PHOSPHORUS

Phosphorus Project

Lambda User Controlled Infrastructure For European Research

HARMONY SYSTEM OVERVIEW

Michel Savoie – Communications Research Centre Canada

(michel.savoie@crc.ca)

Seattle, WA, USA, October 1, 2008

Outline

- **Introduction**
- **Harmony architecture**
- **Harmony AAI**
  - **Authentication (AuthN)**
  - **Authorization (AuthZ)**
- **Harmony service interface**
- **Harmony interoperability**

Phosphorus project

What: 6th FP project in the area "*Research networking test-beds*"
5.1 M€ ($7.2M) EC contribution, 6.9 M€ ($9.7M) budget
20 partners, 814 Person Months

When: 1st October 2006 – 30th March 2009 (30 months)

More: **http://www.ist-phosphorus.eu**

Project Vision and Mission

- The project addresses some of the key technical challenges in enabling on-demand e2e network services across multiple, heterogeneous domains
- Phosphorus has demonstrated solutions and functionalities across a test-bed involving European NRENs, GÉANT2, Cross Border Dark Fibre and GLIF

Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

i2cat

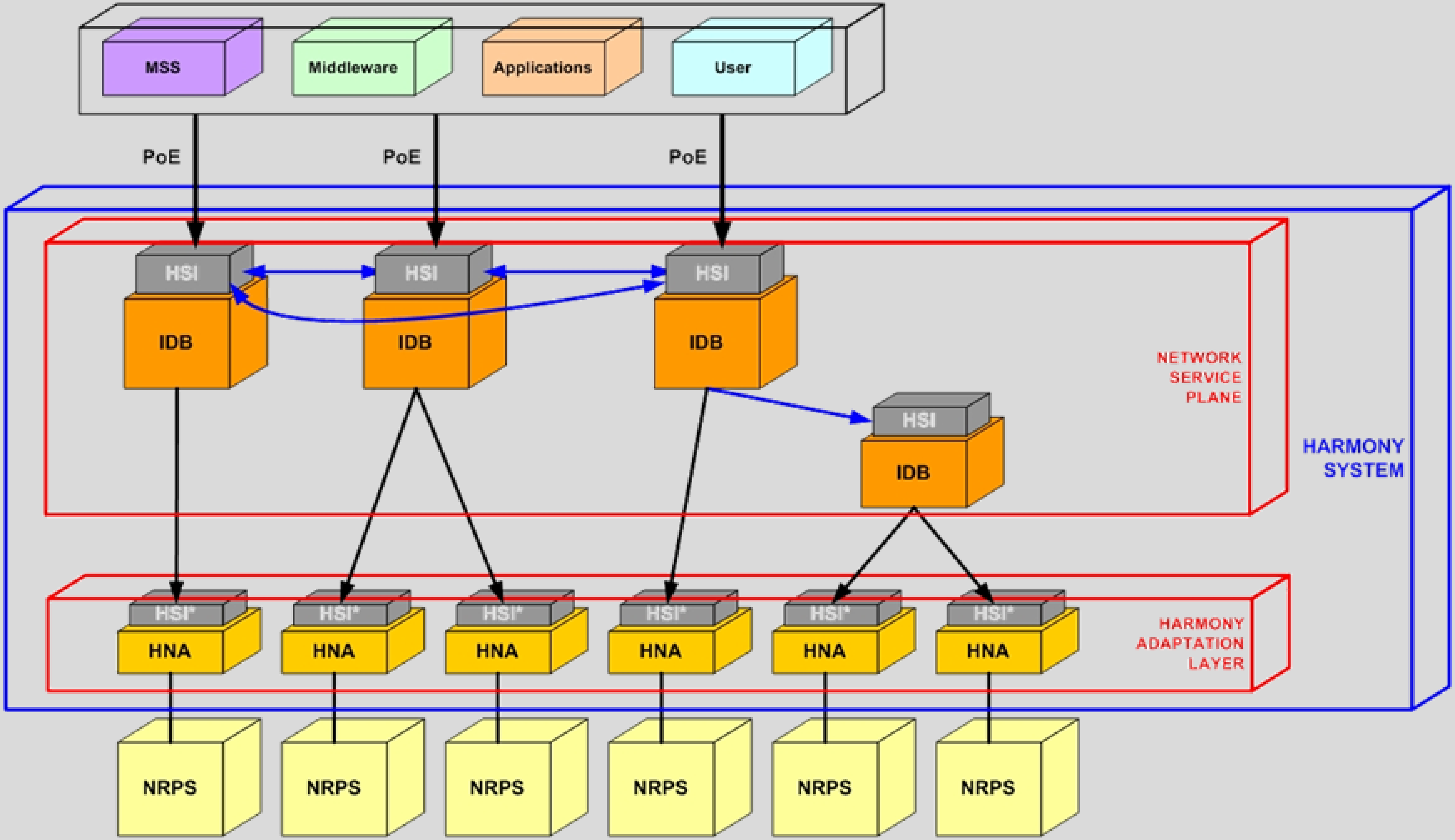
Harmony system

- WP1 system was presented at the OGF23 (Barcelona, May 2008) as **Harmony** system (new branding name)
- What is Harmony?
  - It is an inter/multi-domain path provisioning architecture/system where both Users and Grid applications can book in advance paths and network resources over heterogeneous domains
- Which objective?
  - The objective is to enable users and applications to make dynamic, adaptive and optimized use of heterogeneous network infrastructures connecting various high-end resources

Outline

- Introduction
- Harmony architecture
- Harmony AAI
  - Authentication (AuthN)
  - Authorization (AuthZ)
- Harmony service interface
- Harmony interoperability

Harmony architecture (I)



Legend:

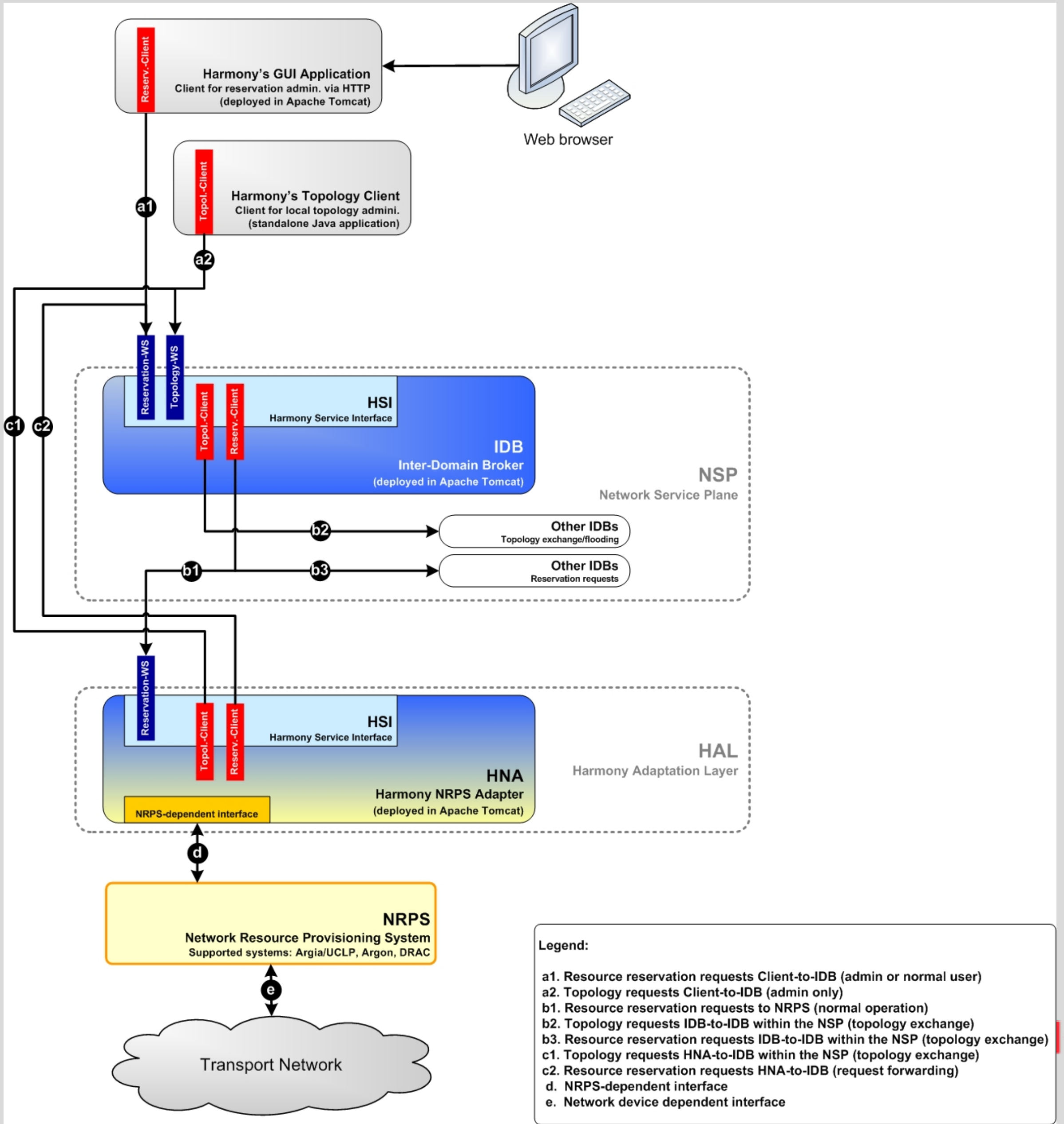
HSI:	Harmony Service Interface
HSI*:	Harmony Service Interface (limited services)
IDB:	Inter-Domain Broker
PoE:	Point of Entry (middleware, administration client)
HNA:	Harmony NRPS Adapter
NSP:	Network Service Plane
NRPS:	Network Resource Provisioning System

Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

i2cat

Harmony architecture (II)


Reserv.-Client
Harmony's GUI Application
Client for reservation admin. via HTTP
(deployed in Apache Tomcat)
Web browser
Topol.-Client
Harmony's Topology Client
Client for local topology admini.
(standalone Java application)
a1
a2
c1
c2
Reservation-WS
Topology-WS
Topol.-Client
Reserv.-Client
HSI
Harmony Service Interface
IDB
Inter-Domain Broker
(deployed in Apache Tomcat)
NSP
Network Service Plane
b2
Other IDBs
Topology exchange/flooding
b1
b3
Other IDBs
Reservation requests
Reservation-WS
Topol.-Client
Reserv.-Client
HSI
Harmony Service Interface
HNA
Harmony NRPS Adapter
(deployed in Apache Tomcat)
NRPS-dependent interface
HAL
Harmony Adaptation Layer
d
NRPS
Network Resource Provisioning System
Supported systems: Argia/UCLP, Argon, DRAC
e
Transport Network

Legend:

a1. Resource reservation requests Client-to-IDB (admin or normal user)
a2. Topology requests Client-to-IDB (admin only)
b1. Resource reservation requests to NRPS (normal operation)
b2. Topology requests IDB-to-IDB within the NSP (topology exchange)
b3. Resource reservation requests IDB-to-IDB within the NSP (topology exchange)
c1. Topology requests HNA-to-IDB within the NSP (topology exchange)
c2. Resource reservation requests HNA-to-IDB (request forwarding)
d. NRPS-dependent interface
e. Network device dependent interface

Key points:

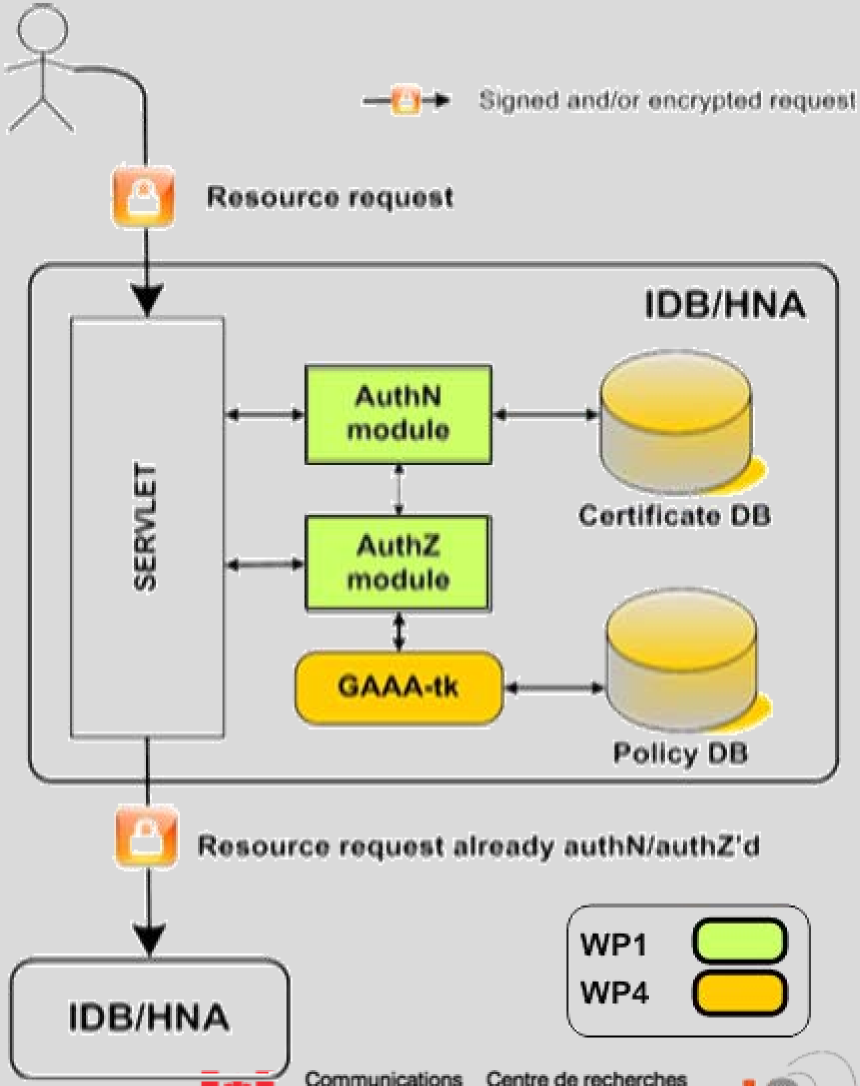
- Distributed (P2P) or hierarchical architecture for the Network Service Plane
- The Network Service Plane is composed of independent entities (Inter Domain Brokers)
- The distinct IDBs flood the information of each domain they control
- Harmony Service Interface is common to the adaptation layer and the network service plane
- The new P2P architecture is being tested over the new virtual testbed

Outline

- Introduction
- Harmony architecture
- Harmony AAI
  - Authentication (AuthN)
  - Authorization (AuthZ)
- Harmony service interface
- Harmony interoperability

Harmony AAI – Overview

- The Harmony System implements an Authentication (AuthN) and Authorization (AuthZ) Infrastructure based on the Generalized AAA Toolkit [1].
- AuthN
  - Based on user certificate + user signature.
  - PKI-based, using certificate X.509.
  - Signature is exchanged using SAML assertions among entities.
  - Signature added as part of the SOAP header in the service request message.
- AuthZ
  - Access control based on XACML obligations using local policy databases.
  - Implemented using GAAA-Toolkit (ver. 0.5).
  - Session is held by exchanging tokens among entities (token := GRI, value, validity)



[1] http://staff.science.uva.nl/~demch/projects/aaauthreach

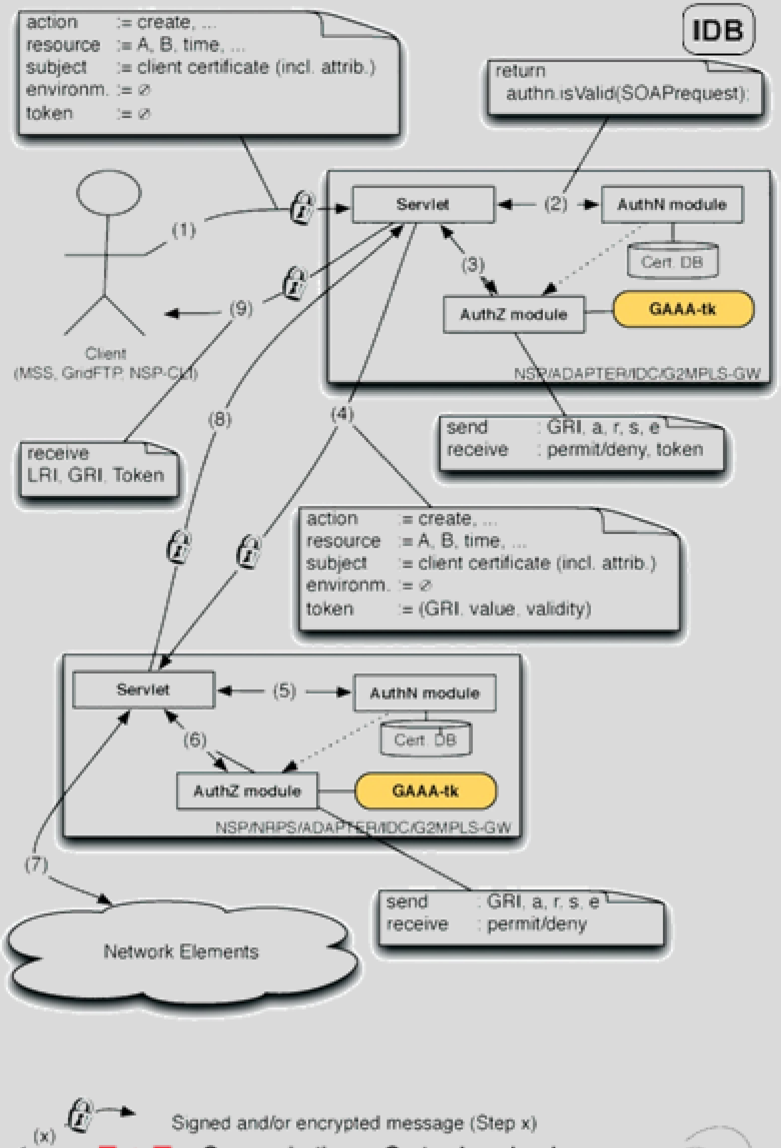
Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

i2cat

Harmony AAI – In detail

- AuthN module
  - SAML assertion (containing signature, credentials) in the request header is checked by the AuthN module.
  - AuthN module verifies the signature and gets the user credentials.
  - SAML assertion includes **resourceID**, **action** and **subject map**.
- AuthZ module
  - Resource/Policy database contains the suitable XACML policies.
    - *Resource example (for Harmony: HNA URI): http://testbed.ist-phosphorus.eu/viola/harmony*
  - Policy DB defines the permissions for each user profile over a given resource.
  - Token maintains the session context along the architecture using a GRI plus a value and a validity.



```
action      := create, ...
resource    := A, B, time, ...
subject     := client certificate (incl. attrib.)
environm.   := ∅
token       := ∅
```

```
return
authn.isValid(SOAPrequest);
```

```
send     : GRI, a, r, s, e
receive  : permit/deny, token
```

```
receive
LRI, GRI, Token
```

```
action      := create, ...
resource    := A, B, time, ...
subject     := client certificate (incl. attrib.)
environm.   := ∅
token       := (GRI, value, validity)
```

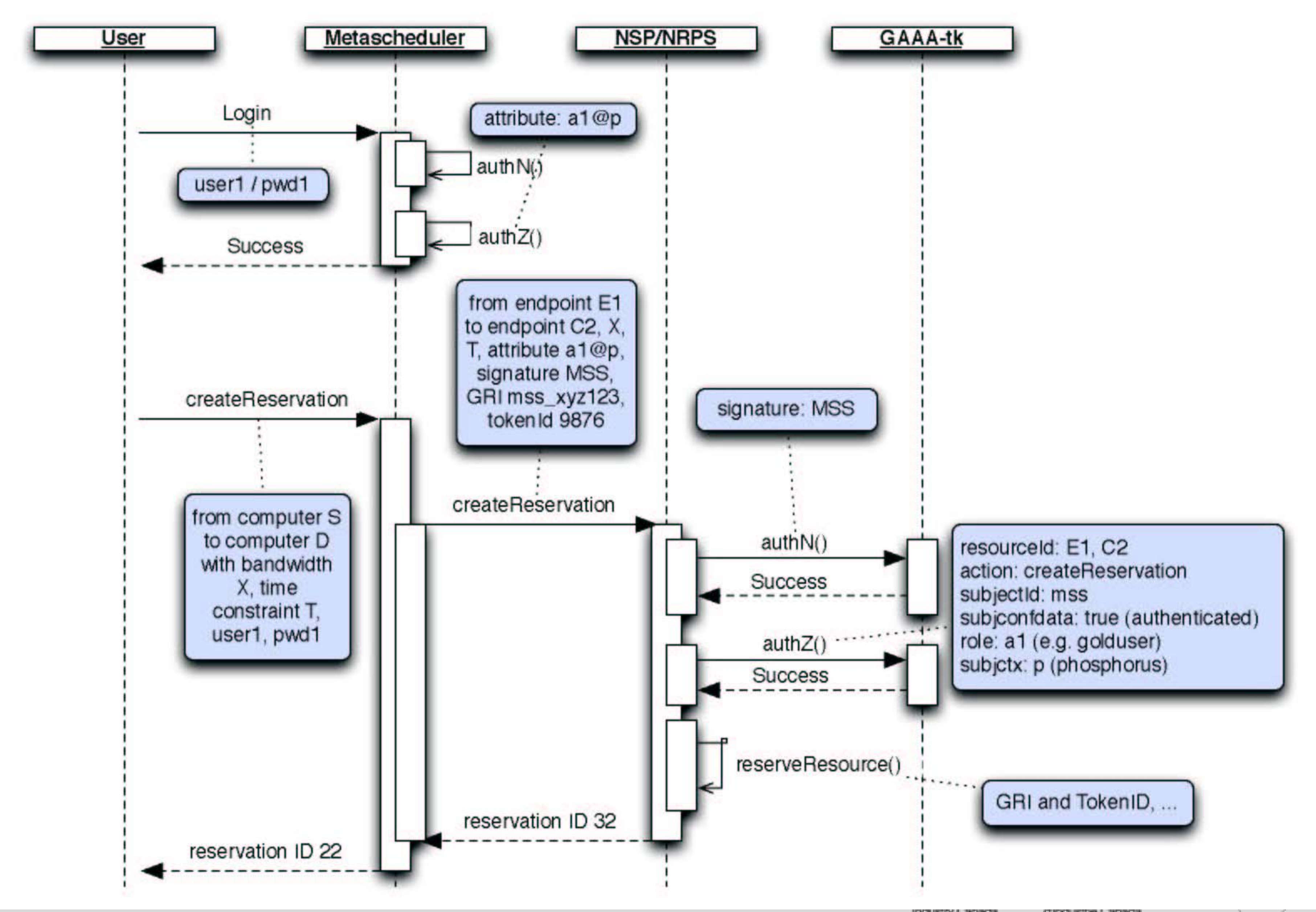
```
send     : GRI, a, r, s, e
receive  : permit/deny
```

Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

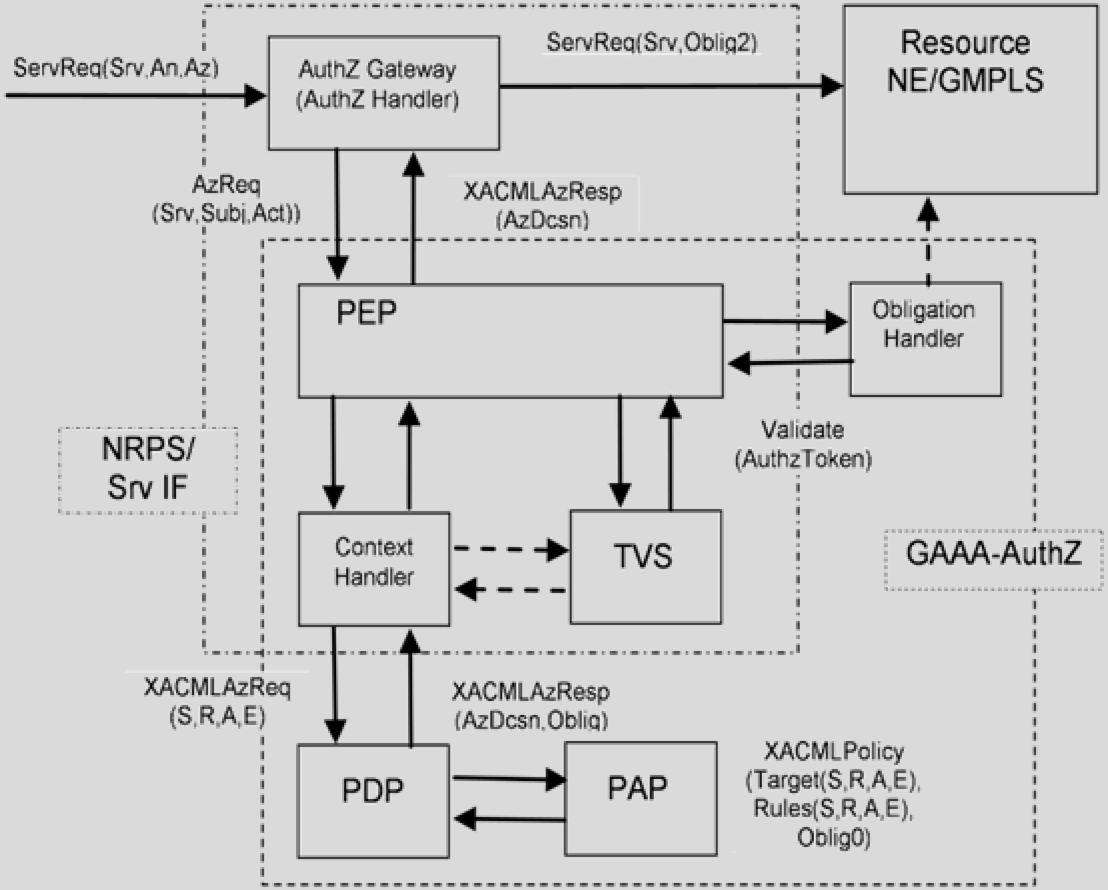
i2cat

Harmony AuthN / AuthZ workflow



Harmony Authorization workflow

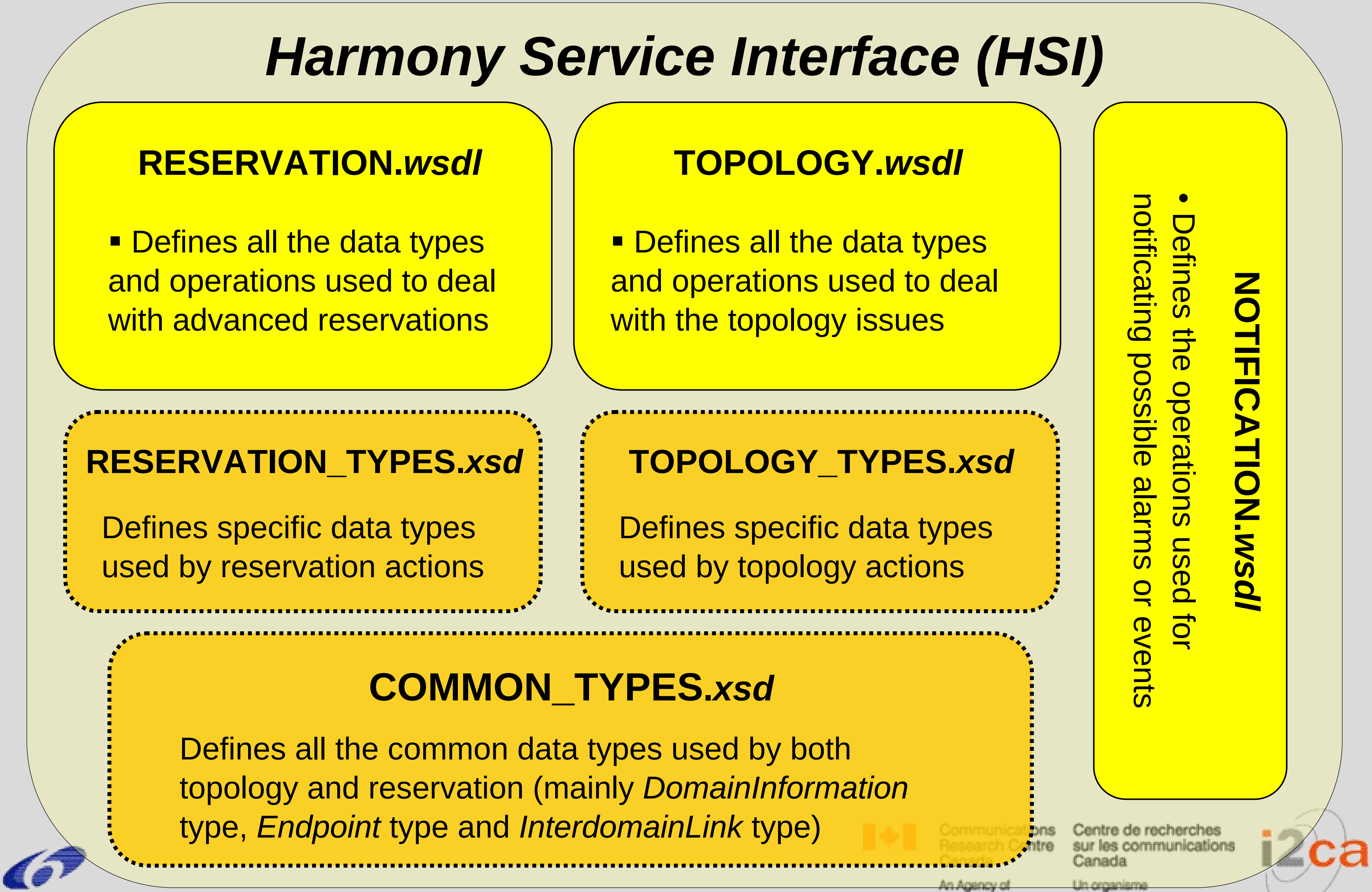
- AuthZ Module (GAAA-TK)
  - PEP gets AuthN parameters and calls the handlers:
    - Context Handler gets the parameters and retrieves the rules from the policies
    - Obligation Handler performs allowed actions over the resource
  - AuthZ ticket/token allow shared sessions for multi-domain environment in the Context handler/TVS (e.g. multiple HNA)
  - TVS performs the validation of a given token.
  - PDP checks the XACML rules from the policies for the desired resources.



Outline

- Introduction
- Harmony architecture
- Harmony AAI
  - Authentication (AuthN)
  - Authorization (AuthZ)
- **Harmony service interface**
- Harmony interoperability

Harmony Service Interface - HSI



Harmony Service Interface (HSI)

RESERVATION.*wsdl*

- Defines all the data types and operations used to deal with advanced reservations

TOPOLOGY.*wsdl*

- Defines all the data types and operations used to deal with the topology issues

NOTIFICATION.*wsdl*

- Defines the operations used for notificating possible alarms or events

RESERVATION_TYPES.*xsd*

Defines specific data types used by reservation actions

TOPOLOGY_TYPES.*xsd*

Defines specific data types used by topology actions

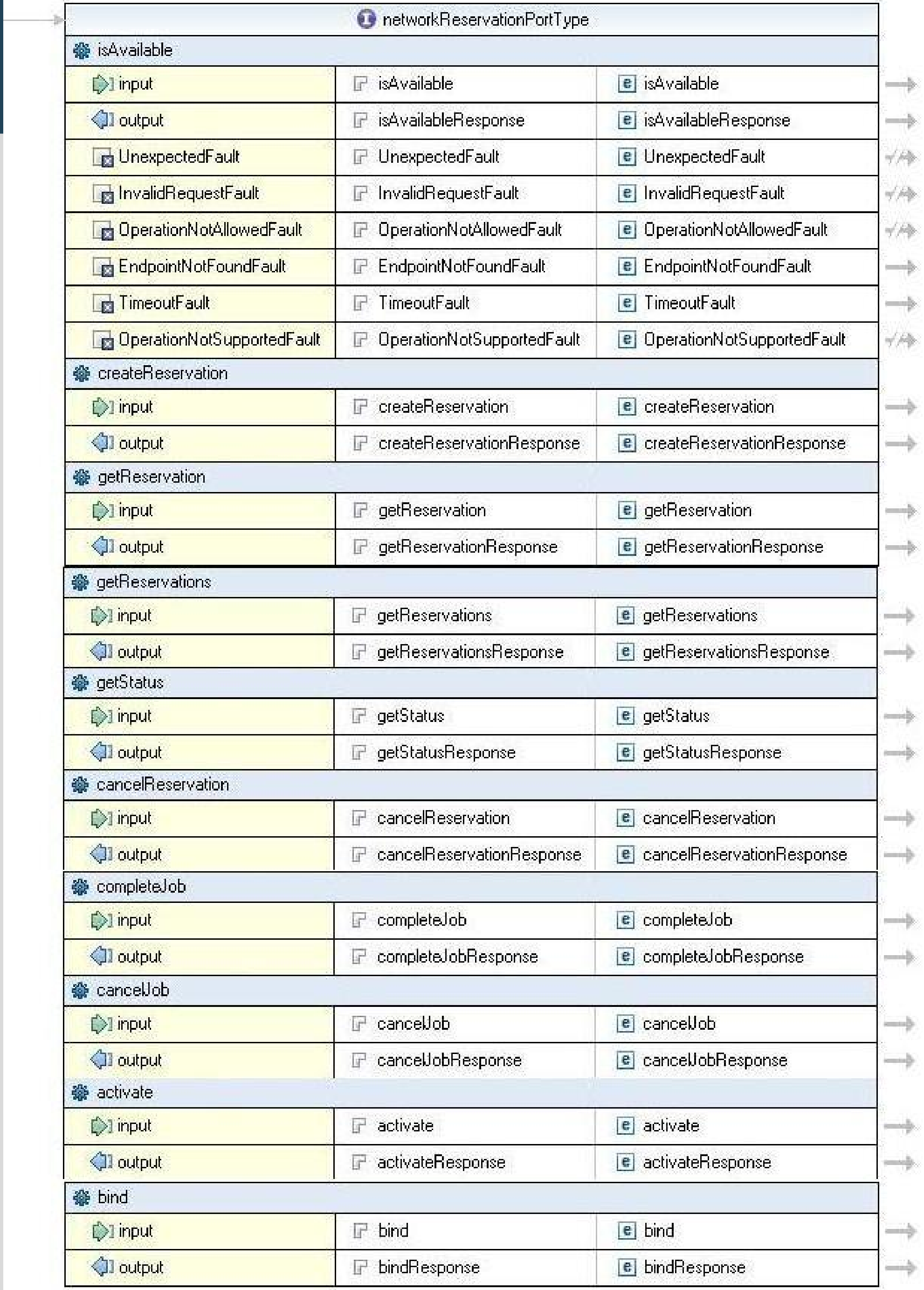
COMMON_TYPES.*xsd*

Defines all the common data types used by both topology and reservation (mainly *DomainInformation* type, *Endpoint* type and *InterdomainLink* type)

HSI – Reservation Service

Key points:

- *isAvailable*
- *createReservation*: Service Info (ID, typeReservation, Connections..), jobID, Notification URL consumer
- *getReservation:* ReservationID, ServiceID
- *getReservations:* Start time, end time
- *getStatus:* ReservationID, array servicesID
- *cancelReservation:* ReservationID
- *completeJob (currently not used)*
- *cancelJob (currently not used)*
- *activate*
- *bind*



networkReservationPortType

isAvailable		
input	isAvailable	isAvailable
output	isAvailableResponse	isAvailableResponse
UnexpectedFault	UnexpectedFault	UnexpectedFault
InvalidRequestFault	InvalidRequestFault	InvalidRequestFault
OperationNotAllowedFault	OperationNotAllowedFault	OperationNotAllowedFault
EndpointNotFoundFault	EndpointNotFoundFault	EndpointNotFoundFault
TimeoutFault	TimeoutFault	TimeoutFault
OperationNotSupportedFault	OperationNotSupportedFault	OperationNotSupportedFault
createReservation		
input	createReservation	createReservation
output	createReservationResponse	createReservationResponse
getReservation		
input	getReservation	getReservation
output	getReservationResponse	getReservationResponse
getReservations		
input	getReservations	getReservations
output	getReservationsResponse	getReservationsResponse
getStatus		
input	getStatus	getStatus
output	getStatusResponse	getStatusResponse
cancelReservation		
input	cancelReservation	cancelReservation
output	cancelReservationResponse	cancelReservationResponse
completeJob		
input	completeJob	completeJob
output	completeJobResponse	completeJobResponse
cancelJob		
input	cancelJob	cancelJob
output	cancelJobResponse	cancelJobResponse
activate		
input	activate	activate
output	activateResponse	activateResponse
bind		
input	bind	bind
output	bindResponse	bindResponse

HSI – Topology Service

Key points:

- *addOrEditDomain*
- *add/delete/edit/get Domain(s):*

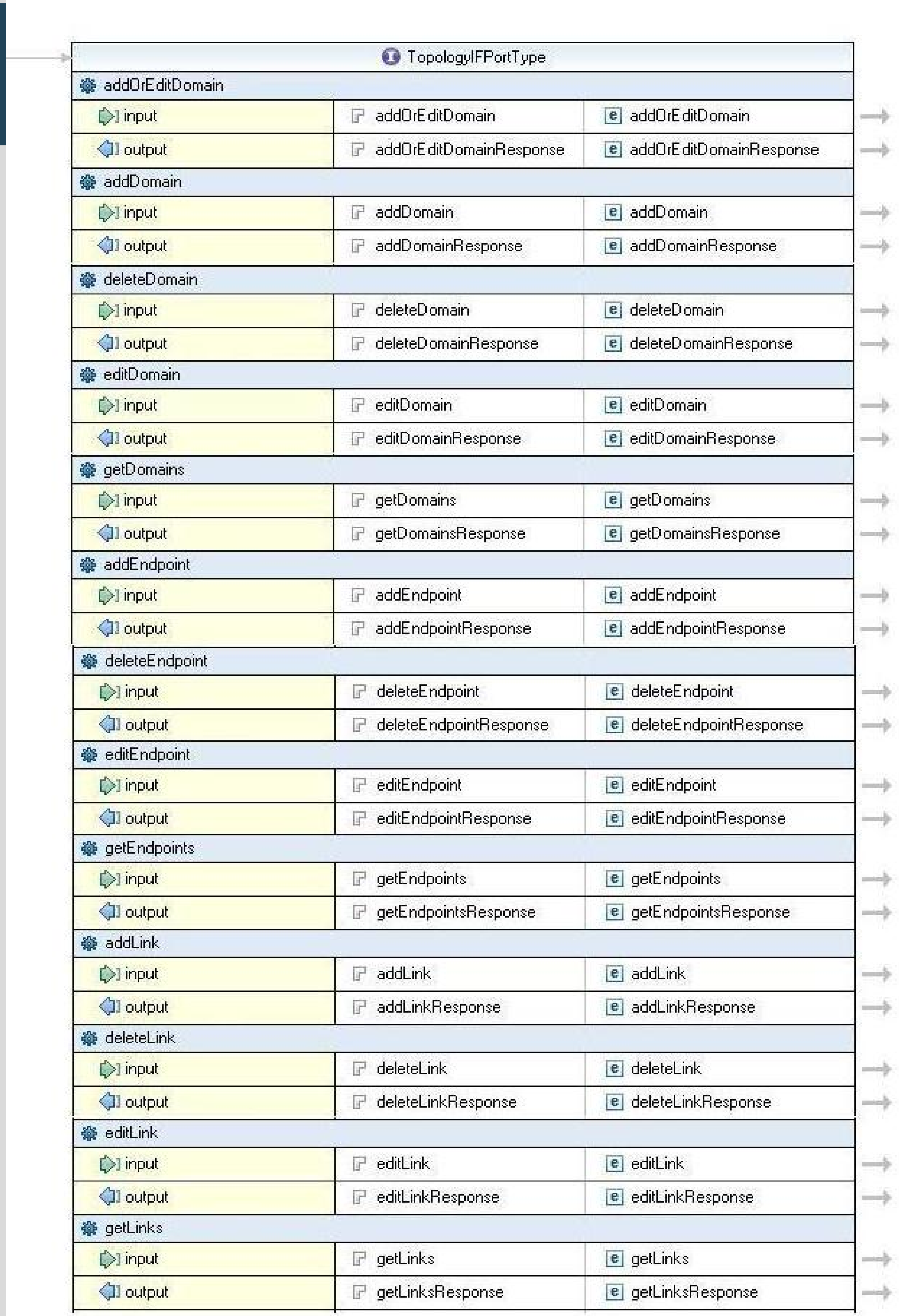
  Identifier, Reservation EPR, Relationship, Bw, Description

- *add/delete/edit/get Endpoint(s)*

  Identifier, Name, Description, Interface, DomainID, Bw

- *add/delete/edit/get Link(s)*

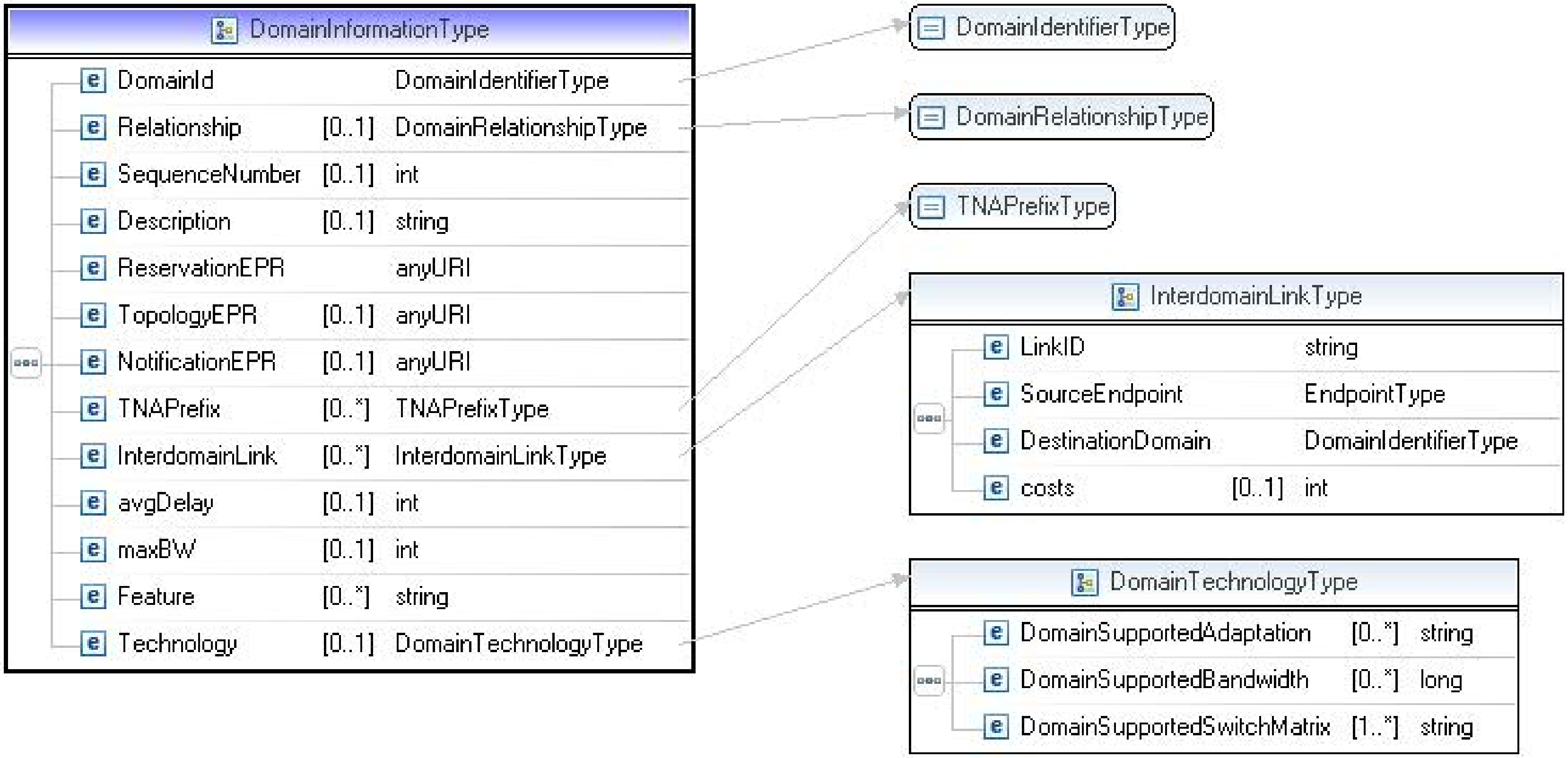
  Identifier, Source Endpoint, DomainID, Costs



TopologyIFPortType		
addOrEditDomain		
input	addOrEditDomain	addOrEditDomain
output	addOrEditDomainResponse	addOrEditDomainResponse
addDomain		
input	addDomain	addDomain
output	addDomainResponse	addDomainResponse
deleteDomain		
input	deleteDomain	deleteDomain
output	deleteDomainResponse	deleteDomainResponse
editDomain		
input	editDomain	editDomain
output	editDomainResponse	editDomainResponse
getDomains		
input	getDomains	getDomains
output	getDomainsResponse	getDomainsResponse
addEndpoint		
input	addEndpoint	addEndpoint
output	addEndpointResponse	addEndpointResponse
deleteEndpoint		
input	deleteEndpoint	deleteEndpoint
output	deleteEndpointResponse	deleteEndpointResponse
editEndpoint		
input	editEndpoint	editEndpoint
output	editEndpointResponse	editEndpointResponse
getEndpoints		
input	getEndpoints	getEndpoints
output	getEndpointsResponse	getEndpointsResponse
addLink		
input	addLink	addLink
output	addLinkResponse	addLinkResponse
deleteLink		
input	deleteLink	deleteLink
output	deleteLinkResponse	deleteLinkResponse
editLink		
input	editLink	editLink
output	editLinkResponse	editLinkResponse
getLinks		
input	getLinks	getLinks
output	getLinksResponse	getLinksResponse

HSI – Common data types (I)

Domain Information type



DomainInformationType

DomainId		DomainIdentifierType
Relationship	[0..1]	DomainRelationshipType
SequenceNumber	[0..1]	int
Description	[0..1]	string
ReservationEPR		anyURI
TopologyEPR	[0..1]	anyURI
NotificationEPR	[0..1]	anyURI
TNAPrefix	[0..*]	TNAPrefixType
InterdomainLink	[0..*]	InterdomainLinkType
avgDelay	[0..1]	int
maxBW	[0..1]	int
Feature	[0..*]	string
Technology	[0..1]	DomainTechnologyType

DomainIdentifierType

DomainRelationshipType

TNAPrefixType

InterdomainLinkType

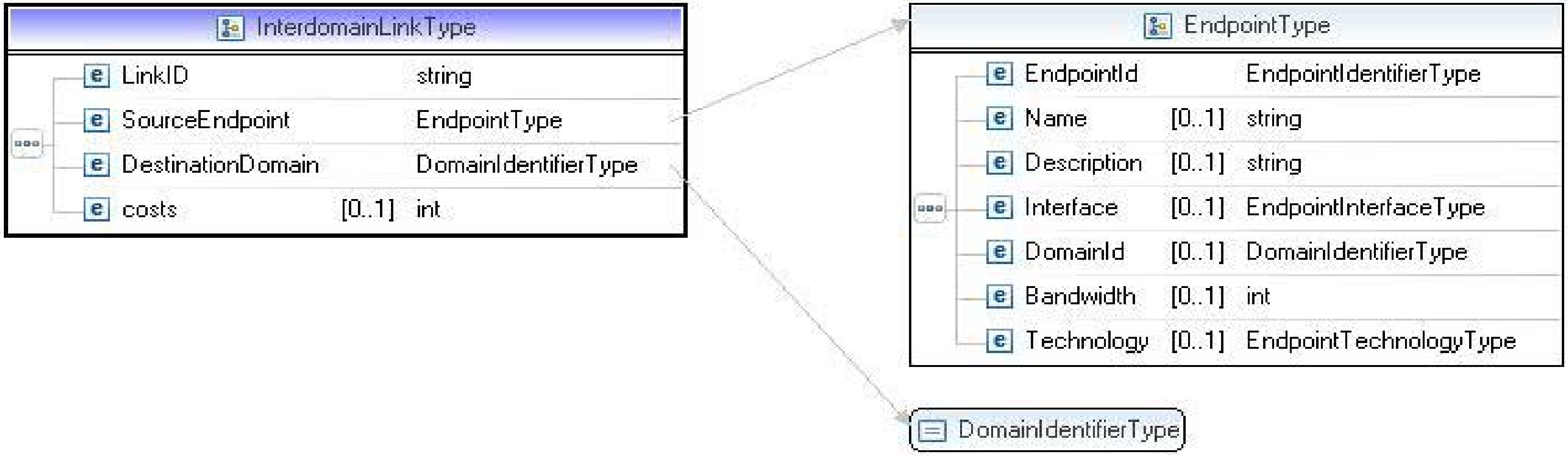
LinkID		string
SourceEndpoint		EndpointType
DestinationDomain		DomainIdentifierType
costs	[0..1]	int

DomainTechnologyType

DomainSupportedAdaptation	[0..*]	string
DomainSupportedBandwidth	[0..*]	long
DomainSupportedSwitchMatrix	[1..*]	string

HSI – Common data types (II)

Interdomain Link type



InterdomainLinkType

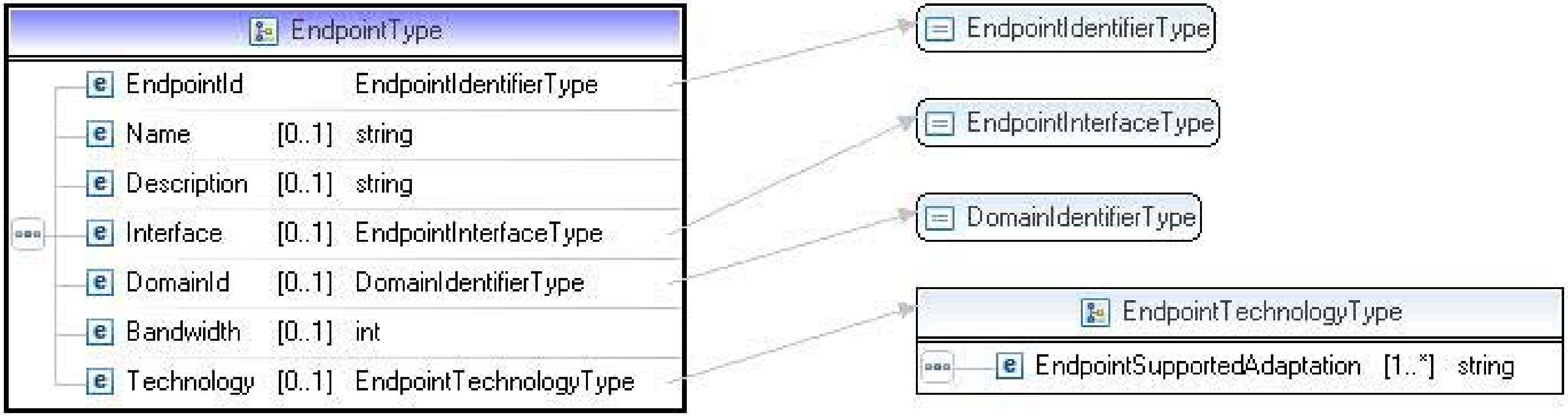
LinkID		string
SourceEndpoint		EndpointType
DestinationDomain		DomainIdentifierType
costs	[0..1]	int

EndpointType

EndpointId		EndpointIdentifierType
Name	[0..1]	string
Description	[0..1]	string
Interface	[0..1]	EndpointInterfaceType
DomainId	[0..1]	DomainIdentifierType
Bandwidth	[0..1]	int
Technology	[0..1]	EndpointTechnologyType

DomainIdentifierType

Endpoint type



EndpointType

EndpointId		EndpointIdentifierType
Name	[0..1]	string
Description	[0..1]	string
Interface	[0..1]	EndpointInterfaceType
DomainId	[0..1]	DomainIdentifierType
Bandwidth	[0..1]	int
Technology	[0..1]	EndpointTechnologyType

EndpointIdentifierType

EndpointInterfaceType

DomainIdentifierType

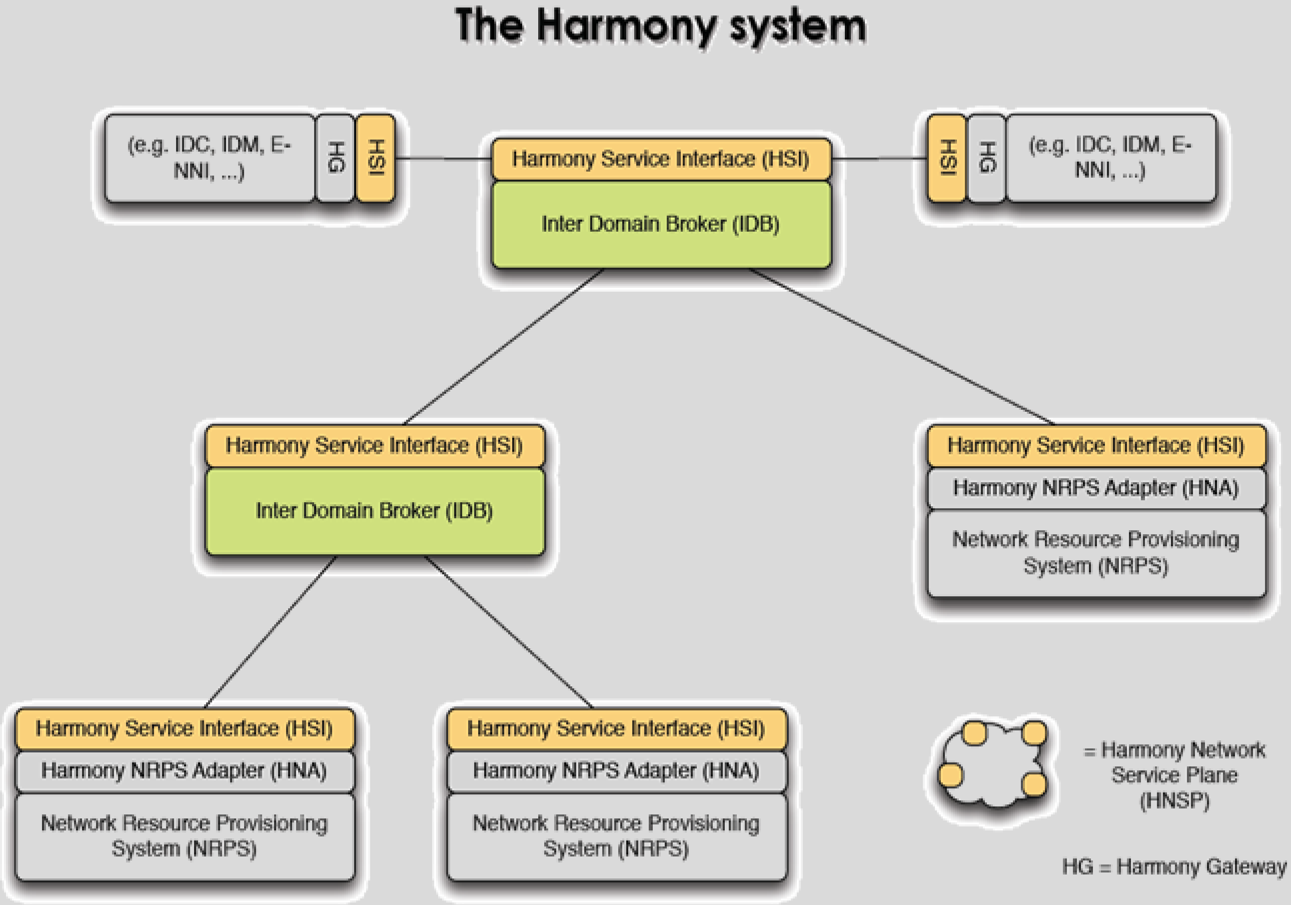
EndpointTechnologyType

EndpointSupportedAdaptation	[1..*]	string

Outline

- Introduction
- Harmony architecture
- Harmony AAI
  - Authentication (AuthN)
  - Authorization (AuthZ)
- Harmony service interface
- **Harmony interoperability**

Harmony System Collaborations


The Harmony system
(e.g. IDC, IDM, E-NNI, ...)
HG
HSI
Harmony Service Interface (HSI)
Inter Domain Broker (IDB)
HSI
HG
(e.g. IDC, IDM, E-NNI, ...)
Harmony Service Interface (HSI)
Inter Domain Broker (IDB)
Harmony Service Interface (HSI)
Harmony NRPS Adapter (HNA)
Network Resource Provisioning System (NRPS)
Harmony Service Interface (HSI)
Harmony NRPS Adapter (HNA)
Network Resource Provisioning System (NRPS)
Harmony Service Interface (HSI)
Harmony NRPS Adapter (HNA)
Network Resource Provisioning System (NRPS)
= Harmony Network Service Plane (HNSP)
HG = Harmony Gateway

Key points:

- For any integration it is necessary to build an Harmony Gateway, with the HSI on the one hand, and the interface of the other system in the other hand
- This HG translates the requests in one system-language to the other system-language, making communication possible between the two different systems.

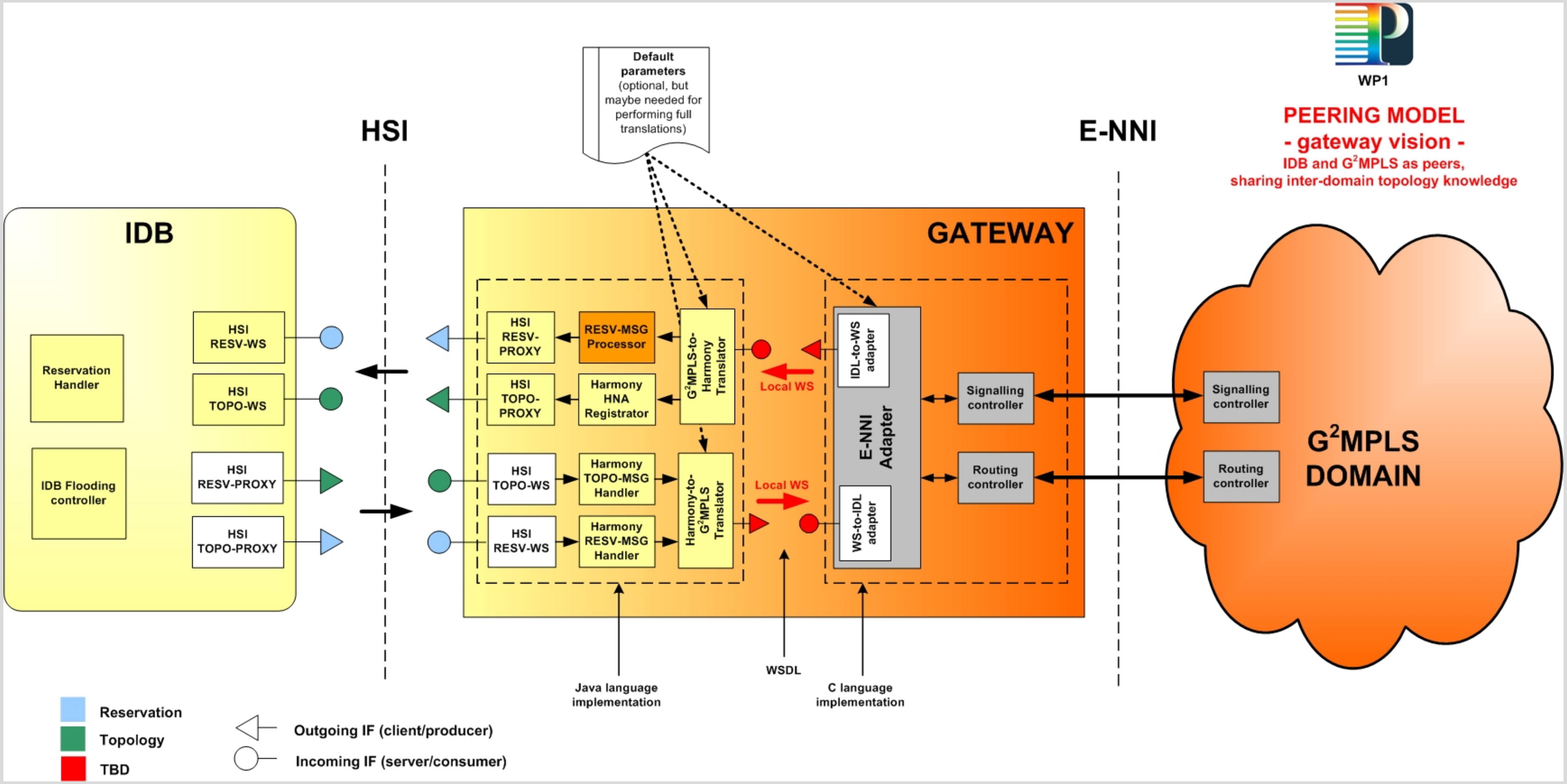
- *The HSI code has been refactorized in order to achieve higher modularization in the architecture for easy integration with other systems.*

Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

WP1–WP2 (G^{2}MPLS) Integration

- Work for WP1-WP2 integration started. First draft design:



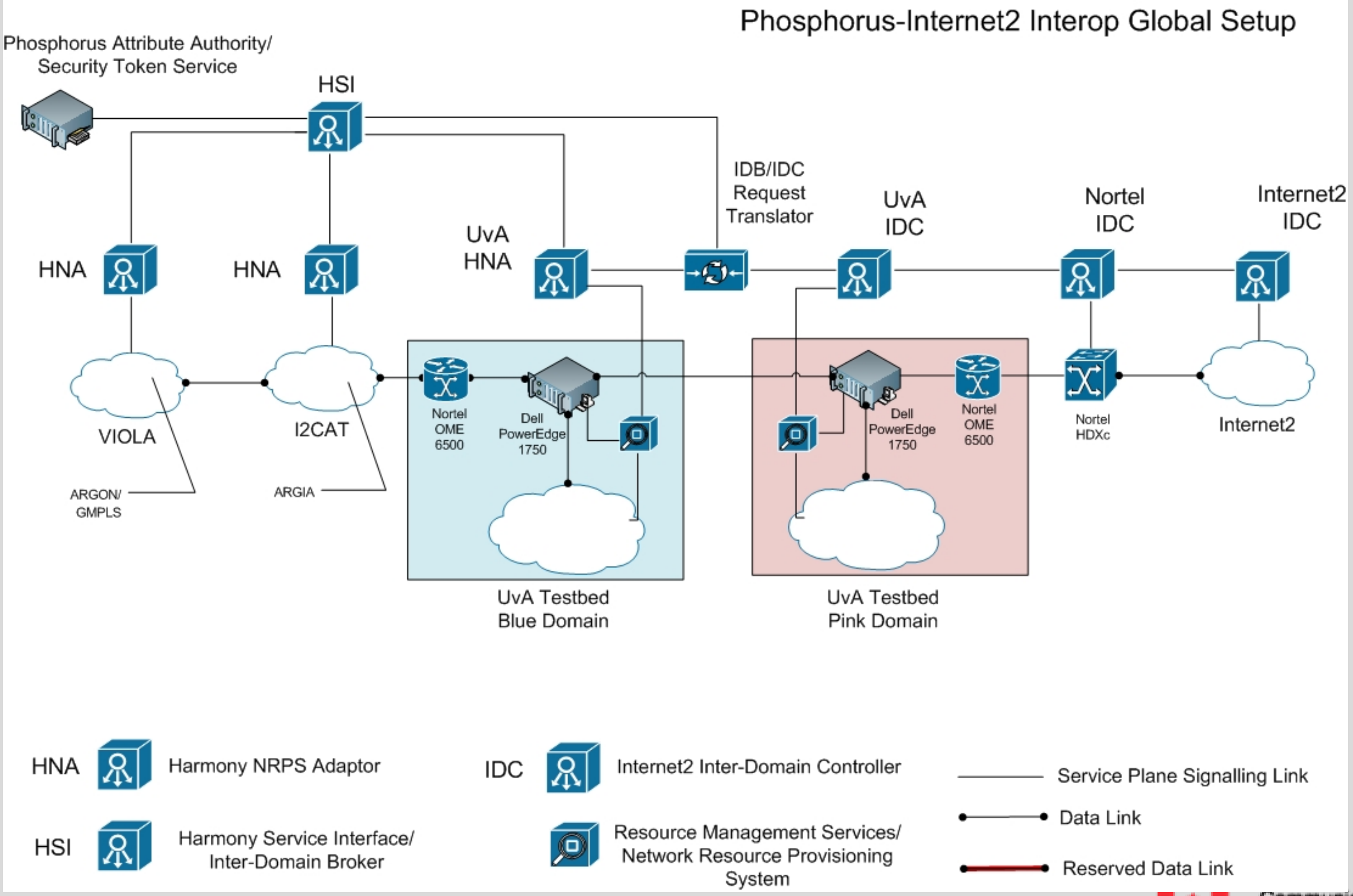
Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

i2cat

Harmony–Internet2 Collaboration

- Setting up a testbed for Internet2-Phosphorus interoperability demos using Harmony



Phosphorus-Internet2 Interop Global Setup
Phosphorus Attribute Authority/ Security Token Service
HSI
IDB/IDC Request Translator
UvA IDC
Nortel IDC
Internet2 IDC
HNA
HNA
UvA HNA
VIOLA
I2CAT
ARGON/ GMPLS
ARGIA
Nortel OME 6500
Dell PowerEdge 1750
Dell PowerEdge 1750
Nortel OME 6500
Nortel HDXc
Internet2
UvA Testbed Blue Domain
UvA Testbed Pink Domain
HNA
Harmony NRPS Adaptor
HSI
Harmony Service Interface/ Inter-Domain Broker
IDC
Internet2 Inter-Domain Controller
Resource Management Services/ Network Resource Provisioning System
Service Plane Signalling Link
Data Link
Reserved Data Link

- New VLAN between i2CAT and UvA provisioned by Netherlight.
- Implemented Harmony-IDC translators.

Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

i2cat

Next goals

Collaborations:

- Interoperability with G^{2}MPLS and Internet2
- Basic interoperability with GÉANT2 JRA3's AutoBAHN and other related projects (G-Lambda?, enLIGHTened?)
- Common interoperability methods definition with those projects
- New collaboration lines: CARRIOCAS and KISTI.

Development:

- Fully working peer-to-peer NSP (M24)
- Operative security infrastructure in the NSP (M24)
- Multi technology support and bandwidth management at the NSP level (M24)
- Operational gateway/translators to G^{2}MPLS, Internet2 and AutoBAHN (M30)

Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

i2cat

Sergi Figuerola – i2CAT Foundation

Barcelona, Catalonia

(sergi.figuerola@i2cat.net)

Communications Research Centre Canada

An Agency of Industry Canada

Centre de recherches sur les communications Canada

Un organisme d'Industrie Canada

i2cat

Thank you

Michel Savoie

Communications Research Centre Canada

Ottawa, Canada

(michel.savoie@crc.ca)