DOCUMENT

IOAG

Interoperability Demonstrator Report

prepared by/*préparé par*	Interoperability demonstrator participating agencies: NASA, ESA, CNES
issue/*édition*	Initial Release
revision/*revision*	1
date of issue/*date d'édition*	03/14/2023
status/*état*	Public release
Distribution/*distribution*	IOAG

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Scope

This document synthesis the main activities and findings raised for both scenarios of the Interagency Operations Advisory Group (IOAG) interoperability demonstrator.

1.2 Reference Documents

[MO_COM]	CCSDS 521.1-B-1 Mission Operations Common Object Model. Blue Book.
[MO_MC]	CCSDS 522.1-B-1 Mission Operations Monitor & Control Services. Blue Book.
[ODM]	CCSDS 502.0-B-2 Orbit Data Messages. Blue Book.
[XTCE]	CCSDS 660.0-B-1 XML Telemetric and Command Exchange. Blue Book

1.3 Acronyms

CCC	Control Command Center
CCSDS	Consultative Committee for Space Data Systems
COM	Common Object Model
EDDS	EGOS Data Dissemination System
EGOS	ESA Ground Operation System
ESA	European Space Agency
ESOC	European Space Operations Centre
HTTP	Hypertext Transfer Protocol
IOAG	Interagency Operations Advisory Group
IOP	Inter-Operability Plenary
IPsec	Internet Protocol security
ISA	Interconnection Security Agreement
ISECG	International Space Exploration Coordination Group
ISIS PL	Initiative for Space Innovative Standard Product Line
IT	Information Technology
ITCOP	Interagency, Tracking, Communications, and Operations Panel
JPL	Jet Propulsion Laboratory
JSON	JavaScript Object Notation
M&C	Monitor and Control
MAL	Message Abstraction Layer
MO	Mission Operations
MOIS	Mission Operations Interoperability Services
MOSSG	Mission Operations Systems Strategy Group
NASA	National Aeronautics and Space Administration
ODM	Orbit Data Messages

OEM	Orbit Ephemeris Message
SCOS	Satellite Control and Operations System
SFTP	Secure File Transfer Protocol
SSL	Secure Sockets Layer
SWOT	Surface Water and Ocean Topography
VPN	Virtual Private Network
XML	Extensible Mark-up Language
XTCE	XML Telemetric and Command Exchange

2 OVERVIEW

2.1 Background

Interagency interoperability for cross support is needed to realize the additional economies resulting from an ability to share the large capital investments made by each agency in mission support systems. For that purpose, the Inter-Operability Plenary (IOP) was convened in 1999.

The IOP convened as a result of a European Space Agency (ESA) and National Aeronautics and Space Administration (NASA) Interagency, Tracking, Communications, and Operations Panel (ITCOP) meeting in December 1998, where ESA suggested that ESA-NASA interoperability issues might be better dealt with in a multi-agency forum. Six agencies met to agree upon a framework to achieve interoperability.

In 1999, the IOP established an Interagency Operations Advisory Group (IOAG) in order to achieve cross support across the international space community and to expand the enabling levels of space communications and navigation interoperability.

IOP-3 added Mission Operations Functions to the IOAG Charter, resulting in the creation of the Mission Operations Systems Strategy Group (MOSSG) in 2013. At that time, IOAG directed MOSSG to address the following:

1. Interoperability topics between the agencies
2. Assess the potential benefits in the medium and long term
3. Assess whether a simulation is needed to quantify benefits to be gained
4. Develop a Service Catalog of Mission Operations Services (Service Catalog #3) and a study report

Per IOAG direction, MOSSG scope was set to address interoperability between mission operations ground systems not to include space segment-related interfaces. MOSSG was to provide references to related Consultative Committee for Space Data Systems (CCSDS) standards, but not to perform a full assessment of adequacy or conduct a full gap analysis.

The objective of the MOSSG is to make recommendations to foster cooperation and ground system interoperability among our Space Agencies.

The IOAG Service Catalog #3 focuses on short- and medium-term efforts to promote interagency interoperability between ground systems. Very long-term visions of seamless joint operations for complex missions embraced by CCSDS or the International Space Exploration Coordination Group (ISECG) are not precluded and can be addressed as technology, common practices, and the available standards evolve.

2.2 Our Mandate

To promote interoperability infusion, IOAG member agencies proposed three paths:

1. Proof of concept demonstrations influenced by real missions
2. Initial infusion by a small mission
3. Initial infusion into a very large mission (e.g., Artemis)

In the short term, the IOAG encouraged member agencies to establish a demonstration environment in which service interoperability (per Service Catalog #3) can be developed, tested, and demonstrated. The development environment shall be designed to allow easy expansion for use by IOAG working groups, CCSDS, new missions, and agency ground segment teams to prove and demonstrate interoperability implementation options.

This group's mandate was to demonstrate interagency interoperability for a typical multi-agency project's use case and identify the benefits, challenges, and mitigation approaches associated with reusable interagency interoperability approaches for mission operations.

Per IOAG Service Catalog #3 specification, *"…service-based development is one valid approach for implementing interoperability functions. Many missions, however, have utilized a message-format approach to exchange information and use a variety of message delivery alternatives. The use of formats-based approaches may provide a simpler development process and could therefore speed adoption across Agencies…"* Therefore, this effort attempts to apply the IOAG interoperability solutions above by using:

- A representative subset of Catalog #3 services to show both IOAG interoperability approaches (i.e., service-based, format-based) and identify the benefits, challenges, and mitigation approaches associated with each approach.
- Three agencies to demonstrate interoperability
- Each agency's representative mission operations systems and infrastructure
- Each agency's security interfaces for authentication and authorization

2.3 Participating Agencies

Centre National d'Etudes Spatiales (CNES)

- Marc Duhaze (Marc.Duhaze@cnes.fr)
- Olivier Churlaud (Olivier.Churlaud@cnes.fr)

European Space Agency (ESA)

- Sebastian Martin (Sebastian.Martin@esa.int)

•César Coelho (Cesar.Coelho@esa.int)

National Aeronautics and Space Administration (NASA)

•Costin Radulescu (Costin.Radulescu@jpl.nasa.gov)

Funding for each agency's activities is internally provided by each agency.

2.4 Demonstrator Context

The goal of this IOAG interoperability demonstrator activity is to implement in an operational environment, two services of the IOAG Service Catalog #3 showing interoperability between three different agencies: NASA, ESA and CNES.

For this demonstration we chose to exercise two scenarios for which we selected two (2) services from the IOAG Service Catalog #3:

1. Scenario #1 is a *service-based* approach using the real-time parameter service to exercise real-time telemetry data exchange.

2. Scenario #2 is a *format-based* approach using the navigation data exchange service to exchange navigation data files.

A common global software system to promote interoperability is not practical. Interagency boundaries must be established and the proprietary nature of each agency's systems must be respected.

The IOAG MOSSG concluded that an interface gateway approach is the most effective method to implement IOAG Service Catalog #3 services and data exchanges, and also supports the integration of legacy systems.

Interface gateways allow for dissimilar mission operations ground systems to communicate with each other using common data exchanges or services over a common infrastructure.

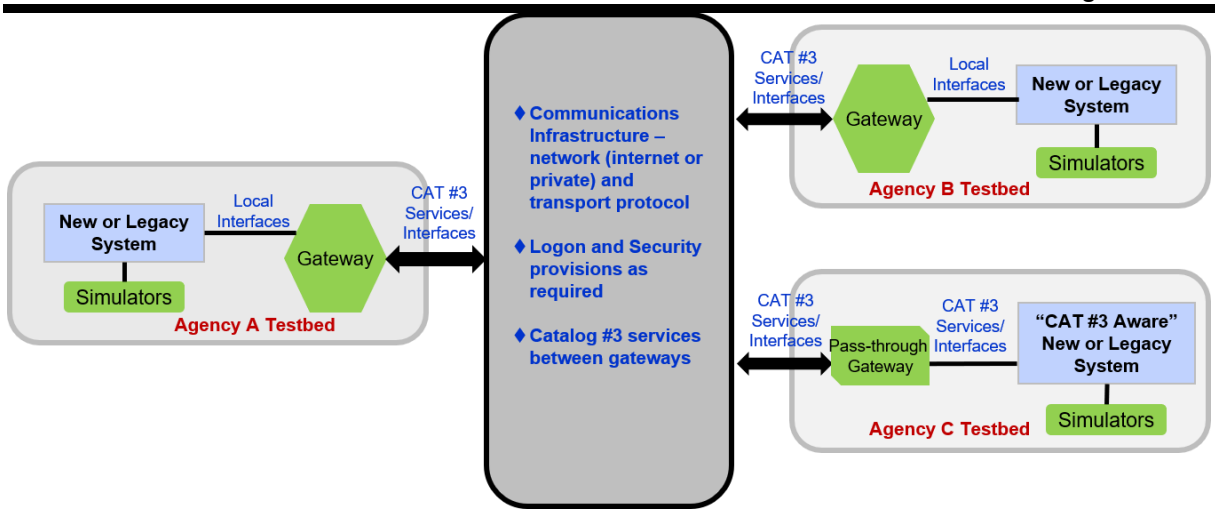

Figure 1 - Interoperability Demonstration Concept

It is critical to define and incorporate common security approaches early since network, applications, and cloud access rules often differ by agency and different data elements may require different security rules.

An interface gateway (front-end processor, edge connector) can also serve as a primary portal between dissimilar systems, supporting interoperable interfaces on one side and legacy interfaces on the other.

It is not realistic to expect that agencies can "start from scratch" and develop interoperable systems. Therefore, interoperability shall account for use of legacy system "adapters," which can be used to match individual components to new format or service standards.

The following interoperability guidelines were considered for this demonstration:

- Support needed for both formats and services to allow development of transformations between the two.
- Use of mnemonics (names) to reference parameters instead of locally generated IDs.
  - Mnemonics are unique across the set of systems.
- Provide descriptive log/event/memo messages when sending across external interfaces (e.g., may include an ID number, flag(s), etc.).
- Minimize storage of one's configuration information on other users' systems.
  - Keeping everything in sync becomes a problem with a big overhead.
  - May need invasive access to each system (e.g., directory update/delete/etc.).

- Assume each agency has its own security approach, which may not be as simple as a unique plug-in.
- Minimize need for cross agency remote database queries and registries (e.g., each partner has an Extensible Mark-up Language [XML] Telemetric and Command Exchange [XTCE] file, and when changes occur within the registry a new XTCE file can be exchanged so that all participating agencies upgrade their systems accordingly).
- Identify the subset of functions applicable across agencies for the primary purpose of interoperability. This may be a small list.
- Separate local system design from the actual use of information (exchange)

Interoperability requires system interactions covering both data exchange and system behavior/processing.

Formats-only standards are easy to implement and provide minimum dependencies in different architectures. Interactions are at least implied, so they must be defined, specified in an interface document, or managed by configuration files or user inputs.

Service standards support the exchange of data with an emphasis on the interaction activity and the types of data exchanged—not necessarily the exact format of the data elements. The services approach initially requires a dedicated development (as opposed to using what already exists: email, sftp, or any pre-existing technology), but has the advantage of including the interaction and utility tool support, which is not possible with a simple format definition.

The IOAG MOSSG recommends that the functional interoperability areas identified in Service Catalog #3 be addressed both by service specification standards and by format specification standards.

2.5 Scenario #1- Real-time Telemetry Data Exchange (Service-based Approach)

Scenario #1 demonstrated real-time exchange of selected parameter values from Agency A to Agencies B and C and vice versa. We used an instantiation of the CCSDS Mission Operation (MO) Parameter Service described in the “Mission Operation Monitoring & Control Services – CCSDS Blue Book 522.1-B-1” [MO_MC].

All three agencies agreed to use the existing CCSDS standards and refrained from inventing any new ad-hoc interfaces. Even though some agencies do not deploy MO-native software internally in their systems, the existing CCSDS data standards can be leveraged to enforce the agreed data exchange between the agencies at their boundaries (e.g., the messages and behavior as specified by the MO Parameter Service and the CCSDS Message Abstraction Layer [MAL] over Hypertext Transfer Protocol [HTTP] and XML-binding).

This approach requires each agency to use a "gateway" to serve as a bridge between MO services and the agency's internal mission operations system to deal with things such as mnemonics, security (authentication and authorization), etc. Domain-related information (e.g., from/to domains) was captured in an Interface Control Document (ICD).

2.6 Scenario #2 - Navigation Data Exchange (Format-based Approach)

The interoperability demonstration team had numerous discussions to define format-based interoperability and how it is strictly different from a service-based approach. Finally, we settled on exercising IOAG Service Catalog #3 Navigation Data Exchange service and sent across CCSDS navigation data formatted messages (this approach also applies to other comparable CCSDS data formats).

The actual "format" is the navigation data message/file, which is structured according to the CCSDS navigation formatted message/files. In this case we exchanged Orbit Ephemeris Message (OEM) files as described in the "Orbit Data Message – CCSDS Blue Book 502.0-B-2." On request of an Agency A, an OEM file generated upon said request is delivered to Agency B and/or Agency C.

There are implicit operations that need to be executed to authenticate, authorize, initiate execution, handle events, and finally terminate the exchange of navigation data (e.g., an instance of a file transfer protocol < Secure File Transfer Protocol (SFTP)>).

The navigation data and the exchange mechanism that define the provider/consumer interfaces need to be documented in an ICD and made available through the gateway to be shared across agencies.

3 IMPLEMENTATION CHOICES

3.1 Usage of a Gateway

We decided to implement the demonstration through gateways since all participants agreed that was the most pragmatic approach.

3.1.1 INTERFACE GATEWAY RATIONALE

The following list outlines some of the benefits associated with a gateway approach:

1. Mission independent
2. Flexible to support various agency-preferred deployments
3. Isolates from legacy systems
4. Reusable and/or adaptable
5. Provides a form of interagency agreements/protocols
6. Design independence from external partners can be maintained
7. Point-to-point configuration using secure pipes (Internet Protocol security [IPsec] tunnels, Virtual Private Networks, etc.) well understood by program managers
8. Easily deployable, known technology, enables use of the Internet
9. Allows for growth (bandwidths, protocols, etc.) to evolve flexibly according to program integration and mission requirements
10. Allows a common bus protocol for communication (e.g., CCSDS Message Abstraction Layer [MAL] implementation)

3.1.2 POTENTIAL BARRIERS TO INFUSION OF INTEROPERABILITY STANDARDS

Potential issue	**Potential solution**
Agencies prefer to use their own proven infrastructure, legacy systems, standards, and applications	An interface gateway isolates existing infrastructure from interoperability impacts

Lack of consistent communications infrastructure creates demands for costly changes within agencies	An interface gateway approach promotes a common communications solution with benefits in the areas of hardware, software, security, and maintenance
Future multilateral exploration missions are not yet sufficiently defined to identify all the needed operational services	1. Start with a subset of the operational services identified in IOAG Service Catalog #3 2. Encourage consideration of mission operations standards and interoperability very early in the mission formulation process
Mission managers require evidence that the technology is ready, proven, and has benefits. The IOAG member agencies must embrace and encourage (enforce) the implementation of interoperability standards	An interface gateway testbed will help mitigate the concern

3.2 Infrastructure

Interface gateways allow for dissimilar mission operations ground systems to communicate using common data exchanges or services over a common infrastructure.

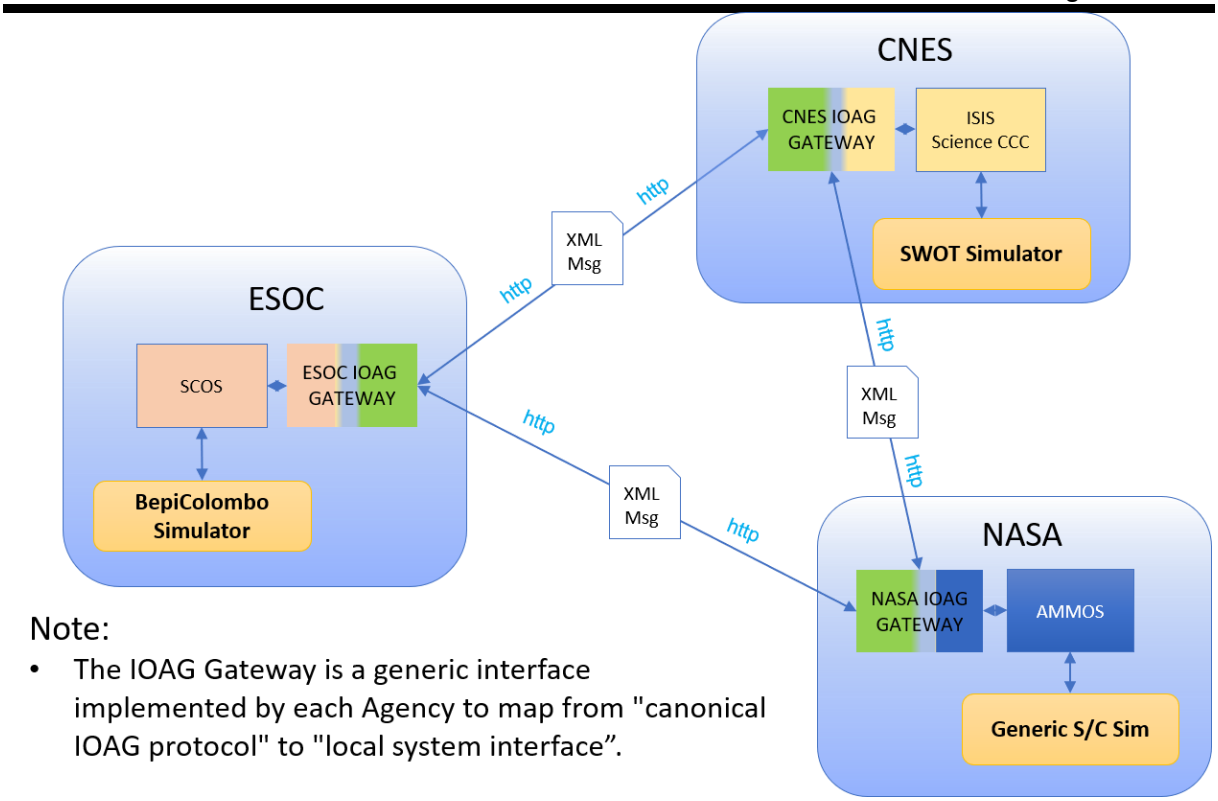

Figure 2 - Demonstrator Topology

As directed by MOSSG, the interoperability team members agreed on the gateway infrastructure architecture before developing or adapting their agency's mission operations system. At a minimum, the team addressed networks, security, and shared data storage systems.

Each agency deployed its representative mission operations system behind its respective gateways (see Figure 2).

ESA/ European Space Operations Centre (ESOC)	- Mission Operations System: SCOS 2000 (Satellite Control and Operations System), providing data to IOAG Gateway via EDDS (EGOS Data Dissemination System). - Spacecraft Simulator: Bepi Colombo dedicated simulator deployed
CNES	- Mission Operations System: ISIS PL (Initiative for Space Innovative Standard Product Line) deployed in Science CCC (Control Command Center)

	- Spacecraft Simulator: Surface Water and Ocean Topography (SWOT) Spacecraft simulator deployed
NASA/Jet Propulsion Laboratory (JPL)	- Mission Operations System: NASA's Advanced Multi Mission Operations System (AMMOS) - Spacecraft Simulator: Generic Spacecraft Simulator (S/C 99) deployed.

Infrastructure setup including communication channels (i.e., IPsec tunnels) and security credentials consumes a considerable amount of time. To simplify gateway deployment and configuration, interagency communication transport and encoding were mutually agreed upon and set to HTTP and XML, respectively.

The following levels of security enforcement were coordinated and established:

- Site-to-site secured connectivity (i.e., Interconnection Security Agreement)
- HTTPS client and server authentication (through Secure Sockets Layer (SSL) certificates)
- User-level authentication and authorization

Remark on user level authentication:

The user level authentication and authorization are obtained by delegation.

(1) All participant agencies are trusted to have secured policies and to correctly protect accesses to a given server (i.e., only authorized people have access to the server).

(2) Due to HTTPS server/client authentication, the recipient of a message (Agency A) is assured of its source being a given agency (Agency B).

Since Agency B is secured through (1) and Agency A is certain that the message is from Agency B through (2) the whole system can be deemed secure.

Future security operational scenarios may require "centralized" or federated authentication and authorization models for security, or otherwise have users be registered with both consumer and provider security domain infrastructures. The gateway infrastructure set up to support this demonstrator activity may serve as a future test ground to validate such security operational scenarios.

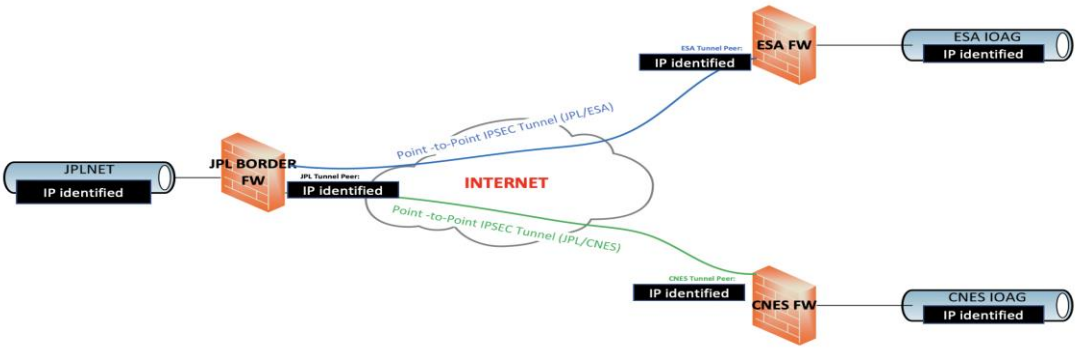

Figure 3 - Site-to-Site Secured Connections

Interagency secured connection included setting up point-to-point IPsec tunnels, which were coordinated and set up by network administrators from NASA/JPL, ESA, and CNES. Furthermore, firewall rules were implemented to only allow traffic from authorized hosts from the participating agencies.

Prior to setting up the site-to-site secured connections and firewall rules, an Interconnection Security Agreement (ISA) was negotiated among all the participating agencies. The table of contents for the ISA can be seen in the figure below.


INTERCONNECTION SECURITY AGREEMENT
Sensitive But Unclassified (SBU)

Figure 4 - Interconnection Security Agreement

3.3 Interoperability Demonstration Testbed Structure

The interoperability demonstration gateway testbed consists of four major constructs:

1. Environment shall include, but not be limited to
    a. Testbeds deployed at three or more agencies
    b. Interface gateways at each participating agency
    c. Secure connectivity between the gateways
    d. The network should be reconfigurable, allowing the testing/demonstration of different network configurations and interoperability concepts
2. Communications infrastructure
    a. Network and transport layer
    b. Login services
    c. Security, etc.
3. Demonstrate interoperability of IOAG Service Catalog #3 services
    a. Agencies would volunteer to install an IOAG Service Catalog #3 “service” in the interface gateway
    b. Access to the “service” would be made available to other agencies (clients)
4. Mission simulator representative of actual mission/project.

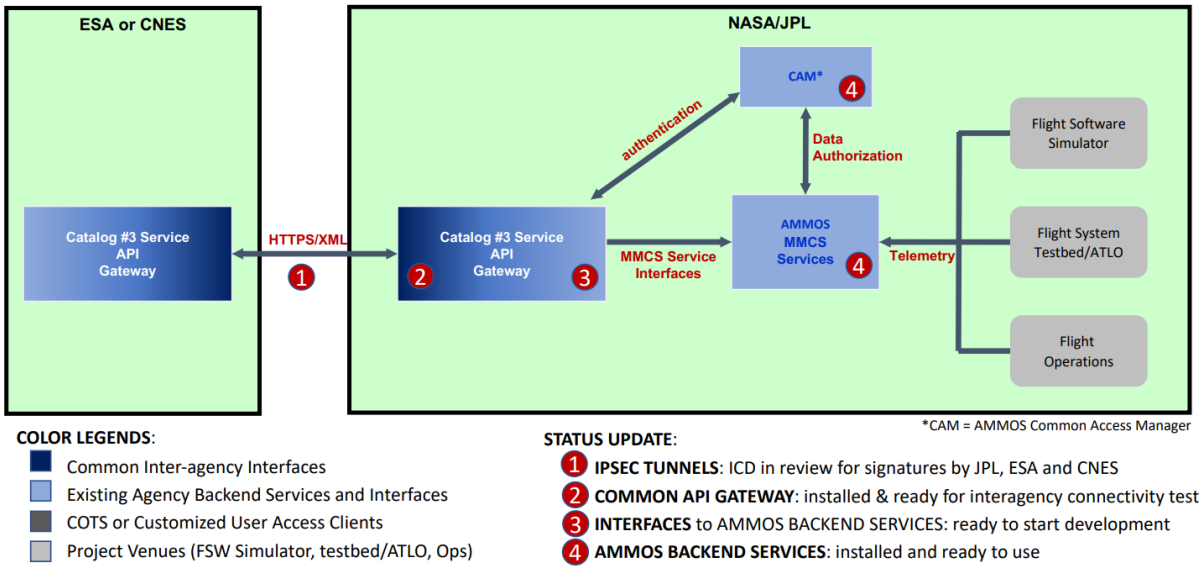

Figure 5 - Example JPL Service Level Interfaces

4 CONCLUSIONS

4.1 Findings

4.1.1 SERVICES ARE NEEDED

The IOAG MOSSG concluded that there is value in both service-based and format-based approaches to support the interactions between agencies. CCSDS standards include both approaches. The term Mission Operations Interoperability Services (MOIS) was introduced to avoid confusion with the CCSDS term Mission Operations (MO) services, which has a broader scope than just ground-based interoperability.

A strict format-based approach still requires some kind of exchange (i.e., "hand-shake") mechanism (e.g., email notifications, publish/subscribe deployment, pre-scheduled SFTP exchange, etc.). The design/architecture in this case may require a trade study to identify where to draw the line between standardized services (e.g., CCSDS MO Services) and custom/specific service deployments (e.g., SFTP, pub-sub, REST services, etc.).

4.1.2 SECURITY IS A CRITICAL ASPECT OF INTEROPERABILITY

Establishing secure custom communication tunnels beyond point-to-point is a tedious process and requires consideration of each agency's information technology (IT) structure and procedures. Typically, ICDs are used to capture such details. User-level authentication and authorization controls are not possible at the action-invocation level unless each user involved in the exchange has identities within the entire interoperability domain. For example, an interoperability user in our case would need identities within each agency's system (CNES, ESA, NASA) in order to enforce action invocation authentication and authorization.

4.2 Recommendations

Each agency participating in the demonstration has current ground systems and is successfully supporting missions. Discussions of interoperability and data exchanges shall address communications between these systems and the intention is not to intrude into the system designs of current systems, nor shall interoperability require the use of common software across agencies.

Three approaches for promoting development and adoption of interoperability standards are recommended so far:

1. A proactive approach that begins with a limited testbed environment targeting a subset of capabilities to demonstrate an interface gateway concept. Over time, we

should build on top of this environment that incorporates all security and operational constraints:

   a. By increasing the capability set of IOAG Service Catalog #3 services on these gateways
   b. By increasing the number of participating agencies

2. Identify some missions to use the interface gateway approach and increase the technology readiness level in preparation for more sophisticated future missions.
3. Within each agency, this gateway environment should be turned into an approved operational means, so that all new multi-agency projects can use this solution by default instead of starting from scratch.

An additional perspective that needs to be considered when discussing mission operations interoperability is cloud deployment. This aspect was outside this group's scope of work at this time, but a future study is highly recommended.

The MOSSG concluded that mission operations is a critical aspect of any mission's success and multi-agency coordination among many programs is essential. Operations and interoperability aspects should be considered in multi-agency cooperative programs from the start, including the appropriate use of applicable standards. The MOSSG recommended that the IOAG consider options for promoting mission operations interoperability activities well into the future.

The IOAG MOSSG interoperability demonstration can be extended to accomplish additional mission operations interoperability activities and look beyond the current "ground system–to–ground system" focus (e.g. cloud).

ANNEX A: IMPLEMENTATION DETAILS

Real-time telemetry data exchange test parameters (service-based approach)

The aim is to show what was needed to perform this exchange using MO services. This information can be used as a draft for an operational ICD.

IMPLEMENTED SERVICES

- Monitor and Control (M&C) Parameter, operations getValue, monitorValue only

TECHNOLOGY

- CCSDS MO Message Abstraction Layer (MAL)
- Transport: HTTPS (as defined in CCSDS 524.3-B-1)
- Encoding: XML (as defined in CCSDS 524.3-B-1)

SECURITY

- End-to-end IPsec Virtual Private Network (VPN) Tunnel
- Certificate exchanges for HTTPS:
    - HTTPS server-side authentication
    - HTTPS client-side authentication

CONNECTING ENDPOINTS

	Provider	Consumer	
CNES	https://<IP>:port/IOAG	https://<IP>:port/IOAG	
JPL	https://<IP>:port	https://<IP>:port/IOAG	

Navigation data exchange test parameters (format-based approach)

The aim is to show what was needed to perform this exchange using a format-based approach. This information can be used as a draft for an operational ICD.

IMPLEMENTATION

- Exchange of an "Orbit Ephemeris Message" (OEM) file
  - 1st step request of Agency A with some parameters (start date, end date, …)
  - 2nd answer of Agency B saying the file is ready to be uploaded
  - SFTP transfer by Agency A

TECHNOLOGY

- For service implementation:
  - HTTPS with JavaScript Object Notation (JSON) messages following a REST pattern
- For file exchange
  - SFTP

SECURITY

- For service implementation:
  - End-to-end IPsec VPN Tunnel
  - Certificate exchanges for HTTPS:
    - HTTPS server-side authentication
    - HTTPS client-side authentication
- For file exchange
  - SFTP

CONNECTING ENDPOINTS

	Provider	Consumer	
CNES	https://<IP>:port/IOAG	https://<IP>:port/IOAG	
JPL	https://<IP>:port	https://<IP>:port/IOAG	
CNES	sftp	User passwd	
JPL	sftp	User passwd	