ONAP Interlude Requirements

Manoj Nair
NetCracker Technology
With input/suggestions from Ext-API Project Team

January, 2019

Agenda

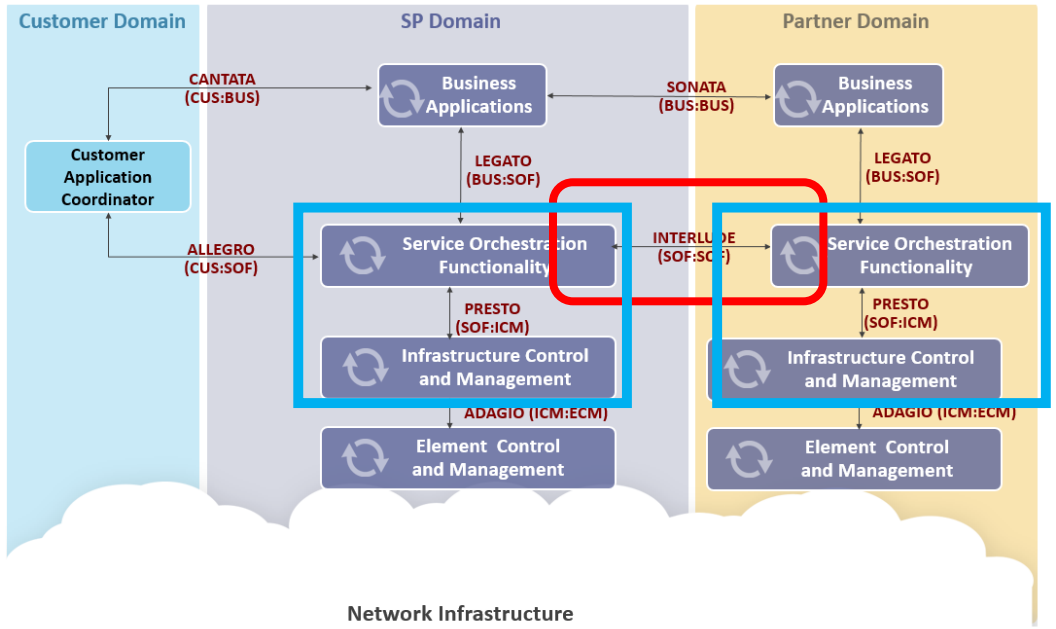
- MEF Interlude Overview
- Inter Provider Interaction General Consideration
- ONAP Component Level Requirements
- Solution Guideline

Context

- Based on study initiated by Ext-API Team to assess the impact of adapting MEF Interlude and equivalent scope in other SDOs
- What this is intended for ?
  - To be used as a reference on possible considerations for adopting MEF Interlude
  - Study focus on the impact on Ext-API project
  - Derive Long Terms Requirements for ONAP Ext-API
  - Guidance for use case teams to leverage MEF Interlude and inter operator interaction
- What this is NOT intended for ?
  - To be used for defining the Ext-API release work items – especially Dublin

MEF Interlude Overview

MEF Interlude Overview



ONAP Scope

SONATA (BUS<->BUS)

- Serviceability Enquiry and Quote Request/Response
- Product Order Request/Response
- Product Order for interfaces, network functions or connectivity

Interlude (SOF<->SOF)

- Service Request for configuration of interfaces, network functions or connectivity
- Connectivity and Performance Testing for the Partner Service
- Reconfigure Partner Service
- Request Performance and Fault Information for Partner Service

Reference : MEF 55

MEF Interlude Scope 2/2

- **Order Fulfillment Orchestration**: deals with establishing or modifying a service through the ordering process
- **Service Control Orchestration** permits the service to be dynamically changed within specific bounds described in policies that are established at the time of ordering
  - Service Control relates to capabilities such as turning on or off connections, throttling bandwidth or other QoS characteristics, etc.

Interlude Scope

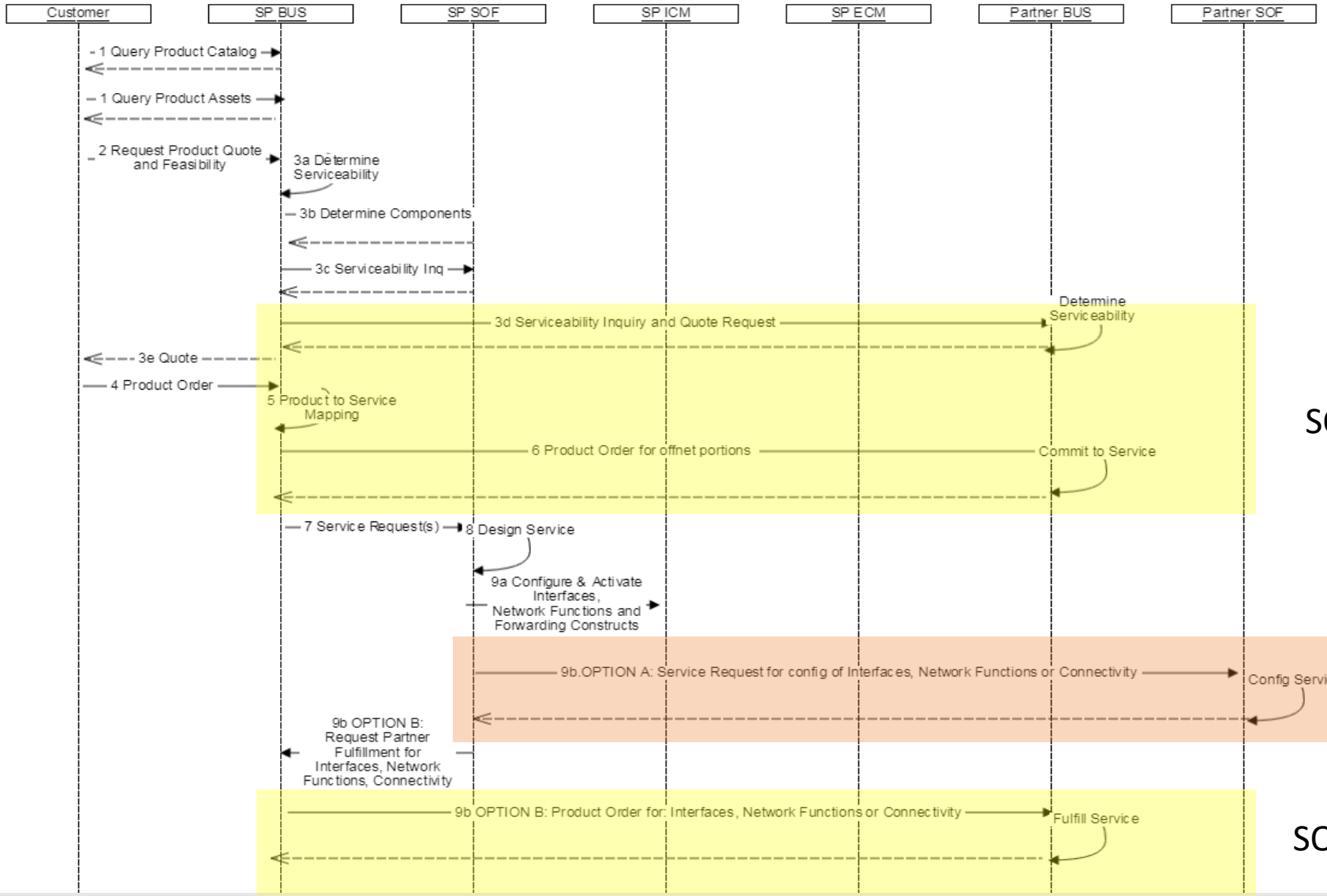
Interlude Prerequisite:

- Service is instantiated through an Order Fulfilment Orchestration process

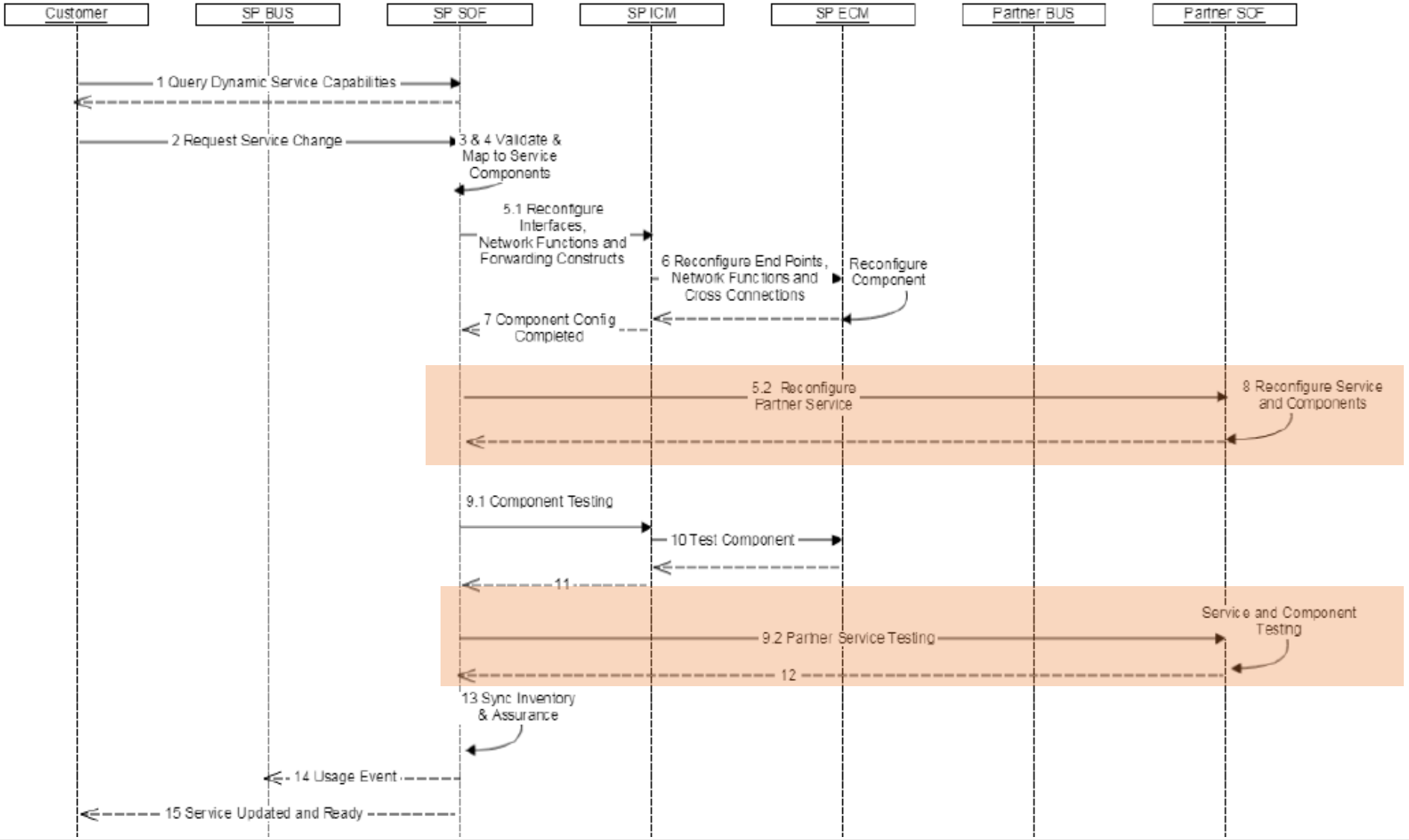
Q. In CCVPN Use Case, Order Fulfilment Orchestration is considered to be part of Ext-API scope via Interlude reference point

- **MEF Interlude scope to be expanded ? – Include Order Fulfilment Orchestration via Interlude**
- **ONAP scope to be redefined ? – Include extended Interlude capability in ONAP**

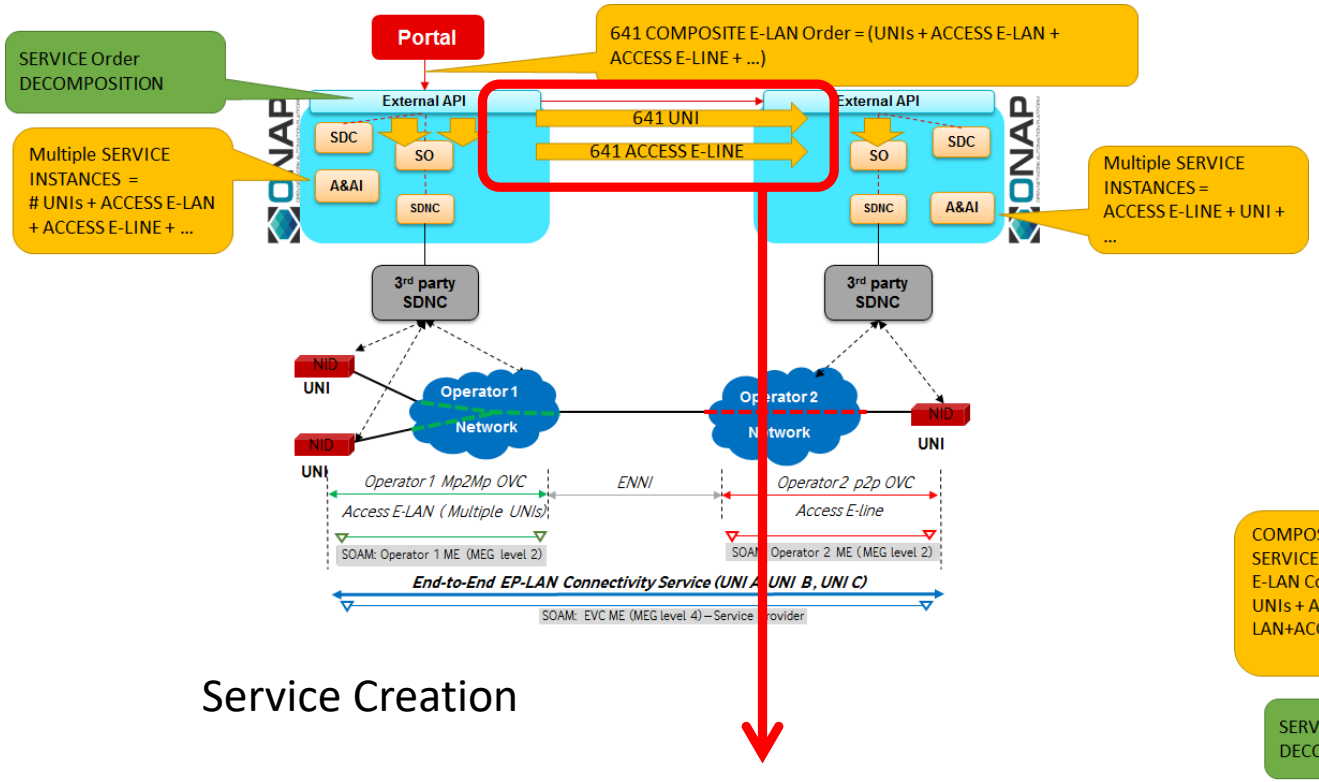
MEF Operational Threads : Product Ordering and Service Activation

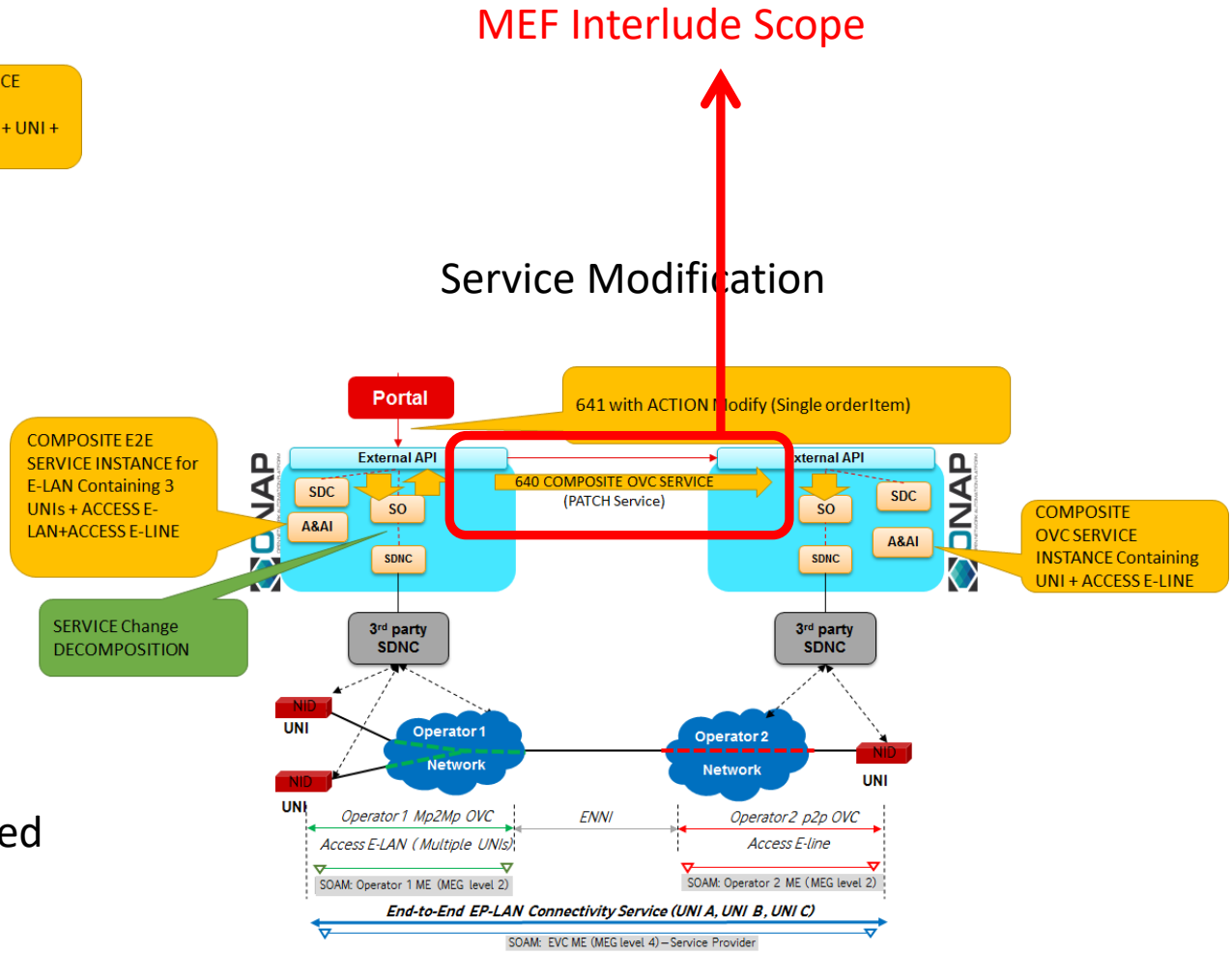


MEF Operational Thread : Controlling Service



CCVPN Use Case D Release Scope





- In CCVPN use case not clarifying how product order fulfilled
- If a product order is initiated at SONATA layer does it continue till service creation or not

Gaps between CCVPN “Interlude-like” implementation and MEF Interlude Scope

Characteristic	CCVPN	MEF Interlude
SOF-SOF interaction scope	Order Fulfilment Orchestration, Service Control Orchestration	Service Control Orchestration
APIs	Current Scope : TMF 641 (Order Management), TMF 640 (Service Configuration) , TMF 638 (Service Inventory Management)	For Full scope : TMF 642, TMF 640, TMF 628, TMF 649, TMF 653
Policy Management	Not supported for inter-provider interaction	To be supported based on the business contract exchanged/agreed over SONATA
Partner Information Onboarding	As part of design process	No reference – handled at SONATA layer
Product Order Management	No reference or no indication of how it is related	Expected to be handled at BSS
Assurance / Closed loop control	Roadmap feature	No closed loop explicitly, but performance and fault notification in scope
Scheduled Service Control Operation	Not supported (Roadmap feature ?)	In scope and to be supported by partner
Service Control/Configuration	Planned for Dublin – But Delete followed by Create of Service	No guidelines on implementation, but operational thread suggests a delta attribute change
Service Test Support	Not supported (Roadmap feature?)	In scope
Subscription for notification	Capability available . Supported at NBI of Ext-API	No explicit requirement, but asynchronous notifications to be supported
Security	No explicit capability other than HTTPS based REST API and Basic Authentication	No explicit requirement . To be governed at LSO level
OSS/BSS Authorization and Notification for Interlude operation	Not supported	In Scope as per the MEF Interlude Access E-Line Use case
Handle Jeopardy conditions	No explicit capability . But can be supported through workflows	No explicit requirement, but required as per Access E-Line use case

Inter Provider Interaction General Consideration and Scope for Ext-API

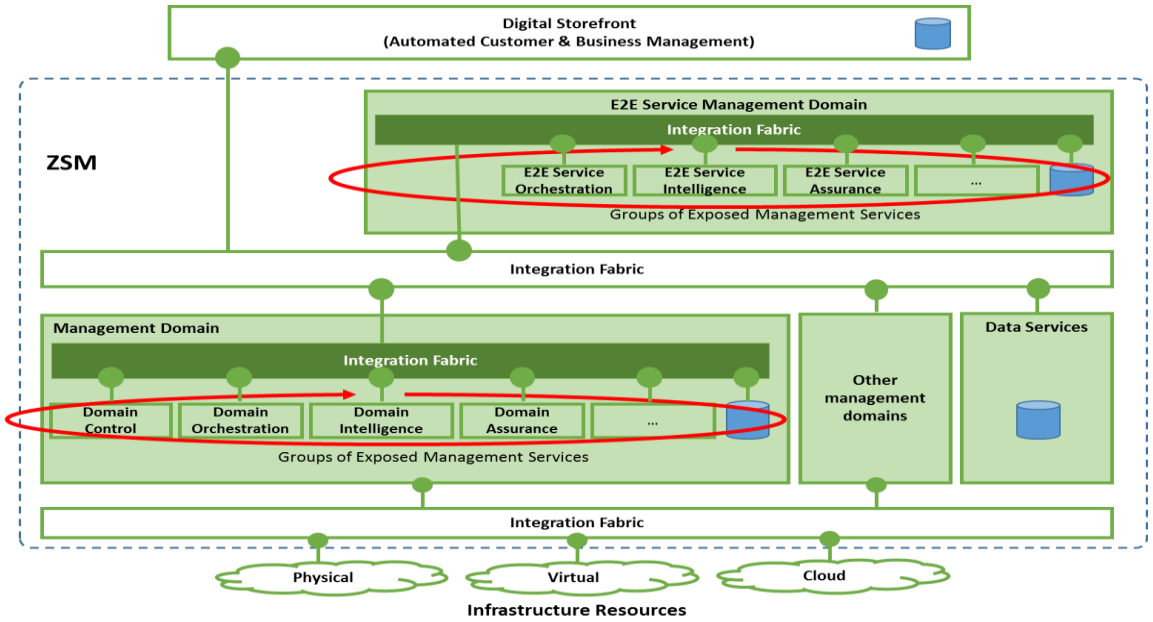
Multi-Domain Interaction

Example Scenario : ETSI ZSM Multi Domain Integration

- End to end Management Domain by SP
- Delegated Management Domain by Partner

Consideration :

- Relevance of Interlude reference point between two administrative domains where E2E domain managed by SP and a specific contextual domain handled by partner



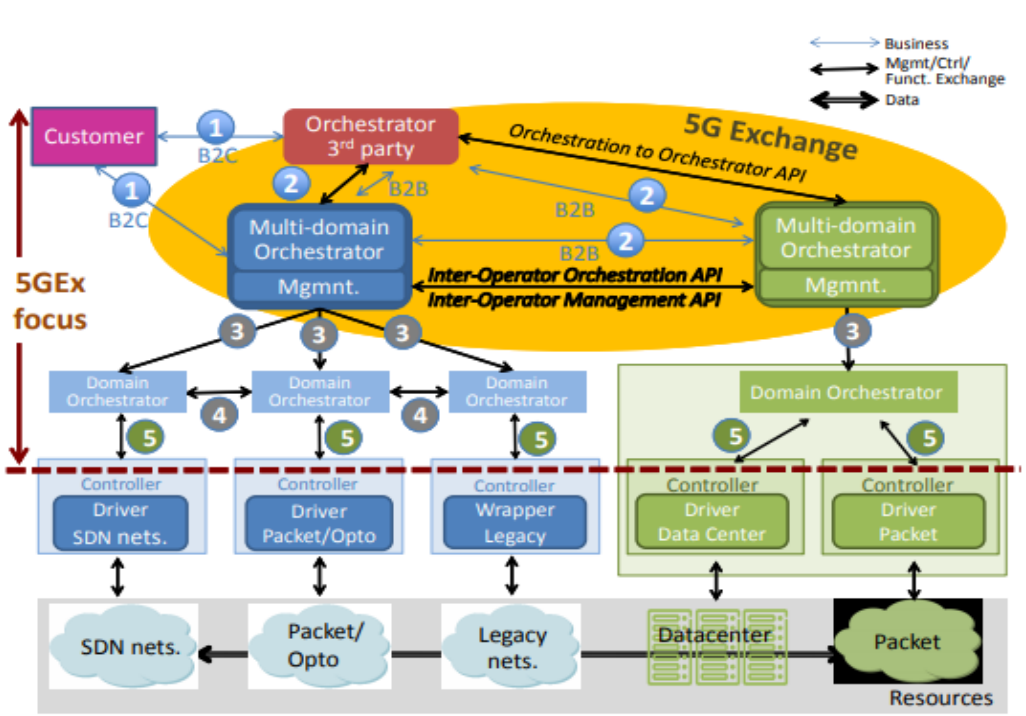
Relevance for ONAP Ext-API :

- **As long as the interaction is via Ext-API and scope is w.r.t what MEF Interlude defines (interaction between SP and Partner for On-Demand Service Control Orchestration) there is no impact**
- **If the interactions has other scope i.e. to other SDO interfaces/APIs (e.g. ETSI Os-Ma) there may be additional scope to be covered in Ext-API**

Federation and Delegation

Example Scenario : 5GPPP 5GExchange Project

- **Peer to Peer Paradigm** : Interaction between Multi-domain Orchestrators in two administrative systems (Federation) – e.g . CCVPN use case
- **Hierarchical Paradigm**: Interaction between Multi-domain Orchestrator and Domain Orchestrators (Delegation) – e.g. Central and Edge Orchestration



Consideration :

- Relevance for Ext-API to support Federation and Delegation models

Relevance for ONAP Ext-API :

- **Ext-API scope is limited to supporting Federation model i.e. east-west communication between two administrative domains with established terms and conditions considering ONAP as a black box (i.e. ONAP considered as a single logical entity, not separate components) and limiting the scope to Service level interactions.**

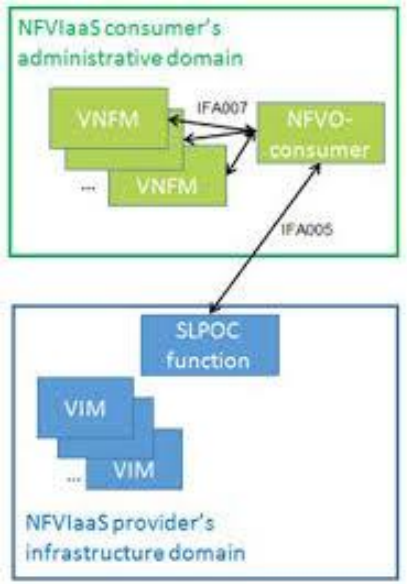
Cross Layer Interaction

Example Scenario : ETSI IFA 028 MLPOC, SLPOC

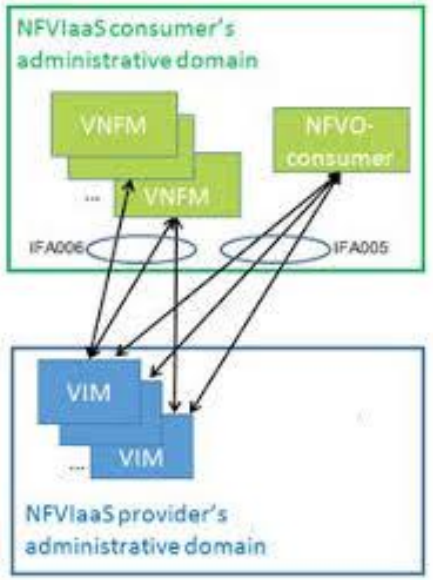
- Single Logical Point of Contact : All interaction between two administrative domains managed through a single function in each administrative domain
- Multiple Logical Point of Contact : Interaction between two administrative domain handled by different components
  - Example : SP ONAP SO interacting with Partner Multi-Cloud

Consideration :

- Between two administrative domain across SP and Partner can there be multiple interaction points or all the interactions need to be channelized through Ext-API
- Relevance of cross component interaction to be channelized through Ext-API



SLPOC



MLPOC

Relevance for ONAP Ext-API :

- **Ext-API will be the single function responsible for Service level interactions between two administrative domains across SP and Partner.**

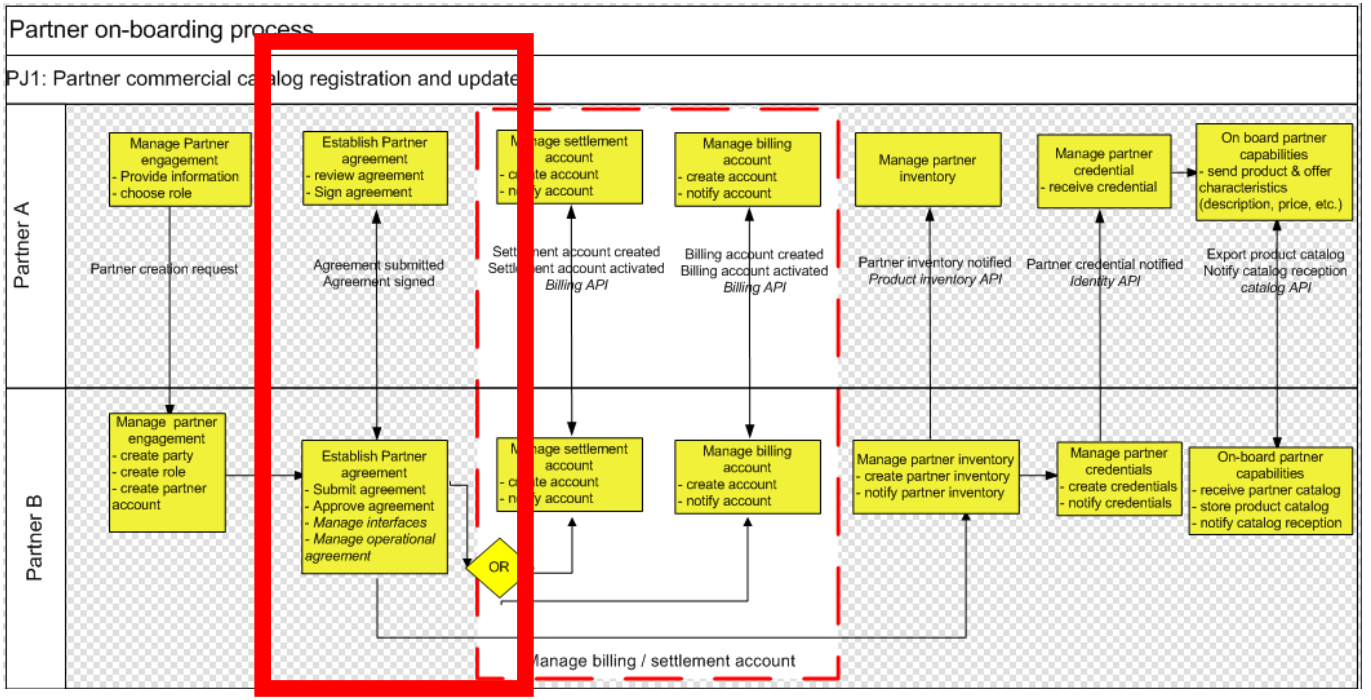
Business Contract & Policy

Example Scenario : Partner onboarding and associated business contract

- Partner onboarding at BSS level and corresponding interactions with ONAP

Consideration :

- Pre-Established Federation governed by business contract and associated policies
- Open Federation managed through capability exchange
- Policies associated with the business agreement and how it is enforced for interaction between SP and Partner



Relevance for ONAP Ext-API :

- **Capability to model and configure policies either via ONAP NBI – optionally through Ext-API, else using the SDC and Policy design time environment**
  - **Design Time Activity : Policy Model based on business agreement between SP and Partner using SDC/Policy Design environment**
  - **Design Time Activity : Policy Model corresponding to product/service driven by product catalog**
  - **Fulfilment Time Activity : Policy Configuration Instance – Created if specific policy to be enforced on a Service – using Policy Configuration API**
- **Ext-API does not support open federation model – in case it is required it requires ability to exchange capability (publicly sharable abstractions of service specification, policies, resources)**
- **Enforcement of pre-established policies at Ext-API – this requires Ext-API to notify policy engine before initiating interaction over the SP-Partner interface and enforcing the decision from policy engine**

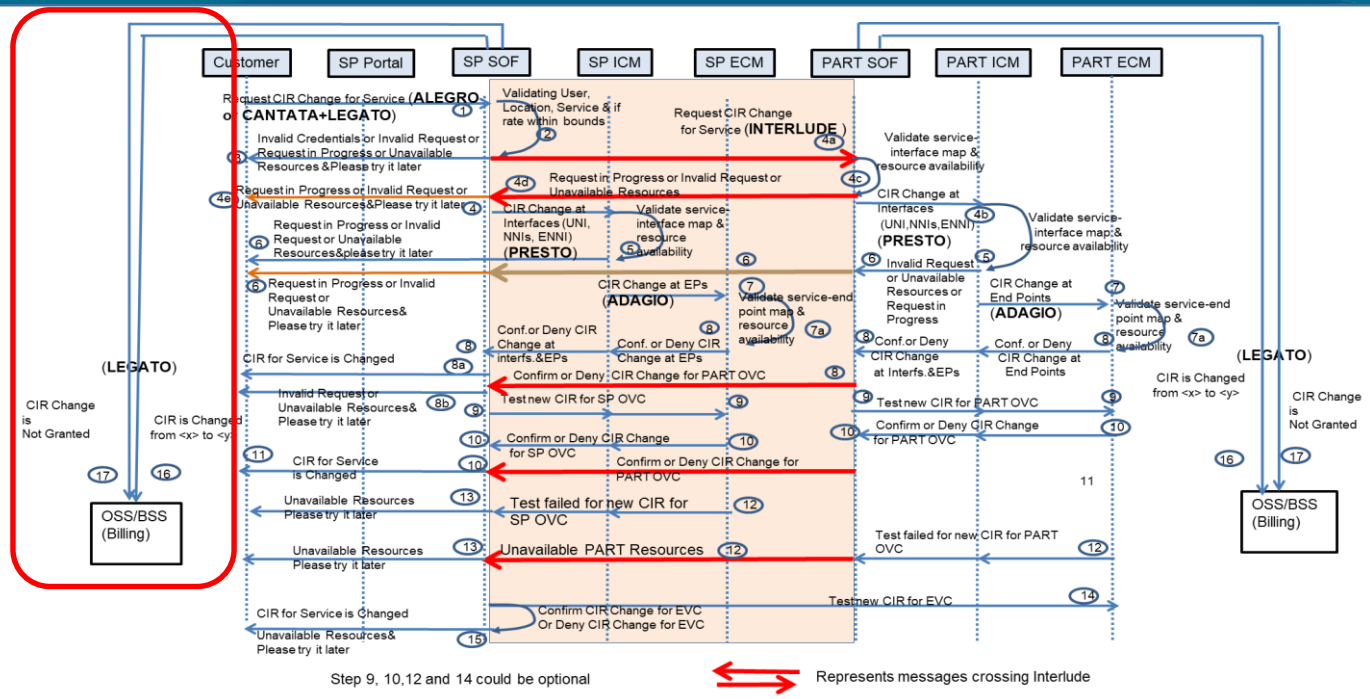
OSS/BSS (Un)Managed Interaction

Example Scenario : SOF notifies OSS/BSS for any interaction over Interlude

- There can be OSS/BSS notified and authorized interactions over interlude and OSS/BSS pre-approved interactions.

Consideration :

- Exchange messages with OSS/BSS to authorize/grant interaction between SP and Partner
- Enable OSS/BSS to provision guard policies to pre-authorize interaction across SP and Partner



Relevance for ONAP Ext-API :

- **API over Legato reference point to request OSS/BSS for authorization of interaction over SP – Partner interface**
- **Ext-API integration with Policy Engine for checking the guard policies for interaction over SP-Partner interface**
- **Service parameter changes on the partner or SP side to be notified to OSS/BSS as this information might be used for billing.**
- **If there is a preconfigured policy in SOF , it will be used for authorization. If there is no policy the authorization request will be forwarded to OSS/BSS over Ext-API**

Design Time Impact

Example Scenario : CCVPN use case - Partner onboarding and associated Design time parameters to be associated with Service

Consideration :

- Currently the partner onboarding in ONAP is done through the SDC by adding an SPPartner Resource
- Limited parameters are supported in the SPPartner currently. MEF Interlude BR demands additional parameters to be supported
- Currently Partner Service attributes are transparent to SDC as these are passed during instantiation as json input

3.9 SPPartner

Attributes	Required	Cardinality	Content	Description
id	M	1	String	Identifier of the SPPartner
url	M	1	String	The url of the ONAP from SPPartner
providingServiceInvarianteUuid	M	1	String	The providing service invariant uuid from SPPartner
providingServiceUuid	M	1	String	The providing service uuid from SPPartner
handoverMode	M	1	String	The handover mode for the cross ONAP. It can be SOTN/SD-WAN

Edge rule in A&AI map SPPartner to Service Id of Partner

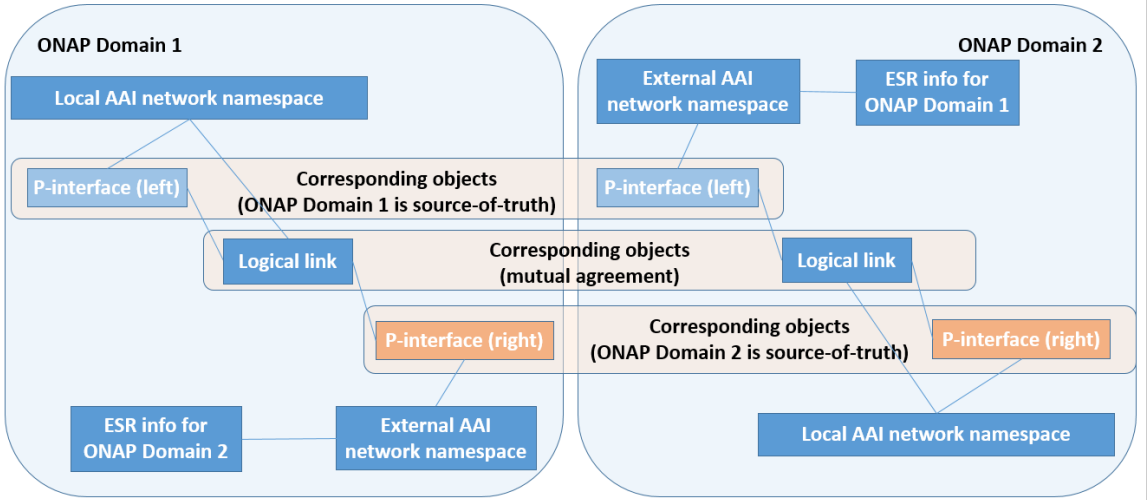
```
{
        "from": "sp-partner",
        "to": "service-instance",
        "label": "org.onap.relationships.inventory.PartOf",
        "direction": "OUT",
        "multiplicity": "ONE2MANY",
        "contains-other-v": "NONE",
        "delete-other-v": "NONE",
        "prevent-delete": "NONE",
        "default": "true",
        "description":"For CCVPN Usecase"
}
```

Relevance for ONAP Ext-API :

- **Partner information capturing in SDC catalog as an additional capability (not as a resource but as an independent entity that can be associated with Service)**
- **Association of SPPartner with Policy in the SDC – To align with Partner level policies**
- **Provision to define SPPartner Service attributes that can be controlled on-demand through the SP – Partner interface**
- **Design Guard Policy to control the authorization of interaction between SP and Partner**
- **Design Configuration policies to define the Service attributes to be controlled over SP and Partner interface**
- **Design Configuration policies to define the constraints for selecting the Partner, checking the capacity, Scheduling Service Control over SP-Partner interface**
- **Ext-API capability to invoke Policy API to check the Guard and Configuration policies**

Inventory Abstraction

Example Scenario : CCVPN use case – Representation/Abstraction of Partner resources in SP local inventory (and vice versa)



Consideration :

- In certain scenarios SP-Partner business contract may restrict direct querying of inventory on the partner side.
- Need for representation of services or resources consumed from the partner in inventory for supporting subsequent operations

Relevance for ONAP Ext-API :

- **This is already handled in ONAP AAI using the network namespace construct (see diagram)**
- **For cases where SP and Partner Business contract supports querying the inventory, Ext-API need to support TMF-638 on the east-west interface between SP and Partner within the boundary/granularity to which the SP is authorized to access**
- **The policies might have to be defined for representing the inventory boundaries that can be queried between SP and Partner**

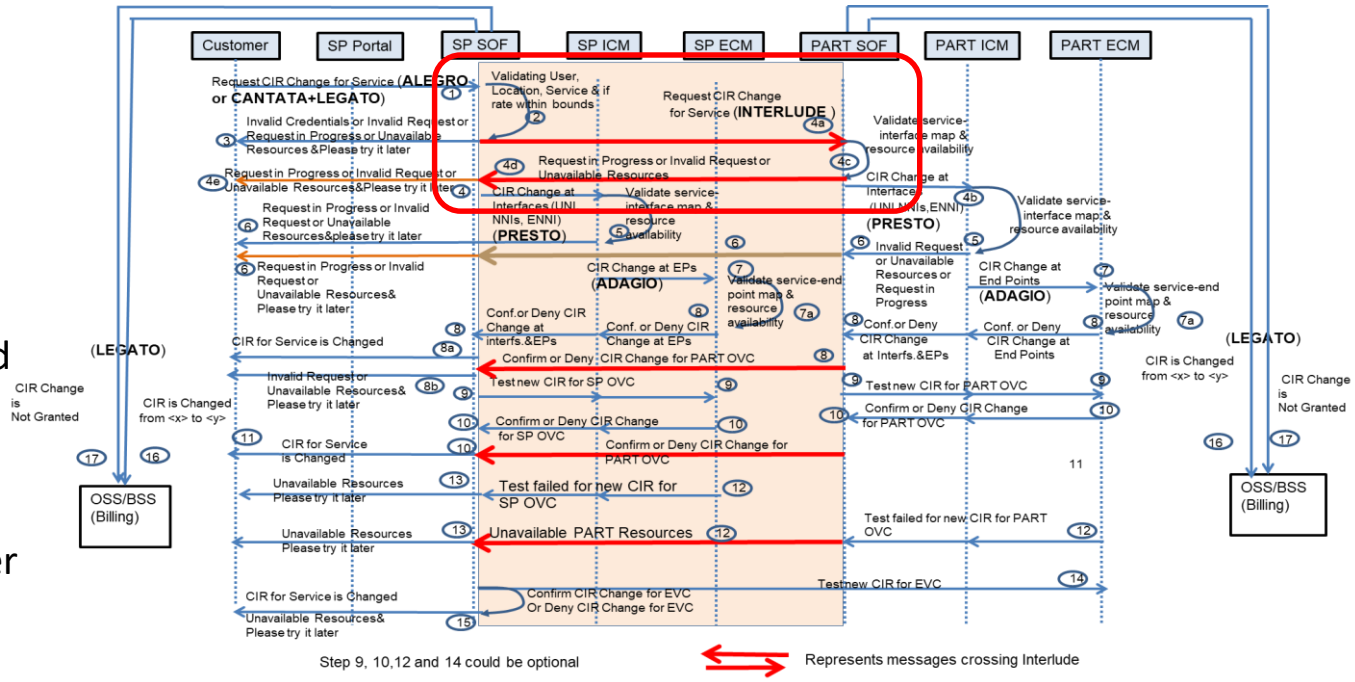
On-Demand Service Control/Modification Support

Example Scenario :

- SP Ext-API receives a request from subscriber or from OSS/BSS for initiating a Service Control/Configuration

Consideration :

- Encapsulation of Service Control/Configuration request via Legato or Allegro interface and possible API support required in Ext-API
- Request that need to initiated on ONAP components for constructing the Service Change/Control Request
- Policy to be checked before initiating request over Sp-Partner
- Error handling mechanism
- Internal handling of a Service Change/Configuration (assuming Partner has an ONAP deployment)

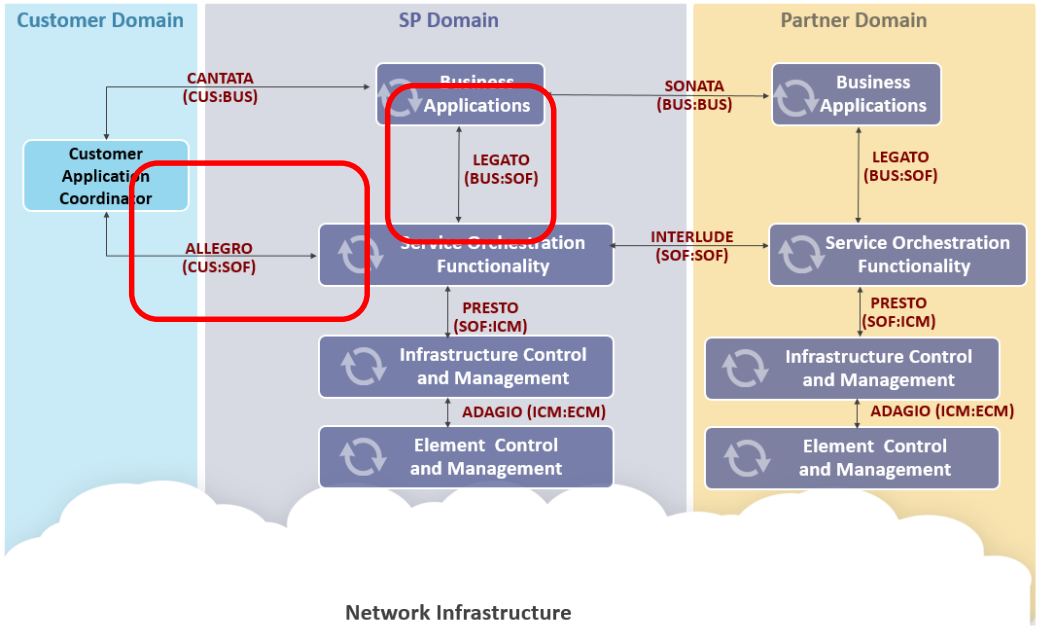


- Service Change Request over Allegra to be supported through TMF 640 supported on Ext-API (real time)
- Service Change Request from OSS/BSS to be supported through TMF 641 Service Order Management (non real time)
- Short term handling of service change request at partner side Ext-API : Delete Service instance and Create Service Instance with modified attributes. A&AI issue of capturing/retaining Service creation parameters to be resolved

On-Demand Service Configuration Initiation

Example Scenario :

- As per MEF LSO architecture, the On-Demand Service Modification can be initiated by Customer via the Allegro interface or by the OSS/BSS via the Legato interface.



Consideration :

- Differential treatment required between requests from two end points in terms of business agreement
- API alignment for supporting request over two reference points – Allegro and Legato
- Need for notifying OSS/BSS about on-demand service configuration/Control
- Pre-authrorization by OSS/BSS to accept/deny requests over Allegro

Relevance for ONAP Ext-API :

- **As per the proposal by Orange, Request over Allegro will be via the TMF 640 API and Request over Legato will be over TMF 641**
- **Any preauthorization required should be initiated through a policy configuration and corresponding differential treatment will be applicable**

Runtime Identifier Management

Consideration :

- Identifiers that can be used as reference for Service Specification, Service outside ONAP
- How these Identifiers are generated/managed
- How these identifiers are mapped to the internal Service Model maintained in the catalog
- Type of Identifiers to be maintained
  - Service Order Identifier that is being used to instantiate Service either via the BSS - SOF Legato reference point or via the SOF-SOF Interlude reference point (assuming Service Instantiation is within the scope of Interlude)
  - Service Instance Identifier for the Service that is being instantiated at Partner side (reference in the A&AI/Inventory system on the Partner side)
  - Service Specification Identifier - Service Specification Identifier used by Ext-API or equivalent component on the partner side
  - Service Model Identifier in the Service Catalog maintained by Partner

Relevance for ONAP Ext-API :

- **Ext-API maintains own catalog for Service Order and Service Specification**
- **The identifier maintained in Ext-API catalog to be the reference used external . External identifiers are managed by Ext-API**
- **Ext-API need to have own mapping logic to map between internal SDC catalog Service Identifier and external Identifier**
- **The identifier maintained by partner and to be referred by SP**
  - **Service Specification Identifier – To be passed on via OSS/BSS to Ext-API via Sonata->Legato or as SDC design input**
  - **Service Instance Identifier - To be passed on to SP via SONATA -> Legato or via interlude in response to TMF 641 (Service Order Mgmt) assuming Interlude has extended scope to instantiate Service on Partner.**

Service Assurance

Example Scenario :

MEF Interlude defines the scope for receiving Service specific event notifications/Performance matrix from the partner.

- Service Provider receives Service specific event notifications from the Partner
- Service Provider receives Service specific performance information from the Partner

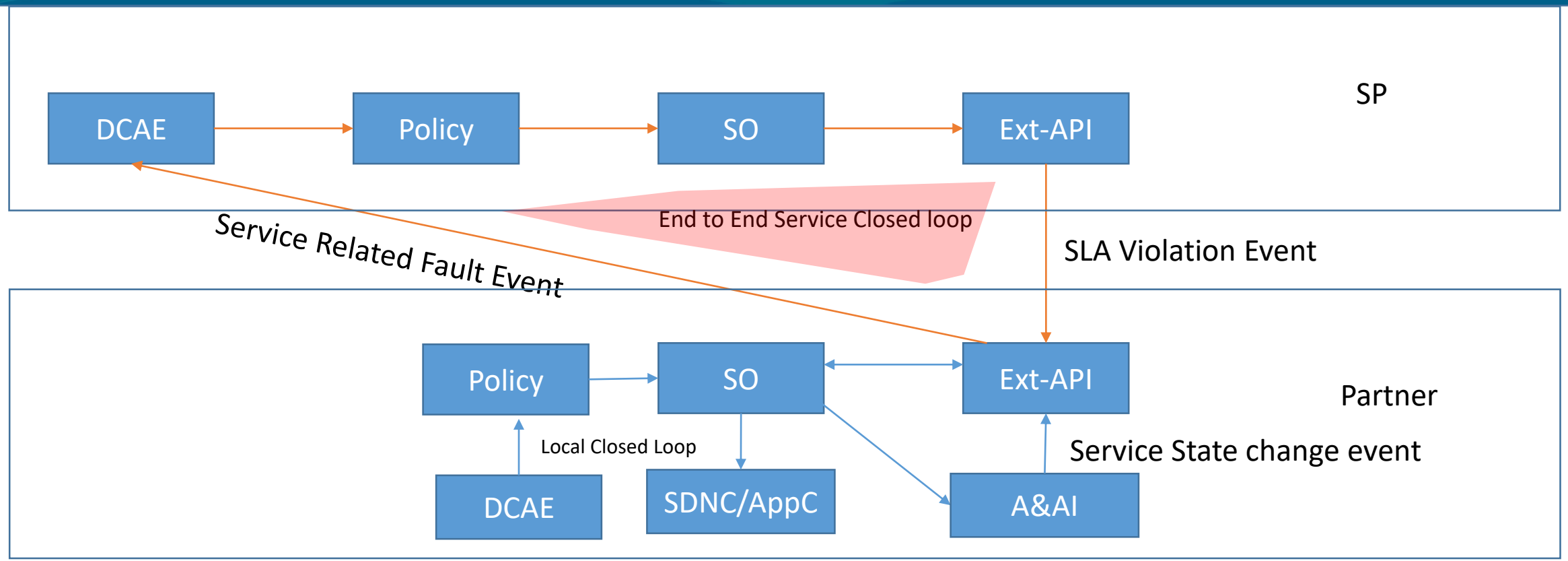
Consideration :

- Registration of events and performance metrics, SLA/SLO on partner
  - Specific request through Interlude
  - Request initiated through the Service instantiation process
  - Requested initiated by OSS/BSS
- Registration of hub resources (holds call back address) for receiving the events and performance metrics SLA/SLO

Relevance for ONAP Ext-API :

- **On the SP side**
  - **Functionally it makes more sense to delegate this function to specialized components like DCAE**
  - **SDC need to have a capability to represent Partner Performance and Fault metrics configuration to be initiated at DCAE (via DCAE Design studio) and associate that with the SPPartner resource . SDC to distribute such Fault/Performance metrics on local DCAE , Ext-API, Policy**
  - **CLAMP/DCAE to initiate the policies corresponding to the Partner Fault and Performance metrics**
  - **Ext-API to initiate hub registration request to partner based on configured Fault/Performance metrics – Call back address to be DCAE collector address**
- **On the partner side**
  - **Ext-API to subscribe to DMaaP aggregate Events for Metrics and Fault for the shared service**
  - **Receives request for registration of hub resources for Fault/Performance data , partner sends the update on the created hub resource**

Closed Control Loop



Consideration :

- Closed loop control for the E2E Service : To be handled based on the E2E SLA and corresponding policies configured on the SP ONAP Policy engine
- Closed loop control for Partner/SP provided Services : Closed loop control is managed through local ONAP instance
- In the absence of the local policy for a specific service state change, notification is forwarded to SP for verifying at the E2E level

Management Connectivity with Partner

Consideration :

- Management connectivity with partner through an adhoc end point URL passed on at the time of Design process
- Management connectivity through a dedicated API gateway (independent of Ext-API on SP and Partners side)
- Management connectivity through an interexchange provider

Relevance for ONAP Ext-API :

- **The second approach listed above is more preferred as all the common services related to managing interaction between SP and Partner can be consolidated**
- **MSB in ONAP currently provides partial capabilities w.r.t API Gateway – Specifically routing and load balancing**
- **Route Ext-API calls to partner via MSB External Gateway – manage policy check, authentication, authorization through MSB**
- **Direct communication from Ext-API through adhoc URL passed on at design time is not recommended due to additional capability required in Ext-API for managing connection and security**

Security

Consideration :

- Information/Platform Security: Securing the data at SP and Partner side so that unauthorized and unintended data access can be avoided, Securing the SP and Partner Access credentials, Keys in a secure storage
- Communication security : Securing the communication channel between SP and Partner
- Regulatory controls : Lawful intercept support, Inter-provider exchange guidance, Country-specific controls etc.
- Policy-based controls: Security controls driven by business agreement between parties.

Relevance for ONAP Ext-API :

- **To be governed by the ONAP Security team**
- **Assuming majority of the Security consideration will be handled by MSB, Policy and AAF**
- **In the CCVPN use case there is a dedicated Partner end point configuration required during design time and this is stored in inventory. Additionally the communication between SP and Partner is over a direct REST API call**
- **For securing the communication and to store the Partner related information securely it is required to leverage dedicated components meant for this**
  - **AAF has Authentication & Authorization capability and can work in a distributed manner, has secret key management and provides SDKs to interact with AAF. AAF can be leveraged for storing the Partner end point credentials and end point address**
  - **MSB supports authentication & authorization for service request with plugin to auth service, service request logging, service request rate-limiting, service monitoring, request result cache, solve cross-domain issues.**
  - **MSB also has an ISTO Service mesh integration which can be leveraged in case a service mesh based interaction is preferred**
  - **Ext-API should leverage MSB and AAF services for secure communication**

Information & Data Model

Consideration : To be decided by Modelling subcommittee, TOSCA Task force. Three options for Entity Model of Interlude

- MCM aligned E-Line Service Model defined in MEF Interlude Contribution - Access E-Line Service Control Classes - 5th Draft (link)
- Work in progress MEF Services Common Model (link) - Proposal for Work Item
- Generic Resource Model (TMF 655) being referenced by the TMF 641/640 (based on SID) (link) - Currently followed by CCVPN use case

Relevance for ONAP Ext-API : Assuming current scope is limited to TMF There are two types of models to be considered with high level information of potential data to be maintained at run time and design time.

Design time model :

- **Partner as an abstract resource placeholder for management connectivity details - Currently this is represented as SPPartner Resource in SDC and A&AI. TMF 632 gives a reference to Organization Resource**
- **Role of the Partner - Primary or Subordinate (Mastership Relation)**
- **Partner activation status**
- **Services subscribed**
- **Related business agreement/policy**
- **Service Assurance Related**

Run-time Model :

- **Partner abstract resource model with runtime connectivity parameters such as session details**
- **Partner provided services as an association between Partner abstract resource and Service IDs**
- **Partner consumed services as an association between Partner abstract resource and Service Specifications (SDC Model ID)**
- **Partner connectivity state**
- **Mastership status**
- **Partner Subscriptions (Hub Resources)**
- **Partner Service State**
  - **Partner Service Performance (future)**
  - **Partner Service Faults (future)**
  - **Partner Service Health**

Standard APIs To Be Supported

Interlude Scope	Possible APIs	Ext-API Capability
Service Provider controls aspects of the Service within the Partner domain (on behalf of the Customer) by requesting changes to dynamic parameters as permitted by service policies	TMF 641 Service Order Management API or TMF 640 Service Configuration and Activation Management API	TMF 641 already supported , TMF 640 to be supported To be verified against policy
Service Provider queries the operational state of the Service	TMF 638 Service Inventory Management API (This may be restricted in some deployment scenarios)	Supported , but to be checked against business contract/policy
Service Provider requests change to the administrative state of a service or service component (e.g. Service Interface)	TMF 640 Service Configuration and Activation API	To be supported
Service Provider requests update to defaulted service parameters which are allowed to be customized (policy-controlled)	TMF 641 Service Order API or TMF 640 Service Configuration and Activation API	TMF 641 already supported , TMF 640 to be supported To be verified against policy
Service Provider requests the creation of connectivity between two Service Interfaces as permitted by established business arrangement	TMF 641 Service Order API or TMF 640 Service Configuration and Activation API	TMF 641 already supported , TMF 640 to be supported To be verified against policy
Service Provider provider queries the Partner's Service Inventory for services provided by the Partner to the Service Provider	TMF 638 Service Inventory Management API	Supported , but to be checked against business contract/policy
Service Provider receives Service specific event notifications from the Partner	TMF 642 Alarm Management API or TMF 640/641 Service Order API (ServiceOrderChangeNotification)	Not supported
Service Provider receives Service specific performance information from the Partner	TMF 628 Performance Management API , TMF 649 Performance Management Threshold API	Not supported
Service Provider requests test initiation and receive test results from the Partner.	TMF 653 Service Test Management API	To be supported

ONAP Component Level Requirements to support Ext-API scope

ONAP Component Level Requirements

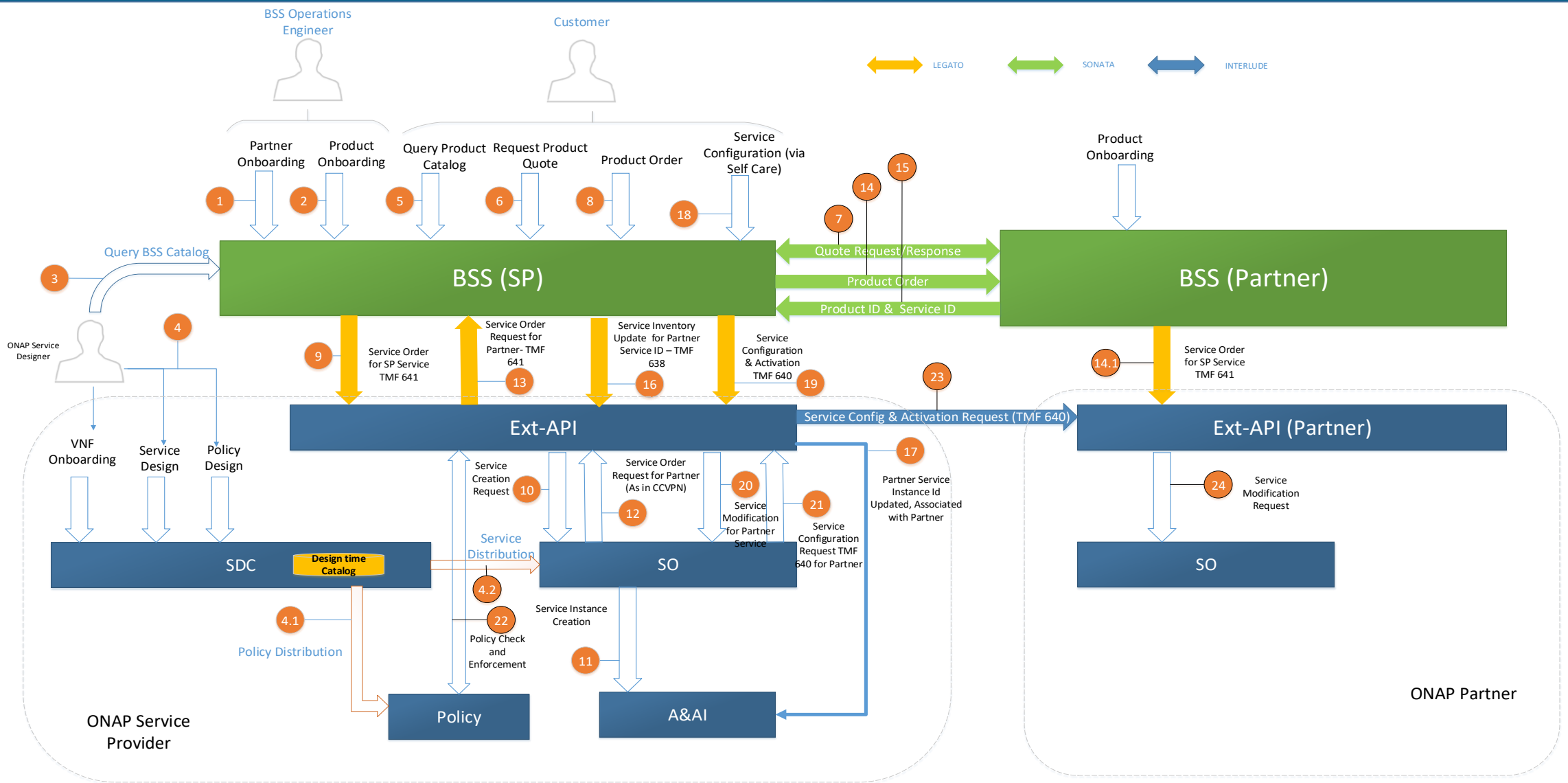
Component	Requirement
Ext-API	1.API support for On-Demand Service Configuration and Control - TMF 640 (Optionally support TMF641 based Service Change Requests – [Service Order with action change] as well) 2.Optional : TMF 641 based Service Order Management to place a Service Order Request on Partner 3.Integration with Policy Engine to check the Partner API access policies, authorization, Service change attribute boundaries 4.Integration with SO to invoke On-Demand Service Configuration/Modification Operation 5.Enhancement of Ext-API to map Service Configuration and Activation Request to SO specific Service Modification Request 6.Enhancement of Ext-API to initiate Service Inventory Query on partner side to check the Service State 7.Enhancement of Ext-API to support notification of Interlude operations to OSS/BSS 8.Enhancement of Ext-API to initiate Partner Service Catalog Query 9.Enhancement of Ext-API to initiate Service Test requests on partner 10.Enhancement of Ext-API to support partner onboarding and integration with AAI or Catalog for persisting Partner registration details 11. Enhancement of Ext-API to register Hub resources for querying Partner service states and receive call backs 12.Integration of Ext-API with MSB and AAF to route the API calls to partner through Ext Gateway 13.Enhancement of Ext-API to manage the external facing identifiers and map it to ONAP internal identifiers (Service instance and Service specification) 14.Enhancement of Ext-API to receive events corresponding to the Service changes from A&AI/SO via DMaaP
SO	1.Support for Service Modification API through a Patch or Put Request 2.Integration with OOF to schedule Service Configuration 3.Additional recipe/workflow for handling Service Modifications locally and for directing it to Partner via Ext-API 4.Handling of Service Modification request with appropriate workflow invocation (dynamic or static workflow) 5.Management of Service Modification jeopardy conditions - additional workflow

ONAP Component Level Requirements

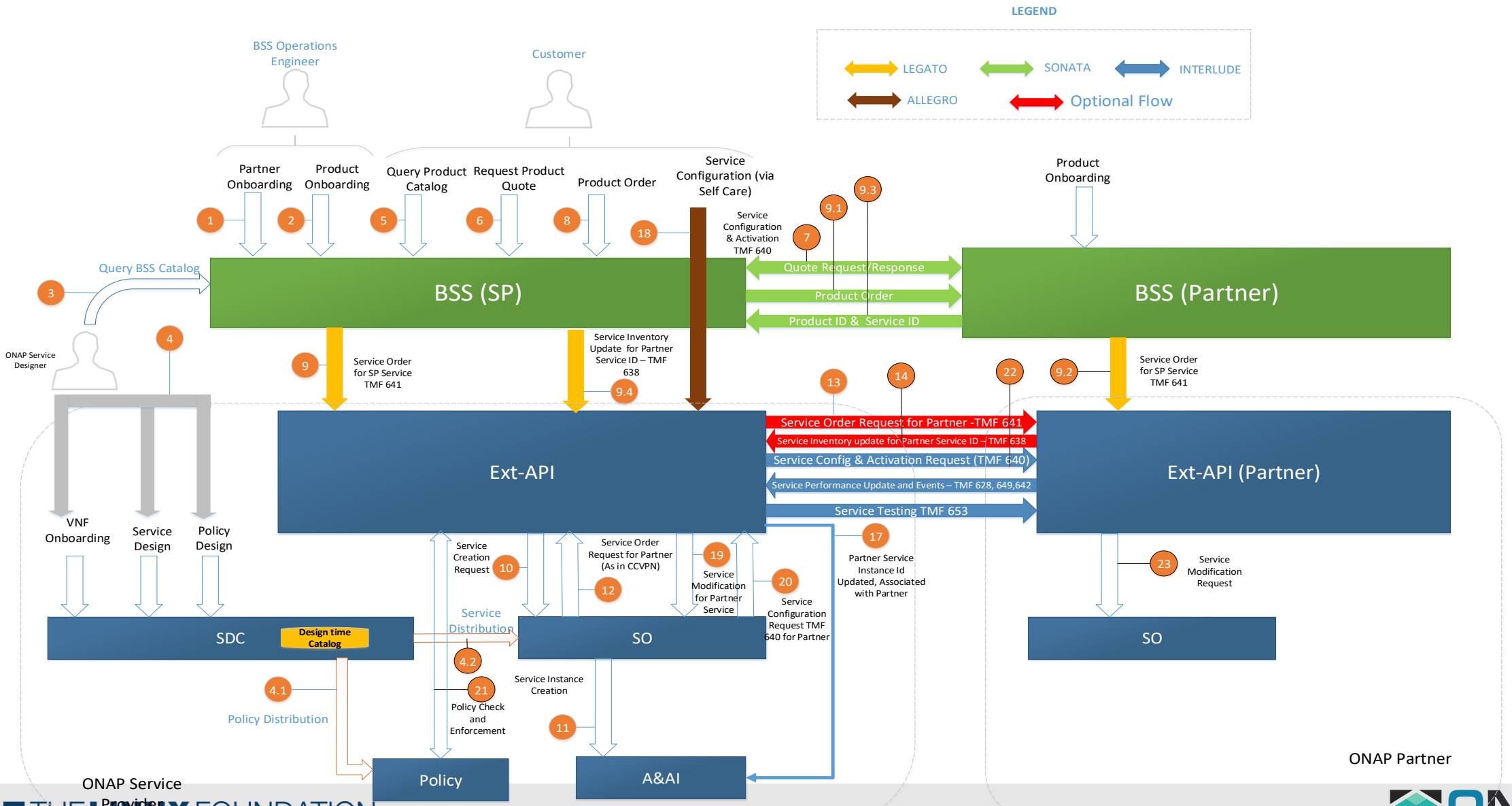
Component	Requirement
SDC	1.Ability to refer Partner registration details either passed on via Ext-API to SDC Catalog or provided as input during design 2.Design and use Policy templates corresponding to business agreement 3.Associate Inter-Provider Interaction Policy with a Partner resource or Service 4.Distribution of Inter-Provider Interaction policies to Policy engine
Policy	1.Pre-loading (without using SDC) or Design time loading of Policy templates for inter-provider interaction policies 2.Creation of Policy for controlling inter-provider interaction control 3.Deployment of inter-provider interaction policies to corresponding PDP (PDP-X) 4.Configuration/Control of PEPs (Ext-API) with Configuration or Guard Policies corresponding to external triggers received by PDP-X
AAF/MSB	1.Configuration of namespace for representing the SP or Partner Ext-API end endpoint AAF 2.Creation of Authentication Certificates (Client and Server) 3.Interaction of AAF across administrative domains 1. Creation of Permissions for SP and Partner Ext-API endpoint as per the policies configured.
OOF	1.Capability to schedule the on-demand service configuration 2.Capability to check the capacity and relevant partner end point for enabling an on-demand service configuration
DCAE	1.To receive Service related notifications from Partner ONAP instance 2. To direct the events to Policy and carry out closed loop control locally at the Partner side or on the SP side for E2E Service 3.Correlate Service related events and enrich with inventory data before passing on to Policy engine

Solution Guideline

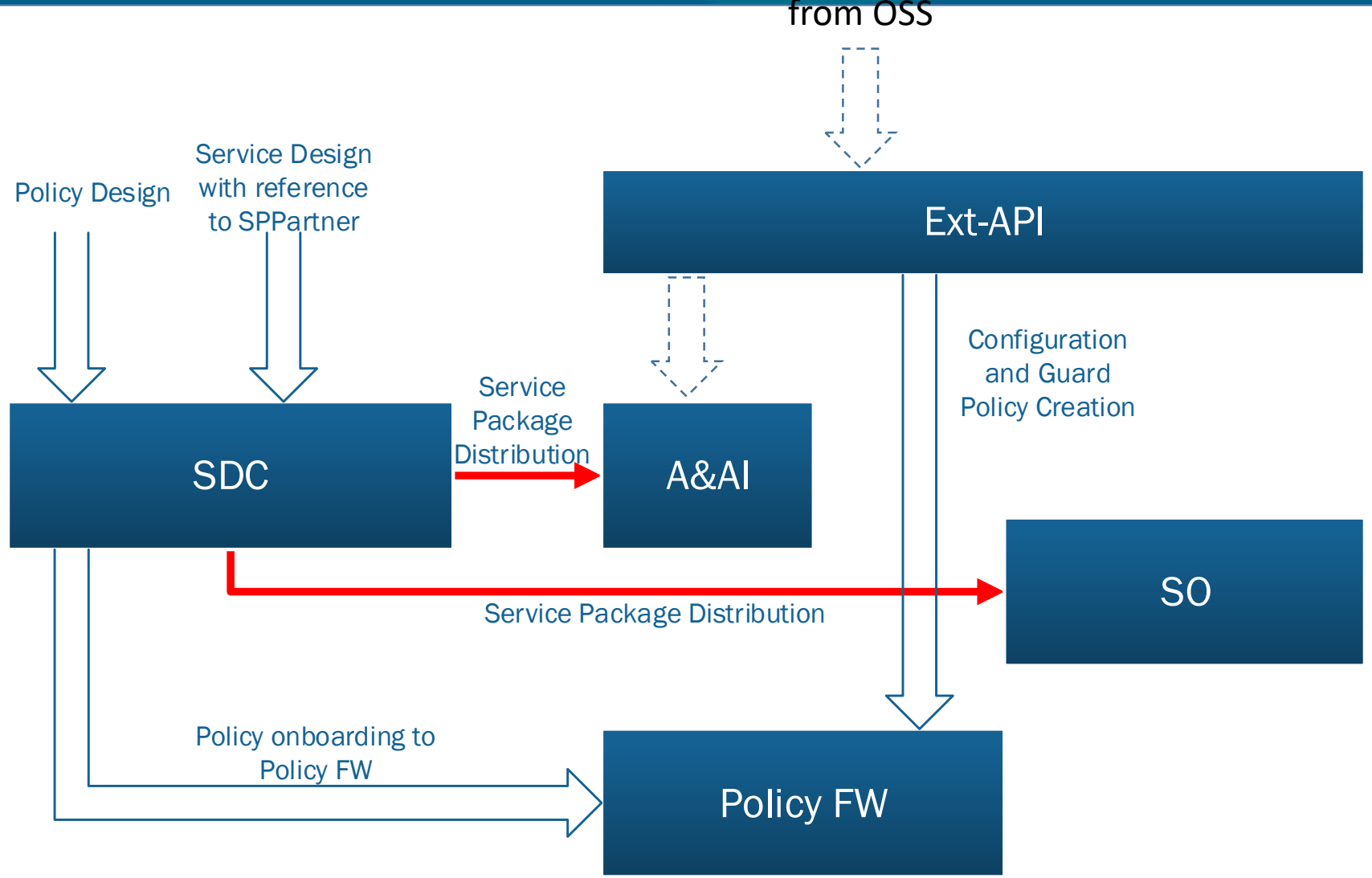
Service Onboarding and Instantiation



Alternate Flow



Onboarding Process



Same for SP and Partner ONAP Instances

Current Method of Representing Partner in ONAP (CCVPN Use Case)

2.2 SOTN VPN Infra Service

Derived from Service

Attributes	Required	Cardinality	Content	Description
sotnConnectivity	M	1	SOTN Connectivity	References the descriptor of the SOTN connectivity
spPartner	O	1	SPPartner	The service provider partner reference

2.3 SDWAN VPN Infra Service

Derived from Service

Attributes	Required	Cardinality	Content	Description
sdwanConnectivity	M	1	SDWAN Connectivity	References the descriptor of the SDWAN Connectivity.
internetCloudAccess	M	1	Internet Cloud Access	References the descriptor of the internet cloud access.
spPartner	O	1	SPPartner	The service provider partner reference

3.9 SPPartner

Attributes	Required	Cardinality	Content	Description
id	M	1	String	Identifier of the SPPartner
url	M	1	String	The url of the ONAP from SPPartner
providingServiceInvarianteUuid	M	1	String	The providing service invariant uuid from SPPartner
providingServiceUuid	M	1	String	The providing service uuid from SPPartner
handoverMode	M	1	String	The handover mode for the cross ONAP. It can be SOTN/SD-WAN

SPPartner with additional attributes are stored in A&AI by SO based on the Service ID received from Partner Ext-API

Edge rule in A&AI map SPPartner to Service Id of Partner

```
{
        "from": "sp-partner",
        "to": "service-instance",
        "label": "org.onap.relationships.inventory.PartOf",
        "direction": "OUT",
        "multiplicity": "ONE2MANY",
        "contains-other-v": "NONE",
        "delete-other-v": "NONE",
        "prevent-delete": "NONE",
        "default": "true",
        "description":"For CCVPN Usecase"
}
```