R7 GuiLin Requirements for 5G Service Modeling, Configuration & Persistency Service, PNF Pre-onboarding, and CMPv2

- ONAP Virtual Face to Face (Apr 21-23, 2020)
- ONAP Requirements Subcommittee Presentation (Apr 21)

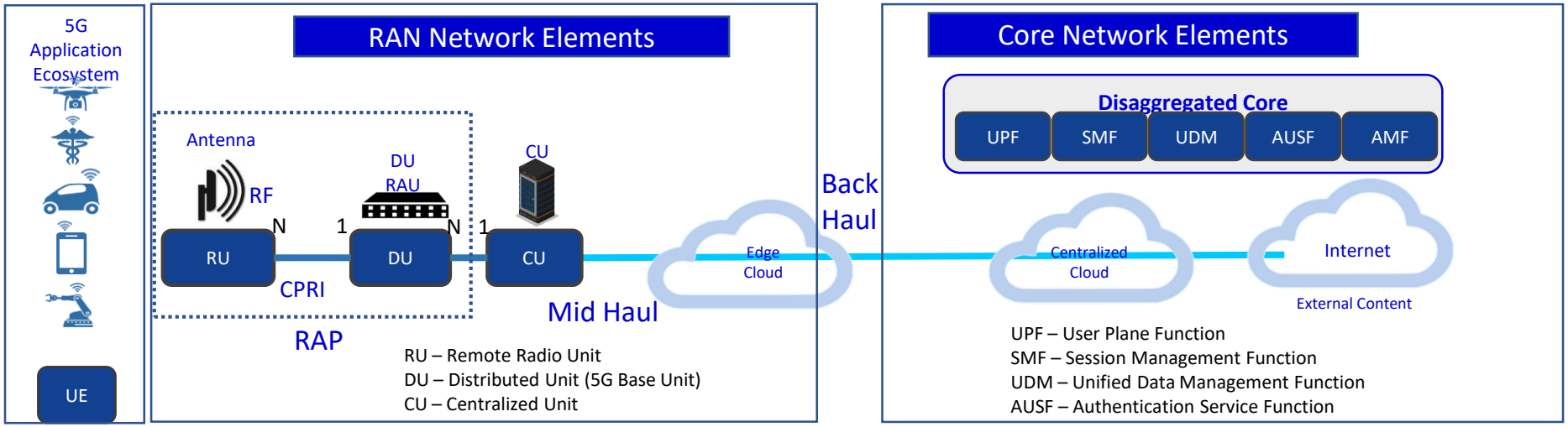
Benjamin Cheung, PhD

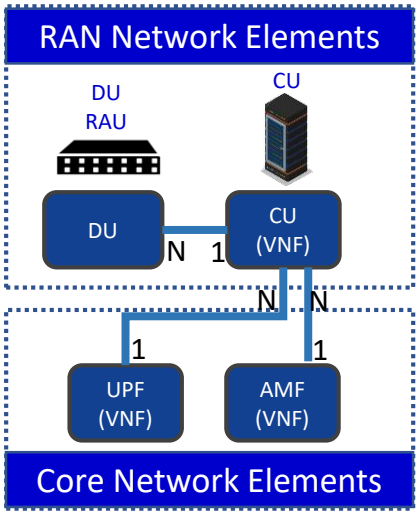
Apr 21, 2020 version 1

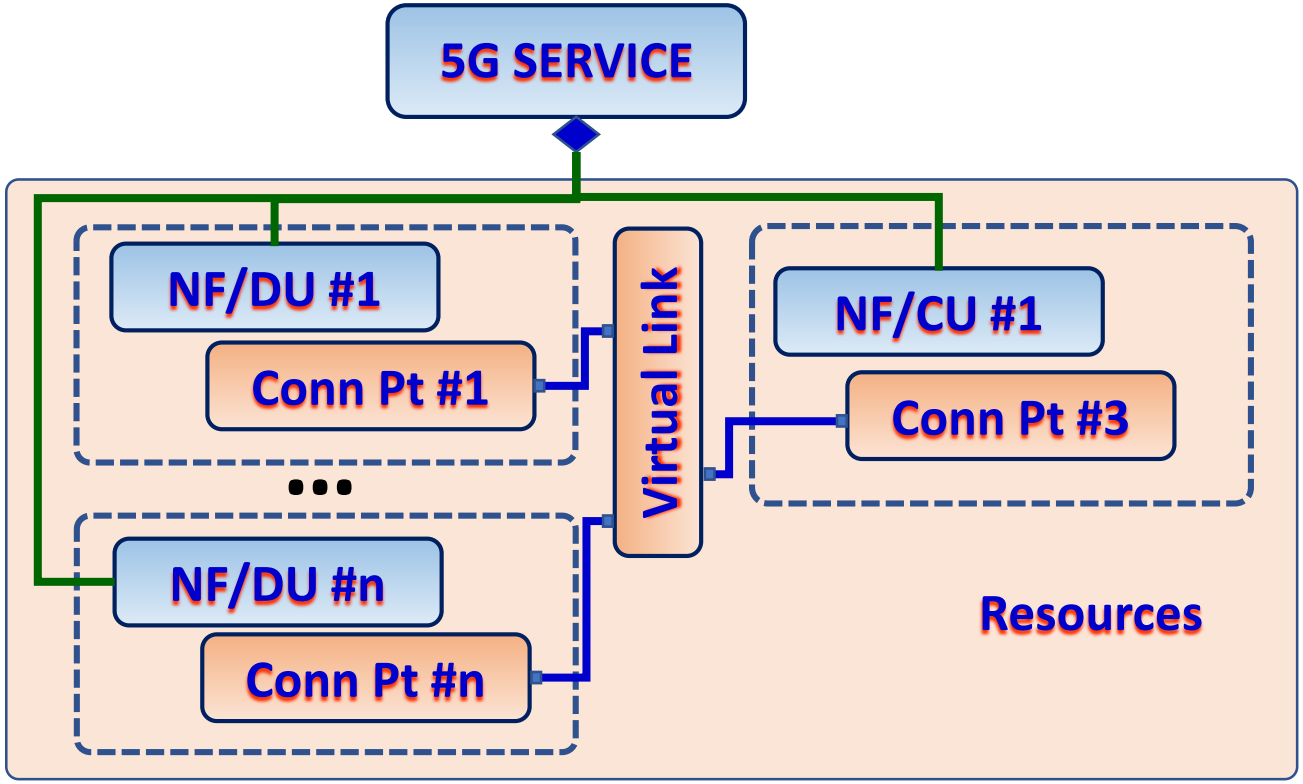
R7 Guilin Requirements

5G USE CASE	DESCRIPTION	Req vs U/C	5G Specific
5G SERVICE MODELING & DEFINITION (5G)	Defining and modeling a 5G Service (in Design Time) and associated Modeling (Platform Info & Data Model).	Requirements	5G
CONFIGURATION & PERSISTENCY SERVICE	Configuration Persistency Service using internal Database for storing Network related data for use in LCM, OSS, Network, Operational applications.	Requirements	General
PNF PLUG AND PLAY	PNF PnP handles the PNF discovery and registration by ONAP during installation & commissioning. PRH (PNF Registration Handler) enhancements	E2E Use Case	General
CMPv2	Certificate Management Protocol	Requirements	General

5G SERVICE CREATION & MODELING in R7 Guilin







5G Service Model & Creation – Business Driver

EXECUTIVE SUMMARY - This requirement introduces platform information model enhancements to document new ISOMII experimental classes from 3GPP TS28.541, the 5G Network Resource Model (NRM).

BUSINESS IMPACT - The requirement, is a critical because it will serve to lay the ground-work for actually "turning on" a real 5G DU (PNF) that might be installed by a Vendor.

BUSINESS MARKETS - This project applies to any domain (wireless, transport, optical, and wireline) that ONAP may manage.

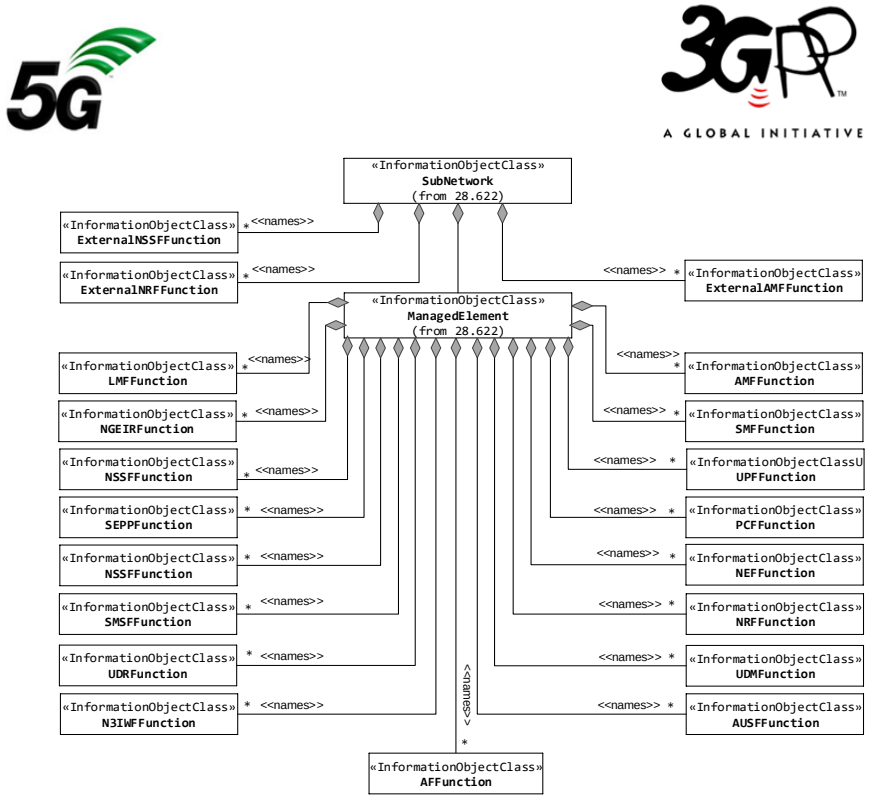
FUNDING/FINANCIAL IMPACTS - Without the groundwork laid down for information model management of a 5G Service, operators will not be able to "turn on" a real live 5G network using "live" PNF resources. No Network. No Business. High OPEX impact.

ORGANIZATION MGMT, SALES STRATEGIES - There is no additional organizational management or sales strategies for this use case outside of a service providers "normal" ONAP deployment and its attendant organizational resources from a service provider.

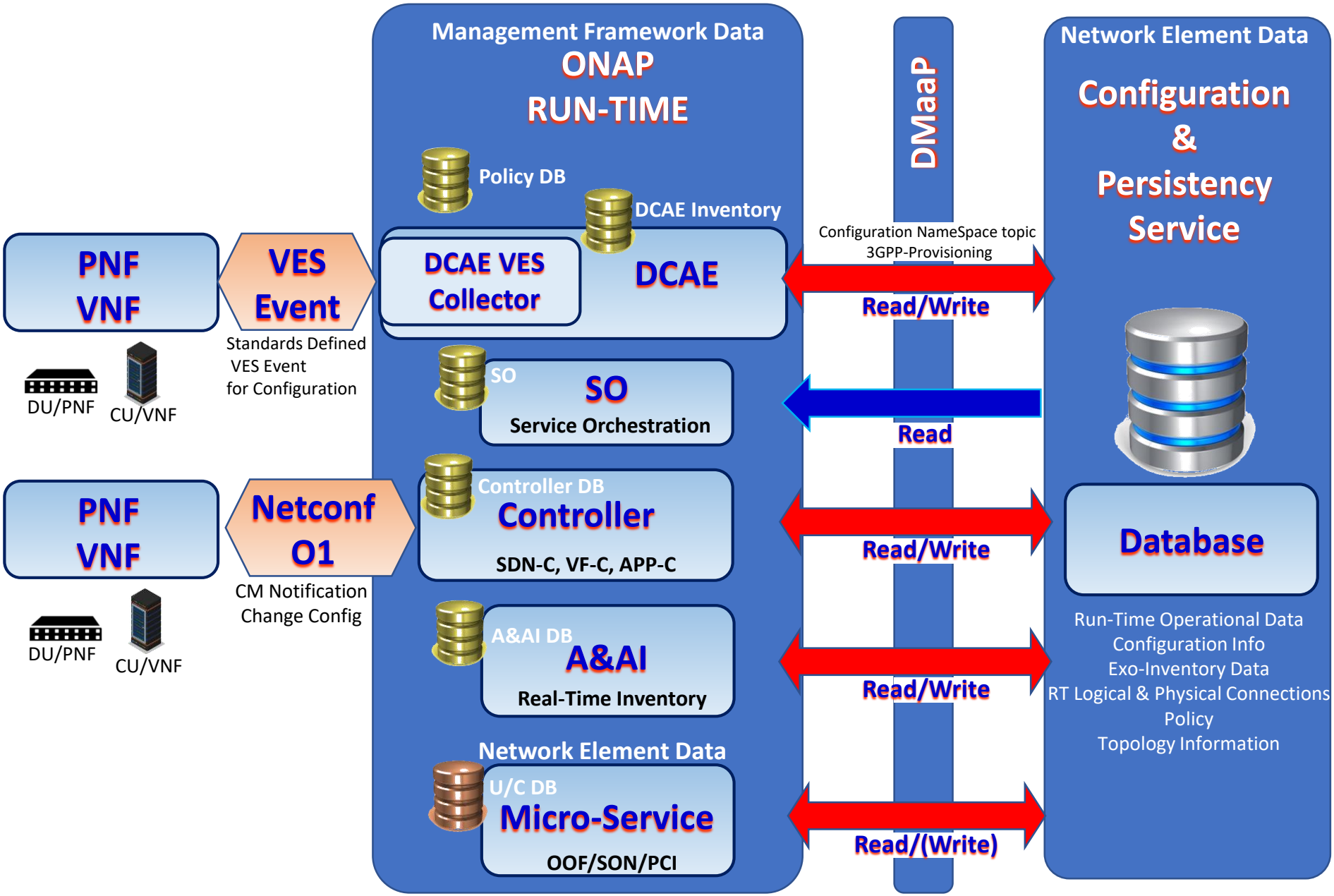
3GPP TS 28.541 V15.4.0 (2019-09)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Management and orchestration;
5G Network Resource Model (NRM);
Stage 2 and stage 3
(Release 15)



Configuration & Persistency Service in R7 Guilin



CONFIGURATION & PERSISTENCY SERVICE in R7 Guilin

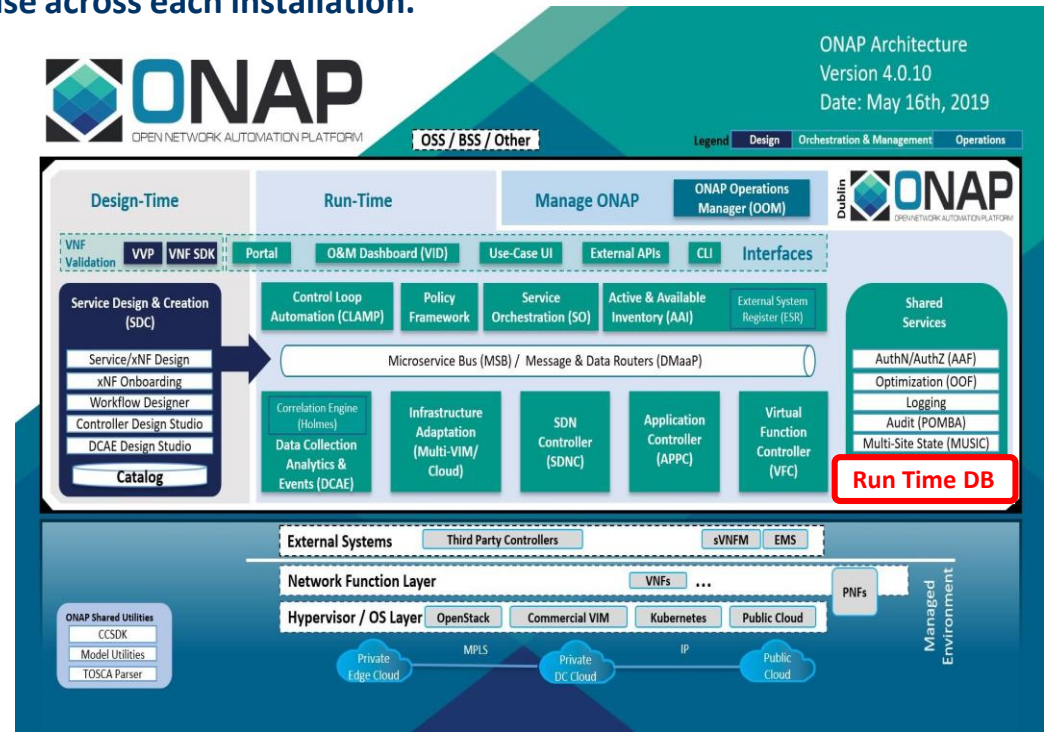
EXECUTIVE SUMMARY - The RunTime Configuration Database / Data Persistency Service is a new platform component that is designed to serve as a data repository for Run-time data that needs to be persistent. As a stand-alone ONAP component, this project provides data layer services to other ONAP platform components and use cases that require persistent configuration or operational data. The R6 development will be enhanced as well.

BUSINESS IMPACT - The ability for service operators to visualize and manage data in a RAN network (PNFs, VNFs, and logical constructs) with ONAP is a critical business function because they are key Life Cycle Management (LCM) and OA&M operations. The project has business impacts to enhance the operation of data-handling within ONAP by providing efficient data layer services.

BUSINESS MARKETS - This project applies to any domain (wireless, transport, optical, and wireline) that ONAP may manage. It is not a market or geographical specific capability. It is expected that scaled ONAP installations such as Edge & Core ONAP deployments will also deploy the database across each installation.

FUNDING/FINANCIAL IMPACTS - This project represents a large potential Operating Expense (OPEX) savings for operators because of the ability to configure networks saving time and expenses.

ORGANIZATION MGMT, SALES STRATEGIES - There is no additional organizational management or sales strategies for this use case outside of a service providers "normal" ONAP deployment and its attendant organizational resources from a service provider.



PNF PRE-ONBOARDING/ONBOARDING U/C OVERVIEW

1 PNF Package Delivery: Vendor creates & delivers PNF Package with PNF artifacts

- PNF Descriptor
- NF Registration
- PM Dictionary Schema (YAML)
- Informational Artifacts
- Configuration Files
- Ansible Playbook

2 PNF Pre-Onboarding: VNF-SDK ( ) to (create) PNF Onboarding Package & *validates* of PNF onboarding package

3 PNF Onboarding package: Package loaded

CSAR Package

Package creation

PNF Onboarding Package

Onboarding

+VENDOR META DATA

Distribute

SO, AAI, DCAE etc.

4 SDC: NF OB Package > SDC catalog

5 ONAP RT Components: Ingest and use CSAR package

PNF PRE-ONBOARDING – Business Driver

EXECUTIVE SUMMARY - This requirement enhances the PNF Pre-onboarding use case. This requirement introduces package security Option2 improvements on Signature per artifact on the Vendor delivered package as defined in ETSI NFV SOL004 v2.7.1. The validation of onboarded PM dictionary data based on schema information will be done. (What is added from existing functionality)?

BUSINESS IMPACT - The enhancement to Onboarding & Pre-onboarding is a critical business function because they are vital to design-time operation to properly onboard vendor packages.

BUSINESS MARKETS - This project applies to any domain (wireless, transport, optical, and wireline) that ONAP may manage.

FUNDING/FINANCIAL IMPACTS - The PNF Onboarding & Pre-onboarding use case has Operating Expense (OPEX) savings for operators because of the ability to saving time and expenses during installation and commissioning of PNF resources.

ORGANIZATION MGMT, SALES STRATEGIES - There is no additional organizational management or sales strategies for this use case outside of a service providers "normal" ONAP deployment and its attendant organizational resources from a service provider.

ETSI GS NFV-SOL 004 V2.7.1 (2019-12)

**Network Functions Virtualisation (NFV) Release 2;
Protocols and Data Models;
VNF Package and PNFD Archive specification**

5.2 VNF package manifest and certificate files

In option 1 (see clause 5.1) the manifest file provides the VNF package integrity and authenticity assurance. In this option the manifest contains the digests (hashes) for each individual file locally stored within the VNF package or referenced from it. Each file related entry of the manifest file includes the path or URI of the individual file, the hash algorithm and the generated digest. A consumer of the VNF package shall verify the digests in the manifest file by computing the actual digests and comparing them with the digests listed in the manifest file.

In option1 the VNF package authenticity is ensured by signing the manifest file with the VNF provider private key. The digital signature is stored in the manifest file itself (see clause 5.3). The VNF provider shall include an X.509 certificate [8] in the VNF Package. The certificate shall be either placed in a certificate file with extension .cert or, if the chosen signature format allows it, the certificate may be included in the signature container itself. The certificate provides the VNF provider public key.

In option 2 (see clause 5.1), the VNF package authenticity and integrity is ensured by signing the CSAR file with the VNF provider private key (option 2 in clause 5.1). The digital signature is stored in a separate file. The VNF provider shall also include an X.509 certificate. The certificate may be included in the signature itself if the signature format allows it or in a separate file. The signature and certificate files shall be siblings of the CSAR file, i.e. placed in the same folder in the parent archive. The signature file shall have an extension .cms and the same name as the CSAR file. Naming conventions for the certificate file are specified in clause 4.3.6.

In this alternative (option 2 in clause 5.1) it is not required to include digests (hashes) per each individual file or artefact in the manifest file. A consumer of the VNF package can verify the signature of the complete CSAR package with the VNF provider public key.

Table 5.2-1 summarizes the characteristics of the two possible options for integrity assurance.

Table 5.2-1: Options for VNF Package integrity assurance: summary of characteristics

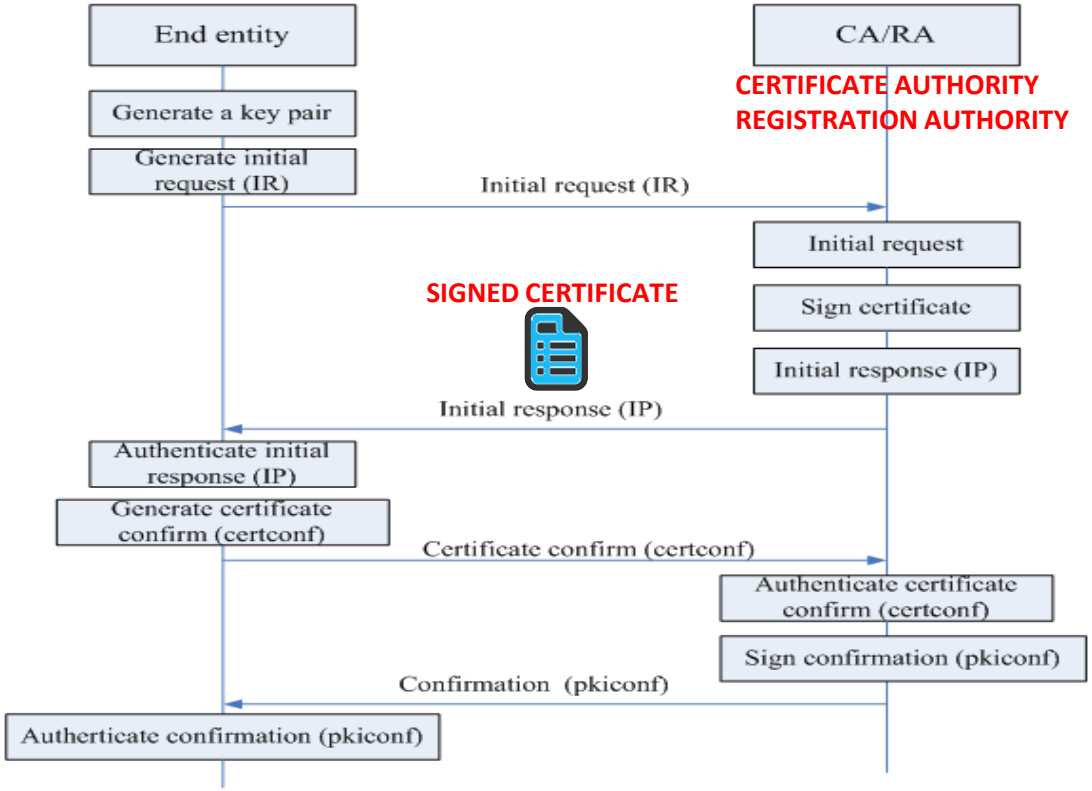
Options	Digest per artifact	Signature per artefact	Support external artifacts	Signature as part of the manifest file	External Signature file for the whole CSAR	Certificate may be part of the signature	Certificate may be in a separate file
Option 1	Yes	Yes (mandatory)	Yes	Yes	No	Yes	Yes
Option 2	No	Yes (mandatory)	No	Yes	Yes	Yes	Yes

The X.509 certificate may contain one single signing certificate or a complete certificate chain. The root certificate that may be present in this X.509 certificate file shall not be used for validation purposes. Only trusted root certificate pre-installed in NFVO shall be used for validation (see clause 5.1).

CERTIFICATE MANAGEMENT PROTOCOL (CMP)

CMP in the TCP/IP model:

application	CMP	CMP			
		HTTP	HTTPS	SMTP	...
transport	TCP				
Internet	IP (IPv4, IPv6)				
link	Ethernet	Token Bus	Token Ring	FDDI	...



- The **Certificate Management Protocol** (CMP) is an Internet protocol used for obtaining X.509 digital certificates in a public key infrastructure (PKI).
- It is defined in **RFC 4210**.
- It uses the **Certificate Request Message Format** (CRMF), in RFC 4211.
- An **obsolete version** of CMP is described in RFC 2510, the respective CRMF version in RFC 2511.
- CMP messages are encoded in **ASN.1**, using the DER method and usually transported over HTTP.

CERTIFICATE MANAGEMENT PROTOCOL (CMP)

EXECUTIVE SUMMARY - This requirement improves ONAP Security with CMPv2. CMP is used by multiple operations including Plug and Play, and NetConf operation. In R6 CMPv2 Certificate Service and basic development was implemented. Integration with server & client to the certificate service will be completed. There are also two ONAP bordering clients to integrate with the certificate service with interfaces to (SDN-C = Done) and DCAE. DCAE interoperation with CMPv2. REQ-140

BUSINESS IMPACT - The enhancement to CMPv2 operation will improve security management within ONAP and affects multiple ONAP functions and use cases, including Plug and Play (PNF registration) and NetConf. As with all security functionality within ONAP, Security is a fundamental aspect of FCAPS, being the "S" for security management.

BUSINESS MARKETS - This project applies to any domain (wireless, transport, optical, and wireline) that ONAP may manage.

FUNDING/FINANCIAL IMPACTS - Potential OPEX savings with enhanced security to prevent breaches and prevent security compromises.

ORGANIZATION MGMT, SALES STRATEGIES - There is no additional organizational management or sales strategies for this use case outside of a service providers "normal" ONAP deployment and its attendant organizational resources from a service provider.