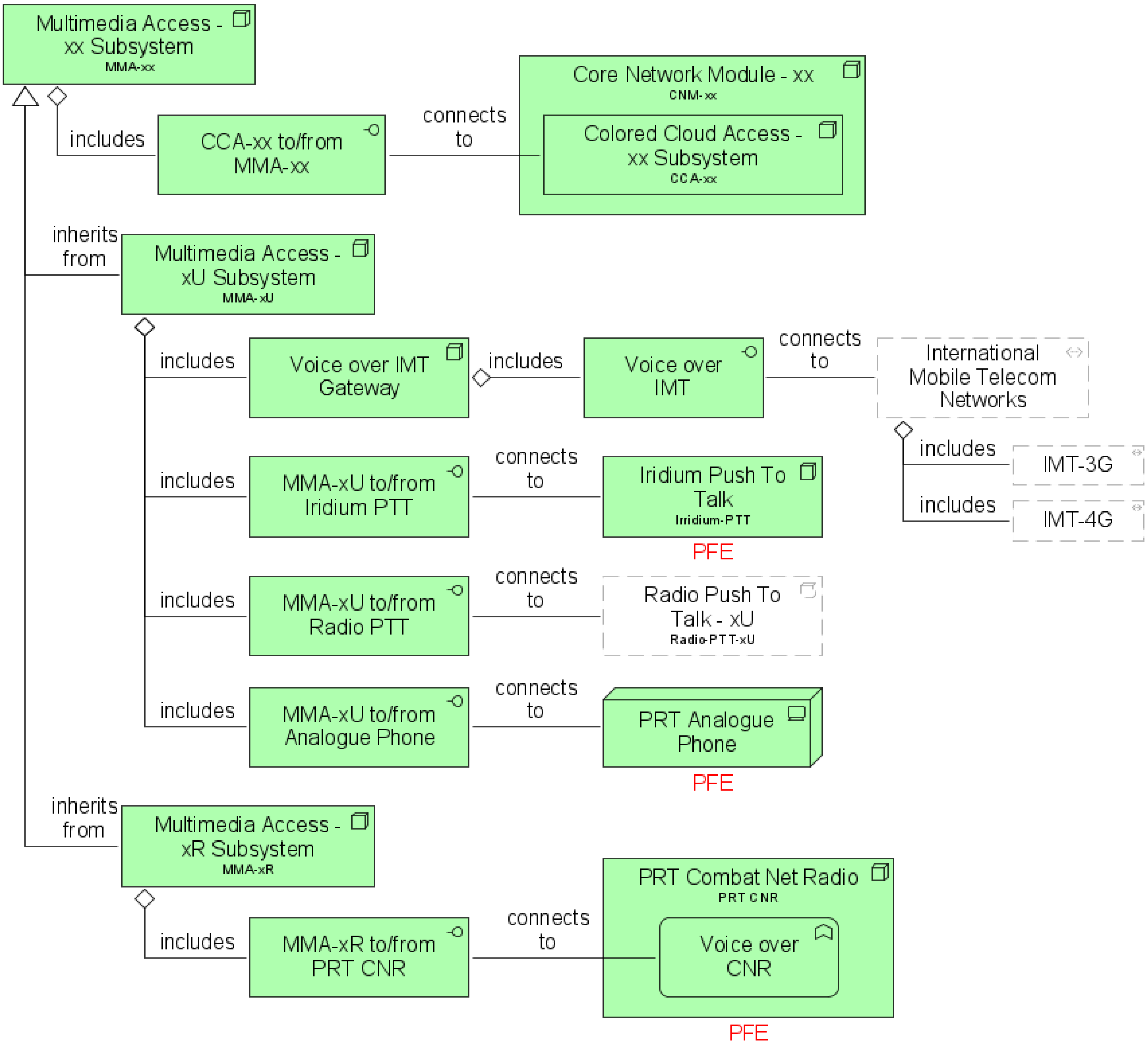

Figure 58 - MMA in context

SRS (PRTTDCIS-1592)

~~SRS-531~~ The MMA subsystem shall implement the MMA functions.

SRS (PRTTDCIS-1593)

~~SRS-532~~ There shall be as many instances of the MMA subsystems as CNMs and security domains (xU, xR and xS).

SRS (PRTTDCIS-1594)

~~SRS-533~~ The MMA subsystem shall implement media stream termination and relay functions using Digital Signal Processing (DSP) hardware acting as Media Termination Point / Trusted Relay Point (MTP/TRP).

SRS (PRTTDCIS-4109)

~~SRS-534~~ The MMA-xU Subsystem shall implement a Voice over IMT Gateway.

SRS (PRTTDCIS-1595)

~~SRS-535~~ The MMA subsystem shall perform codec conversion and use TLS to communicate with the call management function.

SRS (PRTTDCIS-1672)

~~SRS-536~~ The MMA subsystem shall implement the call management function compatible with the specifications of a Cisco Unified Call Manager (CUCM).

SRS (PRTTDCIS-1597)

~~SRS-537~~ The MMA subsystems shall support Dynamic Host Configuration Protocol (DHCP) towards the user appliances connecting via the UAM.

SRS (PRTTDCIS-1598)

~~SRS-538~~ The MMA subsystem shall support local Voice Collaboration Service.

SRS (PRTTDCIS-4307)

~~SRS-539~~ The MMA subsystem shall support local Video Teleconferencing Service in the applicable Nodes.

SRS (PRTTDCIS-1599)

~~SRS-540~~ The MMA subsystem shall implement a Session Border Controller (SBC) function compatible with the specifications of the Cisco Unified Border Element (CUBE).

SRS (PRTTDCIS-1601)

~~SRS-541~~ The MMA subsystem shall support concurrent SIP sessions equals to the largest user quantity possible on a node and in a security domain plus 10%.

NOTE (PRTTDCIS-1603)

~~[138]~~ Software versions are the latest approved versions, these might however be higher during the actual implementation, this will be subject to local coordination and approval prior to any deployment.

SRS (PRTTDCIS-1604)

~~SRS-542~~ All MMA subsystems shall be built and licensed the same, irrespective of the security domain.

SRS (PRTTDCIS-1606)

~~SRS-543~~ Any software component of the MMA subsystem that is able to run on commodity hardware shall be implemented as a workload on the ISM. This is applicable to all security domain (xS, xR and xU).

SRS (PRTTDCIS-1607)

~~SRS-544~~ The implementation of MLPP by the MMA subsystem, shall support, on top of routine calls, levels of precedence and pre-emption, as follows (from highest to lowest):

1) Flash Override; and,
2) Flash; and,
3) Intermediate; and,
4) Priority; and,
5) Routine.

SRS (PRTTDCIS-1608)

~~SRS-545~~ The MMA subsystem shall implement a dial plan compliant with STANAG 4705.

SRS (PRTTDCIS-4464)

~~SRS-546~~ The MMA subsystem shall, as a minimum, support following voice codecs:

- G.729 R8; and,
- G.729 BR8; and,
- G.711 A Law; and,
- G.711 u Law.

SRS (PRTTDCIS-1609)

~~SRS-547~~ The MMA subsystem shall implement a local Call Management instance that refers to the Survivable Remote Site Telephony (SRST) function, this function being a local call processing and management function performed by the CCA subsystem if the node is isolated and loses the connection to a remote Call Manager to ensure intra-node communication.

NOTE (PRTTDCIS-1626)

~~[139]~~ The MTP/RTP instance shall be integrated in the appliance(s) implementing the SBC function.

SRS (PRTTDCIS-1628)

~~SRS-548~~ Any routers, switches and applications in the MMA subsystem shall be duly sized and licensed in order to meet the functional and technical requirements above.

SRS (PRTTDCIS-1629)

~~SRS-549~~ Each MMA subsystem shall, as a minimum, implement interfaces to other subsystems within the Core Network Module as well as to external elements, as per the table below. The need for additional interfaces, or interfaces different from those listed below, as well as their specification, shall be design-driven and shall be justified, based on component selection and functionality sought.

Interface Name	Qty.	Interface Type	Interface Speed	Remarks
CCA-xx to/from MMA-xx	N	Design Driven	Design Driven	N is Design Driven
Voice over IMT	M	Design Driven	Design Driven	Only in MMA-xU M is Design Driven
MMA-xU to/from Iridium PTT	P	Design Driven	Design Driven	Only in MMA-xU P is Design Driven
MMA-xU to/from Radio PTT	Q	Design Driven	Design Driven	Only in MMA-xU Q is Design Driven Interface shall support ED-137/B and SIP/RSTP protocols.
MMA-xU to/from Analogue Phone	4	Design Driven	Design Driven	Analogue Phones are connected through 2 wires.
MMA-xR to/from PRT CNR	1	Design Driven	Design Driven	Only in MMA-xR

Table 30 - MMA subsystem interfaces

SRS (PRTTDCIS-1673)

~~SRS-550~~ All MMA across TDCIS Nodes shall be identical, therefore, the computation of interface quantities have taken into consideration the largest connections possible.

SRS (PRTTDCIS-1630)

~~SRS-551~~ Each MMA subsystem shall implement additional interfaces, as required and as driven by the design, in support of service management and control functionalities.

NOTE (PRTTDCIS-1631)

~~[140]~~ Additional interfaces may be implemented to accommodate other connections and end-points resulting from the detailed design.

SRS (PRTTDCIS-3092)

~~SRS-552~~ The Unified Communication and Collaboration (UCC) solution shall conform to Internet Engineering Task Force (IETF) standards for providing the minimum core features, including voice and video calls, conferencing and content sharing.

NOTE (PRTTDCIS-2906)

~~[141]~~ The VTC Multipoint Control Unit (MCU) implementation is design driven and can either be performed with physical appliances or as a virtual workload to the ISM.

SRS (PRTTDCIS-3835)

~~SRS-553~~ The MMA subsystem shall, as a minimum, support following video codecs:

- H.264 SVC; and,
- H.264 AVC Base Profile.

SRS (PRTTDCIS-1839)

~~SRS-554~~ The MMA Voice Capability shall be compatible with the Phone baseline.

SRS (PRTTDCIS-1596)

~~SRS-555~~ The MMA call management function corresponding application shall run as a workload in the ISM.

SRS (PRTTDCIS-1625)

~~SRS-556~~ The MMA SBC shall be implemented in a dedicated appliance, integrated in the CNM.

SRS (PRTTDCIS-4302)

~~SRS-557~~ The MMA SBC appliance shall be common for Voice and VTC.

SRS (PRTTDCIS-4303)

~~SRS-558~~ The MMA SBC appliance shall implement transcoding function for Voice and VTC services for all codecs as per FMN specifications.

SRS (PRTTDCIS-1262)

~~SRS-559~~ The MMA-xU shall support the integration (mechanical, electrical and logical) of the PFE Iridium terminal.

SRS (PRTTDCIS-1264)

~~SRS-560~~ The MMA IP telephony service in the xR security domain shall integrate the PFE RoIP gateway that will be connected to the CNR voice interface.

5.2.2.3.2 Voice over IMT Gateway

NOTE (PRTTDCIS-4145)

~~[142]~~ The MMA-xU Voice IMT Gateway is an IMT-UE.

NOTE (PRTTDCIS-4146)

~~[143]~~ The purpose of the MMA-xU Voice IMT Gateway, along with the underlying IMT Network Access Service, is to interconnect the TDCIS xU Voice Service with the PRT NDN Infrastructure and the capability to place external calls to public networks, primarily via public IMT networks.

NOTE (PRTTDCIS-4147)

~~[144]~~ The IMT Network Access Service (i.e. SIM cards and subscription) is not a project deliverable.

SRS (PRTTDCIS-4148)

~~SRS-561~~ The MMA-xU Voice IMT Gateway shall consist of Outdoor Elements and Indoor Elements.

SRS (PRTTDCIS-4149)

~~SRS-562~~ The MMA-xU Voice IMT Gateway shall support Public and Private IMT networks.

SRS (PRTTDCIS-4150)

~~SRS-563~~ The MMA-xU Voice IMT Gateway shall be compatible with IMT Network Access Service implementing Private Access Point Name APN).

SRS (PRTTDCIS-4164)

~~SRS-564~~ The MMA-xU Voice IMT Gateway shall implement Multiple Input Multiple Output (MIMO) techniques.

SRS (PRTTDCIS-4165)

~~SRS-565~~ The MMA-xU Voice IMT Gateway shall support a minimum of TWO (02) MIMO layers.

SRS (PRTTDCIS-4151)

~~SRS-566~~ The MMA-xU Voice IMT Gateway shall support a minimum of TWO (02) independent antenna elements.

SRS (PRTTDCIS-4152)

~~SRS-567~~ The antenna shall be able to operate across all frequency bands specified.

SRS (PRTTDCIS-4153)

~~SRS-568~~ The antenna elements shall be detachable and replaceable by a System Administrator.

SRS (PRTTDCIS-4154)

~~SRS-569~~ The MMA-xU Voice IMT Gateway antenna shall be mounted outside, on the Shelter.

SRS (PRTTDCIS-4155)

~~SRS-570~~ The MMA-xU Voice IMT Gateway shall support a minimum of TWO (02) Subscriber Identity Module (SIM) Cards.

SRS (PRTTDCIS-4156)

~~SRS-571~~ SIM-based carrier selection shall be automatic without requiring any System Administrator action.

SRS (PRTTDCIS-4157)

~~SRS-572~~ The MMA-xU Voice IMT Gateway shall support IPv4 and IPv6 dual stack.

SRS (PRTTDCIS-4158)

~~SRS-573~~ The MMA-xU Voice IMT Gateway shall implement 3G/IMT2000 and 4G/IMT-Advanced compliant Radio Access Technology (RAT) including, as a minimum:

- 3GPP's UMTS Release 7 (HSPA+); and,
- 3GPP's LTE Release 11 (LTE Advanced); and,
- LTE IMT-UE Category 11.

SRS (PRTTDCIS-4621)

~~SRS-574~~ The MMA-xU Voice IMT Gateway shall implement 5G/IMT-2020 compliant RAT including, as a minimum:

- 3GPP's LTE Release 13 (LTE Advanced Pro); and,
- 3GPP's 5G Release 15 (5G NR) in Frequency Range 1 (FR1); and,
- 5G+LTE dual connectivity.

SRS (PRTTDCIS-4159)

~~SRS-575~~ The MMA-xU Voice IMT Gateway shall primarily operate with LTE technology and fall back automatically to UMTS technology.

SRS (PRTTDCIS-4160)

~~SRS-576~~ The fall back to UMTS technology shall depend on the RAN technology propagation and coverage conditions, without requiring any System Administrator action.

SRS (PRTTDCIS-4624)

~~SRS-577~~ The MMA-xU Voice IMT Gateway shall primarily operate with LTE technology and switch automatically to 5G technology when in coverage.

SRS (PRTTDCIS-4625)

~~SRS-578~~ The switch to 5G technology shall depend on the RAN technology propagation and coverage conditions, without requiring any operator action.

SRS (PRTTDCIS-4161)

~~SRS-579~~ The MMA-xU Voice IMT Gateway shall implement Roaming techniques.

SRS (PRTTDCIS-4162)

~~SRS-580~~ Any kind of Roaming shall be automatic without requiring any System Administrator action.

SRS (PRTTDCIS-4163)

~~SRS-581~~ The MMA-xU Voice IMT Gateway shall implement Carrier Aggregation (CA) techniques.

SRS (PRTTDCIS-4166)

~~SRS-582~~ The MMA-xU Voice IMT Gateway shall implement global coverage, supporting the adopted bands in the regions of Europe, Africa/Middle East, Asia and Pacific.

SRS (PRTTDCIS-4167)

~~SRS-583~~ The MMA-xU Voice IMT Gateway shall implement a minimum of ONE (01) 3GPP UMTS band per region.

SRS (PRTTDCIS-4168)

~~SRS-584~~ The MMA-xU Voice IMT Gateway shall implement a minimum of TWO (02) 3GPP LTE bands per region.

SRS (PRTTDCIS-4627)

~~SRS-585~~ The MMA-xU Voice IMT Gateway shall implement a minimum of ONE (01) 3GPP 5G NR FR1 band per region.

SRS (PRTTDCIS-4169)

~~SRS-586~~ The MMA-xU Voice IMT Gateway shall implement a Human Machine Interface (HMI) interface that allows monitoring and control of the PCA Data IMT Gateway by a System Administrator.

SRS (PRTTDCIS-4170)

~~SRS-587~~ The MMA-xU Voice IMT Gateway HMI shall provide the minimum following functionalities to System Administrators:

- A clock driven by the IMT Network; and,
- Enabling IMT Gateway parameters configuration; and,
- Collecting, Logging and Reporting Errors, Warnings and Alarms in a Human comprehensive format; and,
- Monitoring and reporting of the IMT Gateway operational status; and,
- MNO currently connected; and,
- Signal strength.

SRS (PRTTDCIS-4110)

~~SRS-588~~ The MMA-xU Voice over IMT Gateway shall support a minimum of 10 concurrent calls.

5.2.2.4 BPS subsystem

NOTE (PRTTDCIS-3053)

~~[145]~~ The following picture illustrates the BPS in context.

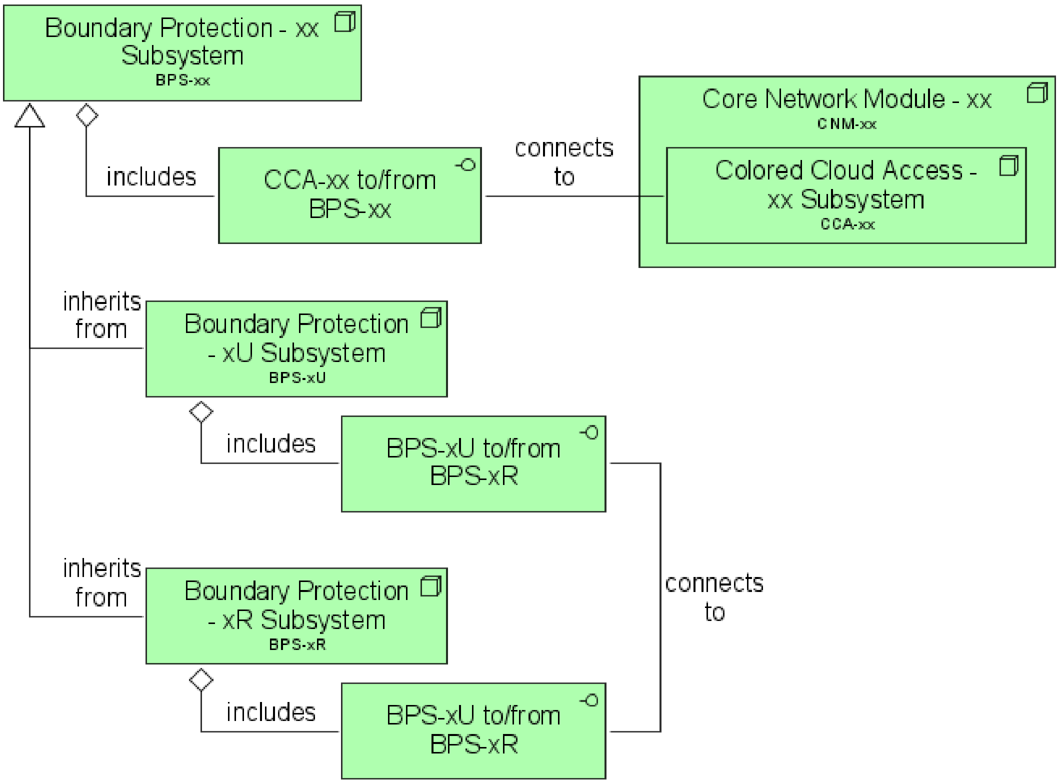

Figure 59 - BPS in context

SRS (PRTTDCIS-1633)

~~SRS-589~~ The BPS subsystem shall implement the BPS functions.

SRS (PRTTDCIS-1634)

~~SRS-590~~ Each BPS subsystem shall be directly connected to the core switching element of the corresponding CCA.

SRS (PRTTDCIS-1635)

~~SRS-591~~ All BPS subsystems shall be built and licensed the same, irrespective of the security domain.

SRS (PRTTDCIS-1636)

~~SRS-592~~ All BPS subsystems shall support up to 3 Gbps of traffic throughput, with the Intrusion Prevention System (IPS) feature enabled.

SRS (PRTTDCIS-1637)

~~SRS-593~~ IPS licenses shall be provided with each BPS firewall (1-year subscription). Licenses shall be based on volume (number of hosts).

SRS (PRTTDCIS-1638)

~~SRS-594~~ The BPS subsystem shall implement interfaces as per the table below.

Interface Name	Qty.	Interface Type	Interface Speed	Remarks
CCA-xx to/from BPS-xx	N	Design Driven	Design Driven	N is Design Driven through CCA switching core
BPS-xU to/from BPS-xR	M	Design Driven	Design Driven	M is Design Driven Only in BPS-xU and BPS-xR to realize xU-xR cross domain function

Table 31 - BPS subsystem interfaces

SRS (PRTTDCIS-3122)

~~SRS-595~~ BPS shall support network segmentation through its single internal interface to the CCA.

SRS (PRTTDCIS-1677)

~~SRS-596~~ BPS shall be realized with physical appliances

5.2.3 Implementation Constraints

SRS (PRTTDCIS-1664)

~~SRS-597~~ The hardware of CNM-xS, CNM-xR and CNM-xU shall be physically built the same, such that these modules are interchangeable.

5.3 Core Network Module Lite

5.3.1 General

NOTE (PRTTDCIS-2858)

~~[146]~~ The Core Network Module (CNM) lite is a variant of the CNM which shares the same description, functionalities and characteristics.

SRS (PRTTDCIS-2861)

~~SRS-598~~ The CNM lite shall comply with all CNM specifications unless specifically specified otherwise.

SRS (PRTTDCIS-2782)

~~SRS-599~~ The design of the CNM lite shall adhere to the architecture presented in following figure.

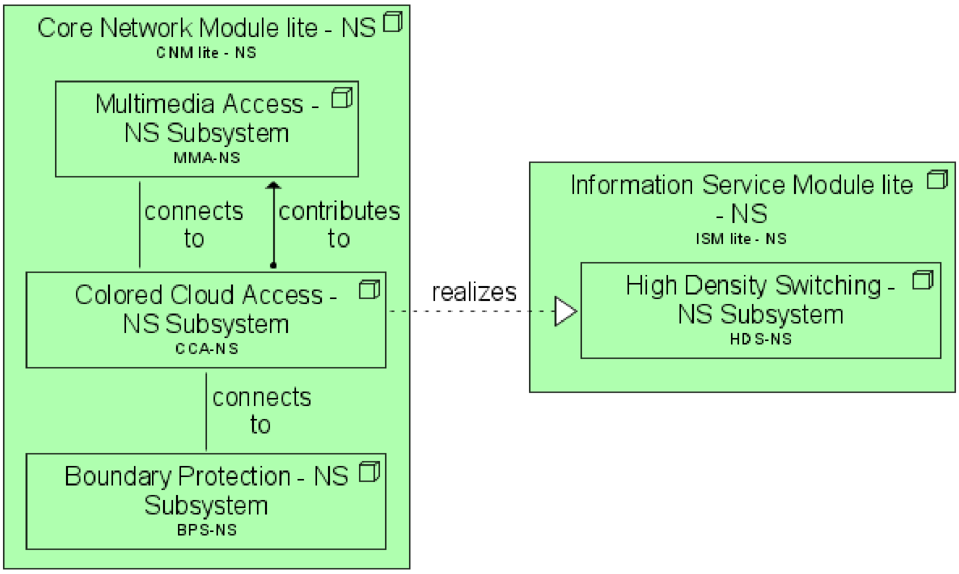
Core Network Module lite - NS
CNM lite - NS
Multimedia Access - NS Subsystem
MMA-NS
connects to
contributes to
Colored Cloud Access - NS Subsystem
CCA-NS
connects to
Boundary Protection - NS Subsystem
BPS-NS
realizes
Information Service Module lite - NS
ISM lite - NS
High Density Switching - NS Subsystem
HDS-NS

Figure 60 - CNM lite architecture

5.3.2 Functional Requirements

SRS (PRTTDCIS-2787)

~~SRS-600~~ The CNM lite shall implement the CCA function.

SRS (PRTTDCIS-3024)

~~SRS-601~~ The CNM lite shall implement the MMA function, including the ISM workload elements, limited to the services specific to the NS Kit.

SRS (PRTTDCIS-4375)

~~SRS-602~~ The CNM lite shall implement the BPS function.

5.3.3 Technical Requirements

5.3.3.1 CCA subsystem

SRS (PRTTDCIS-2789)

~~SRS-603~~ The CCA subsystem in the CNM lite shall implement the functions listed under the CCA-xS function in the CNM.

SRS (PRTTDCIS-2790)

~~SRS-604~~ The CCA subsystem in the CNM lite shall meet the same technical requirements formulated for the CCA-xS subsystem of the CNM.

SRS (PRTTDCIS-2791)

~~SRS-605~~ The CCA subsystem of the CNM lite shall, as a minimum, implement interfaces as per the table below. The need for additional interfaces, or interfaces different from those listed below, as well as their specification, shall be design-driven and shall be justified, based on component selection and functionality sought.

Interface Name	Qty.	Interface Type	Interface Speed	Remarks
CCA-NS to/from MMA-NS	N	Design Driven	Design Driven	N is Design Driven
CCA-NS to/from BPS-NS	M	Design Driven	Design Driven	M is Design Driven
HDS-NS to/from CAS-NS	—	—	—	See ISM lite HDS specifications
CCA-NS to UAM-NS	P	Design Driven	Design Driven	P is Design Driven
CCA-NS to LMM-NS	Q	Design Driven	Design Driven	Q is Design Driven with a minimum of 1 interfaces to connect a Sys Admin Workstation.
PCA to/from NS Kit	1	Eth-FO-LR	1Gbps	Interface can be connected to the TCE621M of the CCA-NS of a Core Node Lite or of a Remote Node Lite
NIP-NS	1	Eth-FO-LR	1Gbps	direct interface on CCA routing platform

Table 32 - CNM lite CCA subsystem interfaces

SRS (PRTTDCIS-2792)

~~SRS-606~~ The CCA subsystem in the CNM lite shall support IP throughput performances of 4 Gbps as a minimum.

SRS (PRTTDCIS-2800)

~~SRS-607~~ Crypto devices shall be removable from the transit cases of the CNM lite, for storage and transport.

SRS (PRTTDCIS-2801)

~~SRS-608~~ The removal of the crypto devices shall be compatible with the implementation of TEMPEST requirements in the transit cases.

NOTE (PRTTDCIS-2803)

~~[147]~~ Foam-padded transport cases able to carry one TCE621M will be used for that purpose.

NOTE (PRTTDCIS-3866)

~~[148]~~ TCE621M transport cases are PFE and will be transported separately from the Node.

SRS (PRTTDCIS-4104)

~~SRS-609~~ Core switching function of the CCA in the CNM Lite shall realize the HDS function of the ISM Lite.

5.3.3.2 MMA Subsystem

SRS (PRTTDCIS-4377)

~~SRS-610~~ The MMA subsystem in the CNM lite shall implement the functions listed under the MMA-xS function in the CNM.

SRS (PRTTDCIS-4378)

~~SRS-611~~ The MMA subsystem in the CNM lite shall meet the same technical requirements formulated for the MMA-xS subsystem of the CNM.

SRS (PRTTDCIS-4379)

~~SRS-612~~ The MMA subsystem of the CNM lite shall, as a minimum, implement interfaces as per the table below. The need for additional interfaces, or interfaces different from those listed below, as well as their specification, shall be design-driven and shall be justified, based on component selection and functionality sought.

Interface Name	Qty.	Interface Type	Interface Speed	Remarks
CCA-NS to/from MMA-NS	N	Design Driven	Design Driven	N is Design Driven

Table 33 - CNM lite MMA subsystem interfaces

5.3.3.3 BPS Subsystem

SRS (PRTTDCIS-4381)

~~SRS-613~~ The BPS subsystem in the CNM lite shall implement the functions listed under the BPS-xS function in the CNM.

SRS (PRTTDCIS-4382)

~~SRS-614~~ The BPS subsystem in the CNM lite shall meet the same technical requirements formulated for the BPS-xS subsystem of the CNM.

SRS (PRTTDCIS-4383)

~~SRS-615~~ The BPS subsystem of the CNM lite shall, as a minimum, implement interfaces as per the table below. The need for additional interfaces, or interfaces different from those listed below, as well as their specification, shall be design-driven and shall be justified, based on component selection and functionality sought.

Interface Name	Qty.	Interface Type	Interface Speed	Remarks
CCA-NS to/from BPS-NS	N	Eth-FO-SR	Design Driven	N is Design Driven

Table 34 - CNM lite BPS subsystem interfaces

5.3.4 Implementation Constraints

SRS (PRTTDCIS-2798)

~~SRS-616~~ The CCA subsystems of the CNM lite shall be implemented using routers and switches compatible with the element management system for routing and switching platforms.

5.4 Information Services Module

5.4.1 General

NOTE (PRTTDCIS-1771)

~~[149]~~ The Information Services Module (ISM) implements a deployable Infrastructure as a Service (IaaS) on which platform services, business applications and CoI services run.

NOTE (PRTTDCIS-1772)

~~[150]~~ The deployable IaaS in the ISM provides Virtual Machines (VM) hosting the software that enables Core Enterprise Services (CES) and Functional Area Services (FAS), as well as software supporting Multimedia Access Module, in conjunction with the MMA subsystem of the CNM.

NOTE (PRTTDCIS-1773)

~~[151]~~ Any software running in a VM is hereafter referred to as Workload.

NOTE (PRTTDCIS-1774)

~~[152]~~ In addition to hosting CES, FAS and MMA workloads, the ISM also hosts the Service Management and Control (SMC) applications in support of the Local Management Module (LMM) for its associated Color Cloud.

NOTE (PRTTDCIS-1775)

~~[153]~~ The ISM IaaS is implemented through Compute, Storage and Networking mechanisms.

SRS (PRTTDCIS-1776)

~~SRS-617~~ The elements inside the ISM have to be identical and interchangeable; noting that the configuration of the ISM defines the security domain.

5.4.2 Functional Requirements

5.4.2.1 General

SRS (PRTTDCIS-4197)

~~SRS-618~~ The ISM shall implements functions as depicted on following diagram:

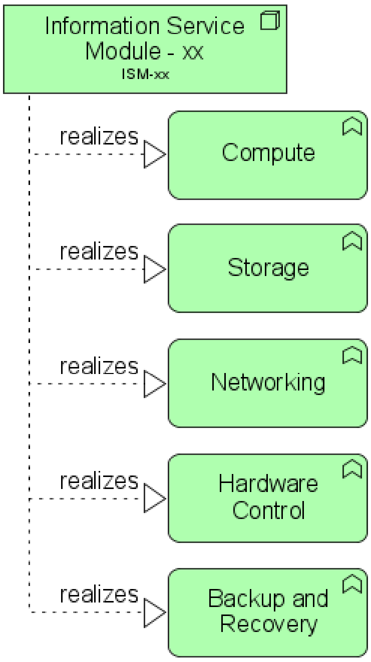

Figure 61 - ISM functions

SRS (PRTTDCIS-1707)

~~SRS-619~~ The ISM shall implement the following functions in support of deployable instances of Infrastructure Services:

1) Compute; and,
2) Storage; and,
3) Networking; and,
4) Hardware Control; and,
5) Backup and Recovery.

5.4.2.2 Compute

5.4.2.2.1 General

SRS (PRTTDCIS-4287)

~~SRS-620~~ The Compute function variants are as follow and as depicted on following picture:

- Software Defined Compute (SDC) function.

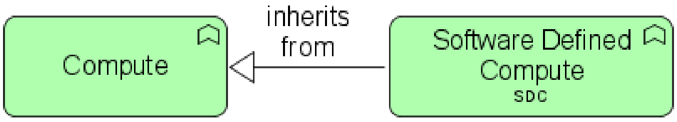

Figure 62 - Compute function variants.

SRS (PRTTDCIS-4288)

~~SRS-621~~ This project shall only implement Software Defined Compute.

5.4.2.2.2 Software Defined Compute

NOTE (PRTTDCIS-1681)

~~[154]~~ The SDC implementation is specified in detail in DCIS CA Annex B.

SRS (PRTTDCIS-1682)

~~SRS-622~~ The SDC function shall:

1) Abstract the physical hardware of the ISM into a VM cluster that shares CPU, memory and peripherals, through the use of virtualization hypervisors; and,
2) Establish, change, monitor, power-on, power-off, snapshot and teardown of VMs within the VM cluster established within the ISM; and,
3) Assure high availability for VMs, by implementing automatic failover to alternate hosts within the ISM; and,
4) Provide a documented and open Application Programming Interface (API) for management and control purposes.

5.4.2.3 Storage

5.4.2.3.1 General

SRS (PRTTDCIS-4289)

~~SRS-623~~ The Storage function variants are as follow and as depicted on following picture:

- Software Define Storage (SDS) function; and,
- Storage Area Network (SAN) function; and,
- Single Server Storage function.

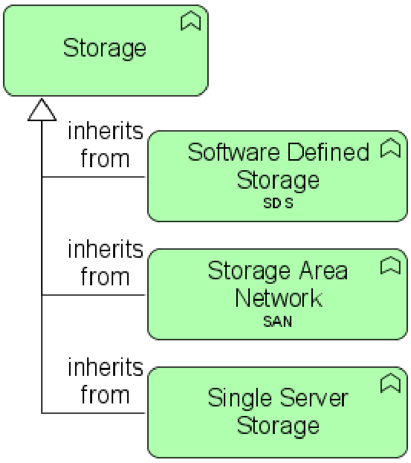

Figure 63 - Storage function variants.

SRS (PRTTDCIS-4290)

~~SRS-624~~ This project shall implement all THREE (03) variants of the Storage function.

5.4.2.3.2 Software Defined Storage

SRS (PRTTDCIS-1684)

~~SRS-625~~ The SDS function shall:

1) Abstract the physical storage of the ISM, and provide virtual disk access to VMs (or ISM cluster) and to collocated machines external to the ISM; and,
2) Support presentation of virtual disks to the VM and networked as a SDS area network through iSCSI. This function is also referred to as Block I/O; and,
3) Provide file access to VMs running on the ISM and to collocated machines external to the ISM as virtual network attached storage through NFS and CIFS/SMB. This function is also referred to as File I/O; and,
4) Provide object-based storage access to VMs running on the ISM and collocated machines external to the ISM; and,
5) Enforce storage quality of service, through configurable limits (maximum) and guarantees (minimum) of storage throughput per VM, per group of VMs, per SDS resource, and per group of SDS resources; and,
6) Optimize storage capacity use, though de-duplication and compression; and,
7) Cluster physical storage resources across all compute nodes (servers); and,
8) Control and monitor the execution of the above described functionalities; and,
9) Provide a well-documented and open API for management and control purposes.

SRS (PRTTDCIS-4206)

~~SRS-626~~ The Software-defined Storage function optimization shall be fully automatic and opaque to the storage consumers.

SRS (PRTTDCIS-4207)

~~SRS-627~~ The Software-defined Storage function optimization shall, as a minimum, support following configuration methods:

- De-duplication and Compression; and,
- De-duplication only.

NOTE (PRTTDCIS-1779)

~~[155]~~ The Storage Optimization may involve automatic storage tiering of less used data to slower storage resources or to external storage, which may potentially be located in the ISM of another TDCIS Node, in the PRT static infrastructure or cloud service.

NOTE (PRTTDCIS-1685)

~~[156]~~ Depending on the available resources at a deployment, the mission profile and its associated security profile, remote storage resources may be used, including NATO or National private clouds.

NOTE (PRTTDCIS-3123)

~~[157]~~ Depending on the available resources at a deployment, the mission profile and its associated security profile, remote storage resources on commercial public clouds may be used for the xU security domain.

5.4.2.3.3 Storage Area Network

SRS (PRTTDCIS-4291)

~~SRS-628~~ The Storage Area Network (SAN) function shall:

1) Provide physical storage on the ISM, and virtual disk access to VMs of the ISM cluster and to collocated machines external to the ISM; and,
2) Provide object-based storage access to VMs running on the ISM and collocated machines external to the ISM; and,
3) Enforce storage quality of service, through configurable limits (maximum) and guarantees (minimum) of storage throughput per VM, per group of VMs, per SAN resource, and per group of SAN resources; and,
4) Optimize storage capacity use, though de-duplication and compression; and,
5) Cluster physical storage resources from the SAN Server; and,
6) Control and monitor the execution of the above described functionalities; and,
7) Provide a well-documented and open API for management and control purposes.

SRS (PRTTDCIS-4280)

~~SRS-629~~ The Software-defined Storage function optimization shall be fully automatic and opaque to the storage consumers.

SRS (PRTTDCIS-4281)

~~SRS-630~~ The Software-defined Storage function optimization shall, as a minimum, support following configuration methods:

- De-duplication and Compression; and,
- De- duplication only.

NOTE (PRTTDCIS-4284)

~~[158]~~ Depending on the available resources at a deployment, the mission profile and its associated security profile, remote storage resources may be used, including NATO or National private clouds.

NOTE (PRTTDCIS-4285)

~~[159]~~ Depending on the available resources at a deployment, the mission profile and its associated security profile, remote storage resources on commercial public clouds may be used for the xU security domain.

5.4.2.3.4 Single Server Storage

SRS (PRTTDCIS-4292)

~~SRS-631~~ The Single Server Storage function shall:

1) Provide physical storage for the Single Server CAS, and virtual disk access to the VMs; and,
2) Provide object-based storage access to VMs running on the Single Server CAS; and,
3) Implement RAID level redundancy for data protection; and,
4) Optimize storage capacity use, though de-duplication and compression; and,
5) Cluster physical storage resources from the Single Server; and,
6) Control and monitor the execution of the above described functionalities; and,
7) Provide a well-documented and open API for management and control purposes.

SRS (PRTTDCIS-4282)

~~SRS-632~~ The Software-defined Storage function optimization shall be fully automatic and opaque to the storage consumers.

SRS (PRTTDCIS-4283)

~~SRS-633~~ The Software-defined Storage function optimization shall, as a minimum, support following configuration methods:

- De-duplication and Compression; and,
- De- duplication only.

5.4.2.4 Networking

5.4.2.4.1 General

SRS (PRTTDCIS-4293)

~~SRS-634~~ The Networking function variants are as follow and as depicted on following picture:

- Software Define Networking (SDN) function.

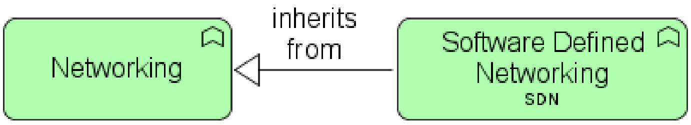

Figure 64 - Networking function variants.

SRS (PRTTDCIS-4294)

~~SRS-635~~ This project shall implement Software Defined Networking in the CAS subsystem.

5.4.2.4.2 Software Defined Networking

SRS (PRTTDCIS-1688)

~~SRS-636~~ The SDN function shall:

1) Establish, change, monitor and teardown virtual Ethernet LAN (VLAN) segments, within the ISM; and,
2) Connect and remove external Ethernet interfaces and VMs to those VLAN segments; and,
3) Support WAN and LAN interfaces to the CCA function of the CNM, for wide-area communications purposes; and,
4) Provide a well-documented and open API for management and control purposes.

5.4.2.5 Hardware Control

SRS (PRTTDCIS-1690)

~~SRS-637~~ The Hardware Control function shall manage the hardware-based Compute, Storage and Networking components, upon which the Compute, Storage and Networking functions and their Software-defined variants run.

SRS (PRTTDCIS-1691)

~~SRS-638~~ To that end, the Hardware Control function shall combine and abstract the hardware-specific management and control interfaces of the components that make up the ISM, into open, standardized and authenticated interfaces (standard networking API).

SRS (PRTTDCIS-1692)

~~SRS-639~~ The Hardware Control function shall:

1) Operate both local as well as networked (i.e. over the WAN), providing both local and remote console access; and,
2) Support the integration with a centralized Hardware Control service in a Deployed TDCIS Node or the PRT static infrastructure, allowing through dashboards the centralized hardware monitoring and control; and,
3) Implement power control: power-on, power-off, graceful shutdown, emergency shutdown; and,
4) Implement boot control, i.e. setting the boot source, boot and reset; and,
5) Implement monitoring of hardware and environmental status; and,
6) Support the installation, updating and configuration of BIOS and firmware; and,
7) Provide interfaces that enable monitor, control and operation host independent CPU, firmware (BIOS) and operating system, in order to grant direct access to the hardware-based compute, storage and network components; and,
8) Interface with the Uninterruptible Power Supply control listening for a "battery low" signal, which shall result in a graceful shutdown and subsequent power-off of the individual compute, storage and networking functions and hosted VMs.

NOTE (PRTTDCIS-1780)

~~[160]~~ Monitoring and Control interfaces are, for example, interfaces to a so-called Baseboard Management Controller (BMC), Intelligent Platform Management Interface (IPMI), Integrated Lights-Out (iLO), terminal/console ports of servers and switches; including access to BIOS, firmware, bootloader, etc.

5.4.2.6 Backup and Recovery

SRS (PRTTDCIS-1695)

~~SRS-640~~ The Backup and Recovery function shall implement the mechanisms, hardware and software in support of snapshotting, backup of, and the recovery from corruption or loss of:

1) a VM realized by the ISM; and,
2) a workload served by a VM realized by the ISM; and,
3) an ISM.

SRS (PRTTDCIS-3846)

~~SRS-641~~ The Backup and Recovery function shall provide snapshots as follow:

1) ONE (01) from each month for last year (12); and,
2) ONE (01) from each week for last month (4); and,
3) ONE (01) from each day from last week (7).

SRS (PRTTDCIS-1696)

~~SRS-642~~ The Backup and Recovery function shall:

1) Be implemented with a deployable backup storage Element, implemented on dedicated hardware, using deployable and networked backup storage hardware, with as many instances available as security domains; and,
2) Be able to create and restore (roll-back) multiple snapshots, or point-in-time copies, of any data stored in the ISM, including storage, file system, infrastructure data and application data.

SRS (PRTTDCIS-1697)

~~SRS-643~~ Snapshots shall include the configuration of compute, networking and storage functions, both at the level of single VMs and clusters of VMs.

SRS (PRTTDCIS-1699)

~~SRS-644~~ The Backup and Recovery function shall create, restore, optimize and manage the storage of snapshots and backups.

SRS (PRTTDCIS-1700)

~~SRS-645~~ Automatic optimization shall minimize the use of storage space on the backup media, using deduplication, compression or a combination thereof, while retaining recovery points as defined in a retention policy that can be configured through the administration interface.

SRS (PRTTDCIS-1701)

~~SRS-646~~ Backup management shall support backups to be automatically tiered to an off-site storage system (not a project deliverable), typically located in the PRT static infrastructure.

SRS (PRTTDCIS-1702)

~~SRS-647~~ The Backup and Recovery function shall maintain a continuous replica of the storage for quick disaster recovery; i.e. Real Time Replication (RtR).

SRS (PRTTDCIS-1703)

~~SRS-648~~ The Backup and Recovery function shall implement application-consistent backups and replicas of VMs running applications supporting Microsoft VSS, and of VMs running applications that support so-called quiescing scripts.

NOTE (PRTTDCIS-1781)

~~[161]~~ Quiescing refers to pausing or altering a device or application to achieve a consistent state, usually in preparation for a backup or other maintenance activities.

SRS (PRTTDCIS-1704)

~~SRS-649~~ The Backup and Recovery function of the ISM shall implement mechanisms to restore and clone an ISM from snapshots, supporting a disaster recovery scenario where an ISM cannot be recovered and is physically replaced with un-configured hardware.

SRS (PRTTDCIS-1694)

~~SRS-650~~ After any restoration of service, the TDCIS shall revert to a configured working state of all services.

SRS (PRTTDCIS-1705)

~~SRS-651~~ The Backup and Recovery function of the ISM shall be implemented such that it can be managed and controlled both centrally and locally, as appropriate for the specific deployment, through the static (in PRT static infrastructure) and deployable (local to the ISM) instances of the LMM.

SRS (PRTTDCIS-1706)

~~SRS-652~~ The Backup and Recovery function of the ISM shall implement a RESTful well-documented and open API (RESTful API), exposing all operations.

5.4.3 Technical Requirements

5.4.3.1 General

NOTE (PRTTDCIS-1743)

~~[162]~~ The Information Services Module (ISM) shall implement three subsystems, as depicted in the following figure:

1) Compute and Storage (CAS) subsystem, providing CPU, RAM and solid state storage, for use by Compute and Storage functions; and,
2) High Density Switching (HDS) subsystem, providing the physical means to interconnect and manage all physical components of the CAS and the DRS subsystems, including external interfaces, for use by the ISM-internal Networking function described above; and,
3) Deployable Removable Storage (DRS) subsystem, comprising the storage infrastructure that is external to and not dependent on the CAS.

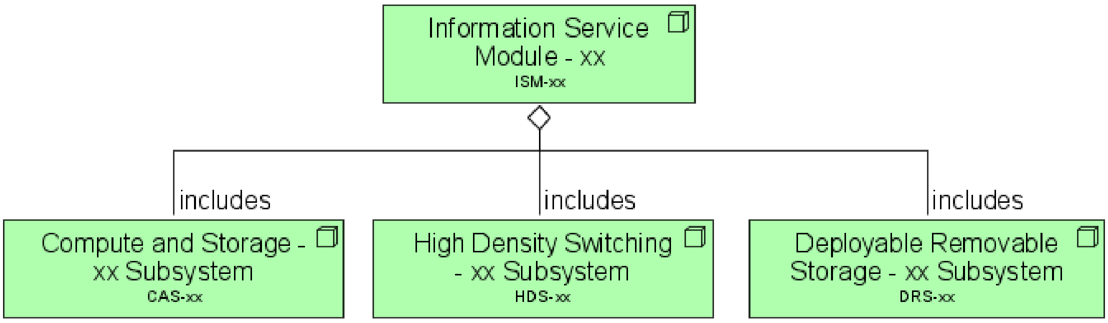
Information Service Module - xx
ISM-xx
includes
includes
includes
Compute and Storage - xx Subsystem
CAS-xx
High Density Switching - xx Subsystem
HDS-xx
Deployable Removable Storage - xx Subsystem
DRS-xx

Figure 65 - ISM Breakdown

SRS (PRTTDCIS-1750)

~~SRS-653~~ It shall be possible to upgrade and/or replace the hardware layer and the virtualization layer of the ISM, in independent cycles. To that end, the hardware and software layers shall be chosen and be validated to support each other's lifecycle. This shall also include the lifecycle of guest OS and workloads.

SRS (PRTTDCIS-1751)

~~SRS-654~~ The ISM shall implement well-documented and open APIs compliant with the following:

1) Representational State Transfer (REST); and,
2) HTTPS, TLS (as a minimum version 1.2 and 1.3):
   - RFC2616:1999, Hypertext Transfer Protocol – HTTP/1.1; and,
   - RFC2616:1999, Hypertext Transfer Protocol – HTTP/1.1; and,
   - RFC2818:2000, HTTP Over TLS; and,
   - RFC5246:2008, the Transport Layer Security (TLS) Protocol Version 1.2; and,
   - RFC8446:2018, the Transport Layer Security (TLS) Protocol Version 1.3; and,

1) IPv4 IETF STD5; and,
2) IPv6 RIPE-554; and,
3) PowerShell support; and,
4) Python support.

SRS (PRTTDCIS-1752)

~~SRS-655~~ Each operation, carried across the corresponding interfaces of the ISM, shall be implemented through:

1) Use of the ISM's hardware and software native RESTful API;
2) Use of custom made scripts developed for the ISM;
3) Use off-the-shelf scripts; or
4) A combination of the native RESTful API, custom made scrips and off-the-shelf scripts.

SRS (PRTTDCIS-1753)

~~SRS-656~~ The implementation of the API shall:

1) Build upon a well-documented and open API framework ; and,
2) Include source code and full documentation of any scripts developed for the ISM.

NOTE (PRTTDCIS-1782)

~~[163]~~ RESTful API Modeling Language (RAML) and OpenAPI Specification (OAS) are example of such API.

SRS (PRTTDCIS-2449)

~~SRS-657~~ In addition to an API, and in support of the Hardware Control function, the ISM shall implement Local console interfaces to hardware components such as servers and switches to provide low level access to the hardware systems (for use by an on-site engineer). These interfaces shall implement authentication.

SRS (PRTTDCIS-2450)

~~SRS-658~~ In addition to an API, and in support of the Hardware Control function, the ISM shall implement Remote console interfaces to all hardware components, as a minimum, through SSH2 or through a web-based terminal interface over HTTPS. These interfaces shall implement both authentication and encryption.

SRS (PRTTDCIS-2451)

~~SRS-659~~ In addition to an API, and in support of the Hardware Control function, the ISM shall implement local management interfaces, to bootstrap the ISM on site when no WAN connectivity is available, or for introducing changes during a communications outage, or to involve the Backup and Recovery function.

5.4.3.2 CAS subsystem

5.4.3.2.1 General

SRS (PRTTDCIS-4199)

~~SRS-660~~ The TDCIS shall implement THREE (03) variants of the CAS Subsystem as depicted on following picture.

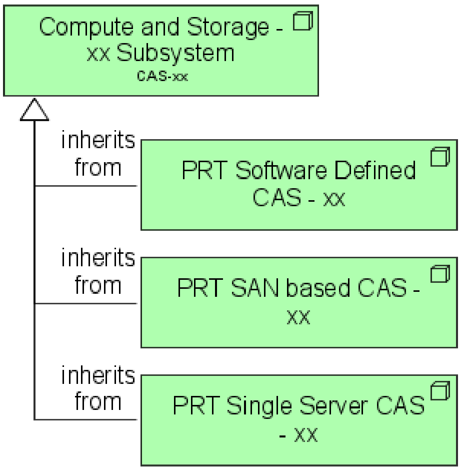
Compute and Storage - xx Subsystem
CAS-xx
inherits from
PRT Software Defined CAS - xx
inherits from
PRT SAN based CAS - xx
inherits from
PRT Single Server CAS - xx

Figure 66 - PRT TDCIS CAS variants

NOTE (PRTTDCIS-1713)

~~[164]~~ The below requirements specify the minimum performance and capacity to be implemented, with respect to CPU, RAM and permanent storage. Neither oversubscription nor any additional capacity necessary to implement resilience, are included in the requirements herein. Any redundancy is considered as additional capacity on top of the minimal capacity required herein.

SRS (PRTTDCIS-1715)

~~SRS-661~~ The CAS subsystem of a single module shall implement CPU cores, where:

1) CPU cores feature as a minimum 16 Cores per processor; and,
2) CPU cores implement Hyper-threading with as a minimum 2 threads per core, and operate at a minimum base frequency of 2.1 GHz; and,
3) All CPUs shall be 64-bit x86 processors implementing AMD or Intel Virtualization Technology (AMD-V or Intel VT-x).

SRS (PRTTDCIS-4295)

~~SRS-662~~ Servers implementing the Compute function in all CAS variants shall be identical and only differ in HDD capacity.

SRS (PRTTDCIS-1716)

~~SRS-663~~ All server hardware realizing the Compute function shall implement:

1) Intel Trusted Execution Technology (TXT) or equivalent AMD technology; and,
2) Trusted Platform Module (TPM) ; and
3) AES New Instructions (AES-NI).

SRS (PRTTDCIS-1712)

~~SRS-664~~ The servers in all CAS subsystem variants shall support and be agnostic to the corresponding Software-defined Compute (Virtualization Hypervisor), Storage and Software-defined Networking.

SRS (PRTTDCIS-1718)

~~SRS-665~~ The CAS subsystem shall implement solid-state storage.

NOTE (PRTTDCIS-1783)

~~[165]~~ Solid State is defined as non-volatile computer storage that stores and retrieves digital information using only electronic circuits, without any involvement of moving mechanical parts.

SRS (PRTTDCIS-1719)

~~SRS-666~~ The CAS subsystem shall rely on storage hardware supporting as 75,000 Input/output Operations Per Second (IOPS) at a mixed random read (70%) and write (30%).

SRS (PRTTDCIS-1720)

~~SRS-667~~ In addition to the storage requirements above, all compute nodes (servers) shall implement dedicated hypervisor boot storage device with sufficient capacity to store the virtualization hypervisor and all necessary software to boot the computer node, to store core dumps and to store logging, following the guidelines and directions of the supported virtualization hypervisor vendors, with a minimum of 32 GB.

SRS (PRTTDCIS-1723)

~~SRS-668~~ The CAS subsystem shall implement the Hardware Control function with dedicated Controller software, hereafter referred to as the ISM Controller, running as a VM installed on the System Administrator laptop of each security domain. Once the ISM is in operation, the ISM Controller shall, in addition, be implemented as a workload in a VM running the management domain of the ISM itself. The ISM Controller software on the laptop shall reach the ISM over a network (IP) link.

SRS (PRTTDCIS-3015)

~~SRS-669~~ The Contractor shall design the CAS subsystem based on all services it has to host.

SRS (PRTTDCIS-3017)

~~SRS-670~~ The contractor shall include following provision for growth in the design of the each CAS Subsystem:

1) 10% for vCPU; and
2) 10% for vRAM; and
3) 20% for Storage.

SRS (PRTTDCIS-1759)

~~SRS-671~~ The implementation of the hypervisor may include additional or 3rd party products as add-ons to those specified above or be part of a unified Software-Defined Data Center (SDDC) platform.

SRS (PRTTDCIS-1763)

~~SRS-672~~ Sufficient software licenses of the virtualization software shall be provided in order to exploit the CPU, storage and RAM capacity of the CAS to their maximum extent.

5.4.3.2.2 Software Defined CAS

SRS (PRTTDCIS-4200)

~~SRS-673~~ The Software Defined variant of the CAS Subsystem shall follow the implementation concept illustrated on following picture.

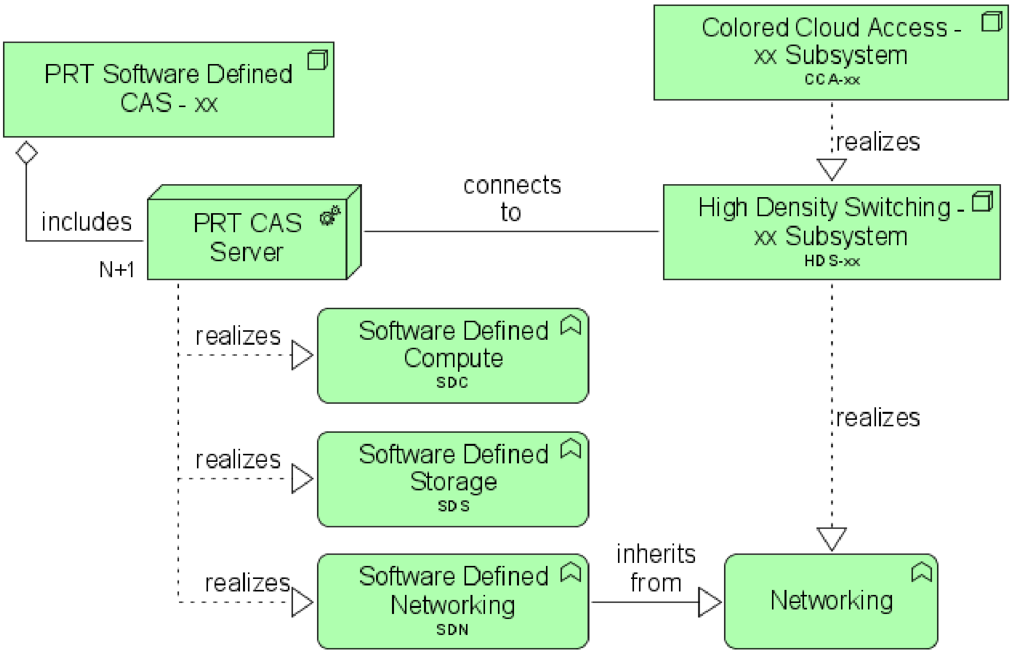

Figure 67 - Software Defined CAS variant implementation concept

SRS (PRTTDCIS-1749)

~~SRS-674~~ Any single hardware failure shall not degrade the capacity and performance specified for the Software Defined variant of the CAS subsystems. To that end, each CAS instance shall implement the following resilience measures:

1) N+1 redundancy for all compute, storage and networking components; and,
2) Distributing storage data blocks across:
   1) Physical storage devices; and,
   2) Physical compute nodes within the VM-cluster.

SRS (PRTTDCIS-1735)

~~SRS-675~~ The Software Defined variant of the CAS subsystems shall implement Software-defined Networking to interconnect virtualized workloads distributed across multiple Compute and Storage instances, and with physical external Ethernet interfaces of the HDS Subsystem.

SRS (PRTTDCIS-1761)

~~SRS-676~~ The Software Defined variant of the CAS subsystems shall implement the software-defined storage function including any necessary additional supporting software.

5.4.3.2.3 SAN based CAS

SRS (PRTTDCIS-4201)

~~SRS-677~~ The SAN based variant of the CAS Subsystem shall follow the implementation concept illustrated on following picture.

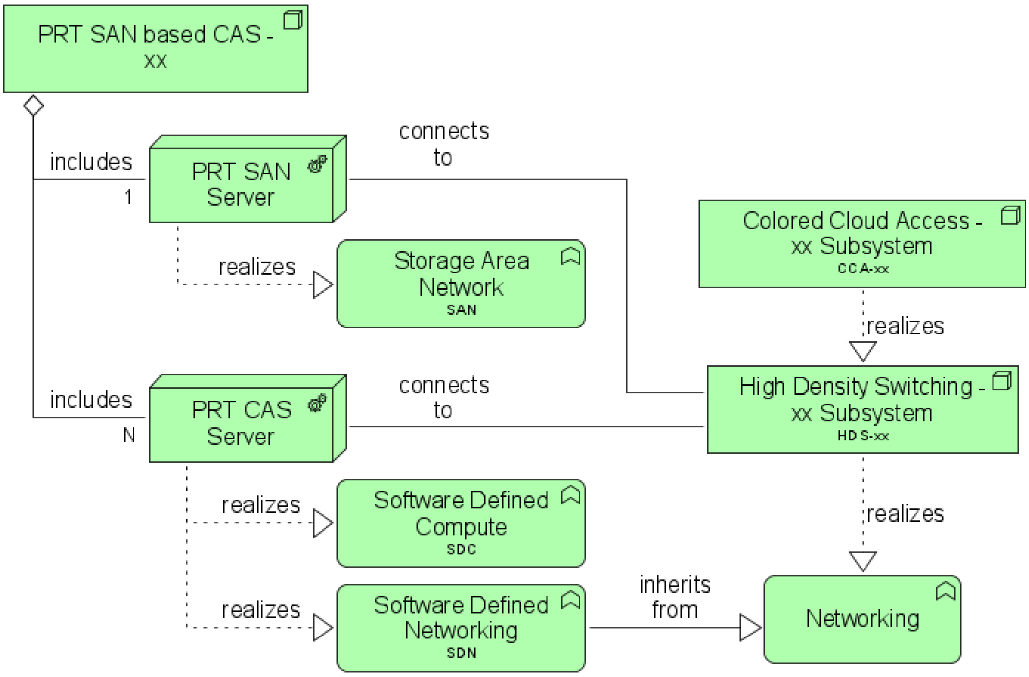

Figure 68 - SAN based CAS variant implementation concept

SRS (PRTTDCIS-4296)

~~SRS-678~~ The Storage function in the SAN based variant of the CAS subsystem shall be implemented with a dedicated SAN Server.

SRS (PRTTDCIS-4297)

~~SRS-679~~ The SAN based variant of the CAS subsystems shall not implement N+1 redundancy.

SRS (PRTTDCIS-4298)

~~SRS-680~~ The SAN based variant of the CAS subsystems shall implement Software-defined Networking to interconnect virtualized workloads distributed across multiple Compute and Storage instances, and with physical external Ethernet interfaces of the HDS Subsystem.

5.4.3.2.4 Single Server CAS

SRS (PRTTDCIS-4202)

~~SRS-681~~ The Single Server variant of the CAS Subsystem shall follow the implementation concept illustrated on following picture.

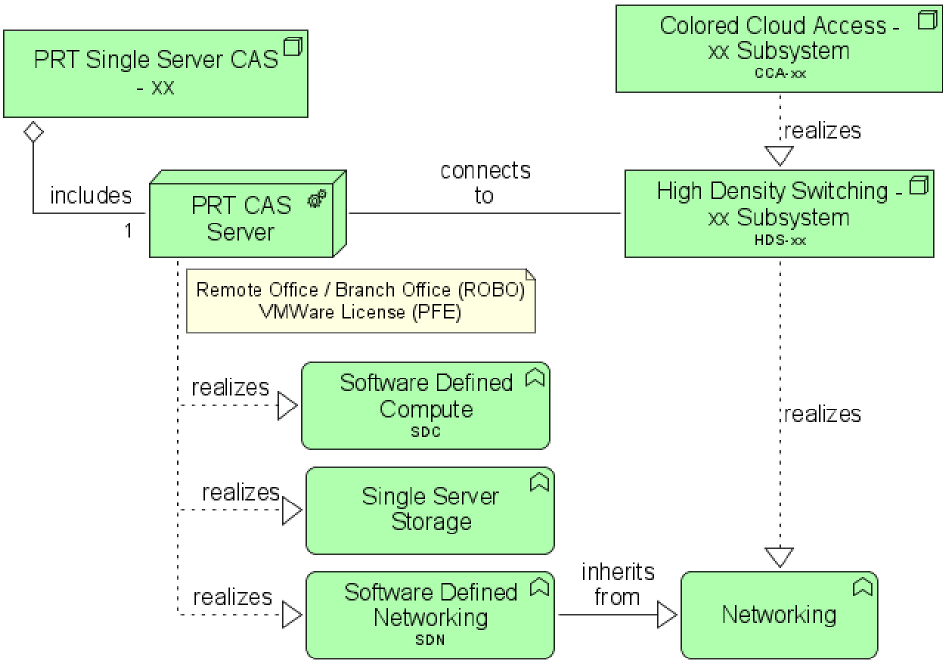
PRT Single Server CAS - XX
Colored Cloud Access - xx Subsystem
CCA-xx
realizes
includes
1
PRT CAS Server
connects to
High Density Switching - xx Subsystem
HDS-xx
Remote Office / Branch Office (ROBO) VMWare License (PFE)
realizes
Software Defined Compute
SDC
realizes
realizes
Single Server Storage
realizes
Software Defined Networking
SDN
inherits from
Networking

Figure 69 - Single Server CAS variant implementation concept

SRS (PRTTDCIS-4299)

~~SRS-682~~ The server in the Single Server Variant of the CAS subsystem shall implement the Storage function with RAID level redundancy.

SRS (PRTTDCIS-4300)

~~SRS-683~~ The Single Server Variant of the CAS subsystem shall implement VMWare as an hypervisor with PFE licenses.

NOTE (PRTTDCIS-4301)

~~[166]~~ The VMWare PFE licenses for the Single Server variant of the CAS subsystem are of Remote Office/Branch Office (ROBO) type with license servers located in PRT NDN.

SRS (PRTTDCIS-4578)

~~SRS-684~~ AN and BCC Nodes shall support the installation of license servers in order to support Nodes with Single Server variant of the CAS subsystem ROBO licenses in place of PRT NDN.