NM B2B CONOPS

Edition: 1.1
Edition date: 30-09-2024
Classi ication: Green

DOCUMENT CONTROL

Document Title	NM B2B CONOPS
Document Subtitle	This field is automatically updated
Document Reference	This field is automatically updated
Edition Number	1.1
Edition Validity Date	30-09-2024
Classification	Green
Status	Final
Author(s)	EUROCONTROL (Internal) NM B2B Focus Group
Contact Person(s)	yves.steyt@eurocontrol.int; jacques.lauzeral@eurocontrol.int

EDITION HISTORY

Edition No.	Validity Date	Author(s)	Reason
0.1	15/09/2023	NM B2B FG	New document
0.2	29/02/2024	NM B2B FG	Initial updates
0.3	29/02/2024	NM B2B FG	Version for NETSYS review of the chapters 1, 2 and 3
0.4	26/04/2024	NM B2B FG	Processed comments from NETSYS on chapters 1, 2 and 3 Version for NETSYS review of the chapters 1, 2, 3 and 4 Reference version for NETSYS/11 30/04/2024
1.0	30/08/2024	NM B2B FG	Processed comments from NETSYS/11, and NETSYS and IMT on chapter 4. Reduced chapter 5, to link to new NM B2B Operational Deployment Document (first version). Reference version for first NDOP/NDTECH approval.
1.1	30/09/2024	NM B2B FG	From NFG#1 30/09/2024. Clarified requirement on “maintenance windows”, in particular what is meant with “planned maintenance window”. Please see sections 3.3.7, 4.3.5 and 4.3.7

TABLE OF CONTENT

TABLE OF FIGURES

1 About this Document

This document presents the Concept of Operations (ConOps) for the future NM Business-to-Business (B2B), which will be delivered through the integrated Network Management (iNM) Programme.

This ConOps is aligned with the High-Level Network Concept of Operations 2029 and is developed in accordance with the Network Flight (4D Trajectory), Flow and iDL (integrated Data Layer) ConOps documents, in terms of intent, data definition, processes, roles, and responsibilities of the Network operational Stakeholders.

The nature of this document is primarily technical: it is talking about B2B. But not only, as this document compiles (to some level) the views from other, more "business-focused" ConOps mentioned above, the materials that feed the decision-making on the technical evolutions of the NM B2B, and its transition from the current situation to the future. Actually, while developing the NM B2B ConOps, it became clear that the "roadmap" aspects were more volatile than the more stable overall ConOps aspects and would therefore be better handled via a document having a faster lifecycle than the NM B2B ConOps. As a result, a companion document of this ConOps has been developed, called the "NM B2B Operational Deployment Plan", dealing with roadmap questions, and expected to have a faster lifecycle than this document a rolling document Both together remain however to be seen as two facets of a single whole.

The NM B2B ConOps has been developed by an NM multidisciplinary focus group, joining operational, strategic, and technical competences from the various NM divisions.

The document is organised as follows:

(1) Chapter 1 (this chapter) introduces the NM B2B ConOps;

(2) Chapter 2 provides an overview of the current and future NM B2B context and scope, and summarises the objectives of its future evolutions to be delivered by the iNM Programme;

(3) Chapter 3 presents the current NM B2B – as-is – situation, including its identified shortcomings;

(4) Chapter 4, following the same structure as Chapter 3 (for eased referencing), describes the solutions that the iNM Programme will bring to the shortcomings described in Chapter 3;

(5) Chapter 5 provides a view on the principles for a transition plan to move from the current NM B2B, mostly through an NM B2B Operational Deployment Plan, to the future NM B2B derived from Chapter 4.

2 NM B2B ConOps Overview

2.1 Introduction

The NM B2B Services enable building an open ATM digital collaborative environment by:

(1) Providing real-time Network situational awareness and supporting collaborative decision making (CDM) processes at the ATM level, in all phases, from strategic to tactical;

(2) Supporting the NM B2B Strategy, i.e. unlocking ATM data and contributing to accelerate ATM digitalisation, while supporting the Stakeholders' transition to SWIM;

(3) Which all comes in support of the implementation of the SESAR Deployment Programme and the CP1 IR - Commission Implementing Regulation (EU) No 2021/116.

2.2 Terminology

The following short list is provided to avoid potential semantic collisions on essential terms that could defined differently in other documents – these terms are consistently used in this document:

1) **NM B2B Client Software ("Client Software" or "Client" in this document)**: a piece of software, operated by an NM B2B Customer Organisation, that accesses and consumes the NM B2B Services – this is most often a backend software component operated by the NM B2B Customer Organisation (vs. an HMI application).

2) **NM B2B Technical User ("User" in this document)**: refers to all technical roles involved in consuming NM B2B services, via Client Software – e.g. IT operations, developers, technical testers, etc.

3) **NM B2B End User ("End User" in this document)**: refers to all operational roles interacting with the NM B2B services via Client Software.

4) **NM B2B Customer Organisation ("Customer Organisation" in this document)**: the organisation that operates Client Software.

5) **NM B2B Service ("Service" in this document)**: exposes a collection of logically grouped service interactions. For example, the 'Flight Preparation' service exposes the following service interactions:
   - FlightPlanValidationRequest/Reply
   - RoutingAssistanceRequest/Reply
   - EvaluateFlowImpactRequest/Reply
   - ReroutingApplyRequest/Reply

6) **NM B2B Service Interaction ("Service Interaction" in this document)**: supports the interaction of a Client with the NM B2B according to one message exchange pattern (Request/Reply or Publish/Subscribe Topic).

7) **NM B2B Business Use Case ("Business Use Case" in this document):** a group of NM B2B Service Interactions that enable the implementation of a specific business

functionality. For example, the 'Flight Filing' Business Use Case groups all the NM B2B Service Interactions that enable the 'Flight Filing' business functionality.

2.3 Objectives / Drivers

The objectives of the NM B2B evolutions expressed in this ConOps document are:

(1) Operational Efficiency: Help NM B2B Stakeholders to integrate the operational requirements from regulations (e.g. CP1), improve their operational efficiency, reduce costs, and enhance productivity through the NM B2B services.

(2) Development Planning: Help NM B2B Stakeholders to build their operational development plans (driven by changes to operational requirements, e.g. FF-ICE/R2 or iDL AIRAC data building) as well as their technology evolution plans (mostly driven by total cost of ownership considerations, e.g. deprecation of legacy protocols), through the provision of the NM B2B development plans (and behind the corresponding backend developments), in a collaborative manner through the NM CDM Process.

This planning is intended to rationalise changes coming from different sources, like iNM (and associated ConOps plans) and regulatory requirements, to avoid a sequence of changes that would better be handled in some specific way and timeframe.

By defining and sharing migration plans, this document also intends to clarify how business continuity of NM B2B services delivered to NM B2B Stakeholders will be supported.

(3) Quality of Service: As all trends today move the ATM community from older technologies (like AFTN) to modern SWIM ones, this document emphasises efforts made in the area of Quality of Service (QoS), considering the intensive use of Internet and its inherent issues (e.g. DDoS), more generally on the many aspects related to risks on service delivery, including scalability and contingency.

(4) User Support: In addition to the QoS objective, the ConOps aims at describing more specifically how NM intends to improve the current User support to address issues promptly and ensure a positive User experience. This implies strengthening the relationships with existing Users, in particular gathering feedback from Users and building on their feedback to continuously enhance the NM B2B services.

Across all these objectives, the NM B2B ConOps aims at realising the appropriate and agreed balance between change and service stability: one should not change for the sake of changing. Consequently, the B2B ConOps will make sure that the proposed evolutions are duly motivated either by regulatory context, and/or obsolescence of technology, and/or business evolution, and/or clearly identified values for the Users.

2.4 ConOps Scope

This ConOps covers technical evolutions of the NM B2B.

The functional scope of this ConOps is the set of existing and future NM B2B services that are planned to be provided by NM to NM B2B Stakeholders between now and 2030.

The current set of NM B2B services is described in the NM B2B Reference Manual, part of the NM B2B documentation (https://doc.b2b.nm.eurocontrol.int/documentation).

Additional information can be found in the “Business Scope” sections of the chapters 3 and 4.

2.5 Stakeholders, Roles and Responsibilities

All operational Stakeholders having an interest in the NM B2B are concerned by this ConOps, being either for technical reasons, and/or with the purpose of planning their development plans from a functional perspective.

However, it is important to note that the functional evolutions of NM B2B services are NOT driven by this ConOps, they are described in the set of respective business ConOps documents. Therefore, this specific NM B2B ConOps does NOT change by itself any Stakeholder’s role and responsibility.

3 AS-IS – Problem Statement

3.1 Introduction

This chapter focuses on the problems identified (by NM) in connection with the various NM B2B services offered today to the NM Stakeholders: the “as-is” situation.

These problems have been categorised as follows:

- Technical aspects – focusing on the most relevant technical issues;
- Service operational aspects – focusing on the most relevant operational issues;
- Business scope – focusing on the most relevant business scope issues.

3.2 Technical Aspects

3.2.1 Consistent B2B

NM offers today many services via various APIs (i.e. web services), all aimed to enable information and data exchanges between NM and the Operational Stakeholders.

The two most relevant examples are today:

1) The NM B2B: the operational B2B services for Airspace, Flight and Flow management, widely documented in the NM B2B Services Documentation;

2) The EAD AIMSL: the API exposed by the pan-European AIS Database (EAD) to the AIS community to provide their national AIM data and consumed by Stakeholders needing information from AISP (e.g. AIP, NOTAM).

In addition to the two widely used APIs above, there are a series of initiatives within NM that wish to expose more services, and potentially new APIs.

Even though all these service families are compliant with the SWIM specifications, they are inconsistent from many aspects, as:

- They do not implement cross-service links although they all involve the same entities;
- They do not implement the same “flavours” of the same standards (e.g. AIXM);
- They are not based on the same communication technologies;
- More generally, they simply do not have anything in common, meaning that from the API consumer perspective, such a heterogeneity requires the learning of distinct standards, rules, constraints, and quality expectations, and ultimately the implementation of distinct solutions… which is significantly cost-ineffective.

The next sections detail the main technical aspects that ALL NM B2B services should respect, consistently, and not necessarily as they are implemented today by NM.

In order to reach the expected NM B2B consistency, some “fundamentals” must be formally defined, basically made of a set of standards, rules, and constraints to which the API provider (entities within NM) and its consumers must all conform, which is not necessarily always the case today:

- Regulatory context;
- Service lifecycle and versioning;
- Platforms;
- Message exchange patterns;
- Exchange protocols;
- Service consumer identification;
- Security;
- Quality of service;
- Usage policy;
- API design guidelines.

3.2.2 Regulatory Context

3.2.2.1 General

The following European Commission Implementing Regulations impose regulatory requirements to the NM B2B:

- Commission Implementing Regulation (EU) 2017/373 of 1 March 2017: laying down common requirements for providers of Air Traffic Management/Air Navigation Services and other Air Traffic Management Network functions and their oversight;
- Commission Implementing Regulation (EU) 2023/1769 of 12 September 2023: laying down technical requirements and administrative procedures for the approval of organisations involved in the design or production of Air Traffic Management/Air Navigation Services systems and constituents and amending Implementing Regulation (EU) 2023/203;
- Commission Implementing Regulation (EU) 2021/116 of 1 February 2021: on the establishment of the Common Project One (CP1).

3.2.2.2 SWIM Compliance

The services and information exchanges supported by the NM B2B are covered by the European Commission Implementing Regulation 2021/116 on the establishment of the Common Project One (CP1) which mandates that these services must be SWIM Compliant. SWIM Compliance is therefore a regulatory requirement for the Network Manager and must be considered through all phases of a service lifecycle.

SWIM Compliance is established through a self-assessment process which consolidates evidence of the satisfaction of the requirements defined in the EUROCONTROL SWIM Specifications.

The following consolidates the SWIM Compliance status of the APIs exposed by the Network Manager:

- The NM B2B is SWIM Compliant and publishes with each release the SWIM Compliance assessment;
- The EAD AIMSL is SWIM Compliant and publishes with each release the SWIM Compliance assessment.

There is no common process within the Network Manager that defines how the SWIM Compliance self-assessment must be done, or that establishes the criteria that identify which APIs should follow the processes to demonstrate SWIM Compliance.

It is unclear how the evolution of the SWIM Specifications impacts the SWIM Compliance status of existing services. Demonstrating compliance with a specific version of the SWIM Specifications does not guarantee that the service will remain compliant with future major releases of the SWIM Specifications. The regulation is not explicit on how the evolution of the SWIM Specifications is to be handled with respect to existing SWIM Compliance assessments.

3.2.3 Service Lifecycle and Versioning

This section describes the current issues that have been identified with regards to the NM B2B lifecycle, i.e. the full process that takes place between the definition of a future API change on paper till its deployment in operations.

Late deployment

The current deployment plan of a new service (or of a service update) can be summarised as follows:

- About one year before OPS deployment: publication by NM of the NM release notes that contain a high-level description of the changes and the potentially impacted Stakeholders;
- About three months before OPS deployment: publication of a draft version of the API change;
- About one month before OPS deployment: deployment of the API change on the PREOPS platform;
- OPS deployment of changes.

Such a deployment plan does not cater well for either the Client Software development periods or the Users' and End Users' training periods. For example, the possibility to dynamically activate/deactivate RAD restrictions was planned to be delivered by Release NM 27.0:

1) This new feature was announced by the NM 27.0 Release Notes published in March 2022;
2) In December 2022, a draft version of the RADRestrictionActivationRequest/Reply was published;
3) In March 2023, the RADRestrictionActivationRequest/Reply was deployed on the PREOPS platform;
4) In April 2023, the RADRestrictionActivationRequest/Reply was deployed on the OPS platform;
5) However, just after the OPS deployment, it was decided to disable this Request/Reply until January 2025, to allow the interested Users to develop their Client Software, but also to enable the training of the impacted operational Stakeholders (AMCs, Airspace Users, CFSPs and FMPs).

More generally, the current deployment plan is not satisfactory for the following reasons:

- It does not offer a large enough timeframe to gather User feedback on the API proposal;
- Neither a Client Software development period or a Users' and End Users' training period is foreseen. As a result, the new service (or the service update) starts being used only several months (sometimes years as emphasised by the previous example) after its OPS deployment;
- As soon as it is deployed on the OPS platform, corrections to the API become difficult to implement before the next API version, which is too late too;
- For some operational needs, NM also provides an HMI on top of the service, allowing users of this HMI to benefit from the evolution of the service much earlier than End Users relying on NM B2B Client Software. This can become a source of operational difficulties as NM HMI users might introduce data in the system that NM B2B Client Software is not capable to process yet, leading to the misalignment between the information accessible via NM HMI and via NM B2B.

Mandatory yearly upgrades for Users

The current NM B2B lifecycle ensures that a major version remains available during one year after the deployment of a new major version, meaning that Users have a period of one year to migrate to the new version.

However, NM deploys a new major version on a yearly basis. As a result, Users are forced to upgrade their Client Software every year even when the new major version does not bring them significant operational benefits. Moreover, some Users must notify their regulators about any change, including the upgrade of the URL to the new NM B2B version.

Incomplete exposure of the OPS release on a non-OPS platform

Each NM release is deployed on the PREOPS platform one month before its deployment on the OPS platform. Consequently, during this one-month period, Users have no test environment aligned on the current OPS platform, meaning that during that month Users are prevented from validating their Client Software against the currently deployed NM B2B.

Also, Users do not have a way to assert that their Client Software interact in the same way with the new release as with the previous one.

Limitations of current versioning policy

Today NM deploys one B2B version per year.

Each B2B version may contain backward compatible and/or backward incompatible changes.

At each yearly NM release, NM deploys a new version of B2B but keeps supporting the previous version for another year. This approach comes with two major benefits:

1) It offers business continuity to Customer Organisations (no urge to jump to the new version);
2) It gives NM the freedom to evolve the API without the constraint of keeping it backward compatible.

Every NM B2B version has two digits *X.Y*, which may give the impression of a *Major,Minor* versioning scheme. But, de facto, the versions are actually of the form *X.0*, and each version is a major version (e.g. 25.0, 26.0, and so on).

However, this parallel deployment of two major versions, while very useful for backward-incompatible changes, is too restrictive for backward-compatible changes. For example, when NM wishes to deploy a new B2B service, operation or simply add a new optional input parameter, it is forced to do so in the context of a new major version that will be deployed alongside the existing one in the next NM release.

The lack of a *minor version* concept strongly limits the NM ability to deploy backward-compatible changes at a faster pace.

3.2.4 Platforms

3.2.4.1 Normal Operations

During normal operations, Stakeholders may access the NM B2B on the following platforms:

Pre-Operational (aka PREOPS)

Used for development and testing of Client Software by external Stakeholders but also for validating such applications for operational compliance before being granted access to OPS (as part of the *OPS Validation* process).

Operational (aka OPS)

This is the Operational NM B2B platform, which is connected to the operational backend systems of NM. It is the most critical of the NM B2B platforms.

ENVPREVAL.NEXT

This platform exposes the environment data defined for the next AIRAC cycle. The new AIRAC data is usually propagated to OPS six days before the AIRAC switch. However, some Stakeholders expressed the need to be able to access the data earlier so as to validate the impact on the flight plan filing.

ENVPREVAL.ADHOC and ENVPREVAL.ADHOC5

These two platforms are similar to the ENVPREVAL.NEXT but they are designed to expose future AIRAC data (e.g. six months in advance) for the same purpose.

3.2.4.2 Disaster-Recovery

In case of disaster-recovery scenario, the NM B2B is made available on the following platform:

Contingency

This platform is geographically located at a different site in a separate data centre and is activated only in case of serious disaster in the main data centre.

3.2.4.3 Additional Platforms

Additional platforms exist and are sometimes exposed to external Stakeholders in less formal ways:

OPS Maintenance

This is a platform that runs the same software as OPS and is used to validate patches before they are installed in OPS.

OPEVAL

Used by the Airport unit to validate CDM airports – not an officially published platform and hence not documented in the NM B2B Reference Manual.

SAT-I, SAT-X, and SAT-T

Used by SAT for acceptance testing, but sometimes exposed externally for feedback gathering.

NMVP

An experimental platform used to support and validate SESAR concepts.

3.2.4.4 Issues

The current platform ecosystem is the result of an evolution of the requirements during the years coupled with the need for keeping the cost under control.

The following problems have been identified:

Platform abuse

The deployment of extra platforms such as the three ENVPREVAL chains to provide access to different airspace data is suboptimal because:

1) It adds complexity to the deployment;
2) It requires more hardware resources;
3) It requires the Client Software to access different URLs.

The mixed use of OPS Maintenance as a test bed for OPS patches and as a validation platform for DPI messages requires extra coordination, which often was missed, leading to annoying issues and loss of data (albeit test data).

Also, this leads to incoherent and disharmonized OPS validation, which is for some services done on PREOPS and for others done on OPEVAL.

The proliferation of platforms was introduced to compensate the lack of built-in concepts (e.g. “branching” for airspace data).

OPS Validation

Due to the increasing adoption of NM B2B, the PREOPS platform is heavily used and makes it sometimes difficult to perform OPS validations because it contains a lot of fictitious data generated by the Users during their development/testing process.

Some OPS Validation tools (e.g. DPI eval from the Airport unit) expect the data in specific data-warehouse instances and require therefore specific deployments (see OPEVAL). This results into multiple OPS validations, performed by the User on different platforms and with different NM teams (Airport unit and NM B2B Office).

There is therefore a clear need for one or more dedicated platforms on which to perform OPS validations in a controlled and undisturbed environment.

PREOPS – OPS alignment

The data (airspace, flights, etc.) in the PREOPS platform is kept aligned with OPS to some extent, to offer a similar experience to the User who is developing and testing Client Software. In practice, most OPS data is transferred or replayed on PREOPS, sometimes with only a slight delay.

However, the two platforms are not perfectly in sync and the PREOPS cannot be considered an “OPS shadow”. Furthermore, the PREOPS platform, being used for Client Software development and testing, also receives the data submitted by these Client Software under development and testing (e.g. AUP, flight plans, measures, flight updates, etc.), so it will always differ from OPS.

This apparent OPS-PREOPS data alignment can be exploited by the Users in different manners:

- Users testing their Client Software will benefit from a platform that is as close as possible to OPS in terms of data;
- A User who would simply want to “play around” with NM B2B to explore its possibilities or to investigate a new business use case could exploit the fact that it can obtain the same data as from OPS (this did happen in the past).

Today, NM B2B is not capable to discriminate these two usages. It does not expose a “degraded” service for the sole purpose of research.

Automated testing

It is today practically impossible for a User to implement and execute automated tests:

- Automated testing requires stable and reproductible data. The OPS data alignment implemented today on the PREOPS platform does not fulfil this requirement. In an extreme case, if there is no traffic (which is not unimaginable, e.g. volcanic ash), there is no flight data to test against.
- Users do not have the possibility to test their Client Software in isolation from other Users. If different tests try to change the state of the same resource, they will receive unexplainable and unreproducible errors. The output of a flight filing test can be different depending on possible creation of test regulation(s).

This lack of support for automated testing prevents Users from:

- Complying with stringent (ED-153) software assurance level requirements, e.g. FDPS;
- Developing according to the engineering best practices (relying on frequent and automated test execution).

Deployment of future versions

Today, there is no platform dedicated to the early exposure of the future NM B2B versions. As explained in Service Lifecycle and Versioning (Deployment Plan paragraph), the lack of such a dedicated platform prevents NM to gather User feedback about the API changes before their OPS deployment. It also prevents Users that would like to use the new services and/or capabilities to start their developments sufficiently in advance to be ready when the version is deployed on the OPS platform.

3.2.5 Message Exchange Patterns

3.2.5.1 NM B2B

Today, the NM B2B API supports four message exchange patterns:

Synchronous Request/Reply (S-R/R)

1) The Client sends a request;
2) The NM B2B returns a synchronous reply.

Asynchronous Request/Reply (A-R/R)

1) The Client sends a request;
2) The NM B2B returns a synchronous request receipt reply;
3) The NM B2B publishes an asynchronous reply message.

Event Publish/Subscribe (E-P/S)

1) The Client subscribes to a topic;
2) The NM B2B publishes messages when topic events occur;
3) Issue: The E-P/S message exchange pattern is not homogeneously supported across the NM B2B API. The FLIGHT_DATA, FLIGHT_PLANS, and FFICE_PUBLICATION topics support the synchronisation of the subscription – the subscription synchronisation allows the User to receive the topic messages, recently published, but anterior to the subscription activation. Such a synchronisation is not supported by other NM B2B E-P/S topics.

File Download

1) The Client sends a download request;
2) The NM B2B returns a file location from which the User can download the file.

3.2.5.2 AIMSL

Today, the AIMSL API uses two other message exchange patterns:

Scheduled Publish/Subscribe (S-P/S)

1) The Client subscribes to a topic with a given schedule (e.g. the Client subscribes to the daily publication of the ATFCM situation at 06:00, 12:00 and 18:00);
2) AIMSL publishes messages according to the subscribed schedule.

File Upload

1) The Client sends an upload request (including a file);
2) AIMSL uploads the file.

3.2.5.3 Lack of Guidelines

Today, only two NM B2B Requests/Replies (AirspaceDataRetrievalRequest / Reply / ReplyMessage and AirspaceDataIncrementRetrievalRequest / Reply / ReplyMessage) are exposed as A-R/R.

Several NM B2B Requests/Replies that possibly require a long processing time, e.g. Routing AssistanceRequest / Reply, are only exposed as S-R/R.

Some mission critical NM B2B Requests/Replies, e.g. FlightPlanCreationRequest / Reply, might benefit from an A-R/R pattern, as it allows a deferred treatment, in case of resources overload or temporary unavailability.

No guidelines/selection criteria are defined yet to help the API designer decide which pattern to use to expose a service. Similarly, no guidelines assist API consumers in selecting the right pattern when multiple options are available.

3.2.6 Exchange Protocols

Up to now, no proper cross-domain assessment has been conducted with the purpose of identifying the best SWIM-compliant solution(s) for the entire NM scope.

3.2.6.1 Synchronous Exchanges

3.2.6.1.1 HTTP

NM B2B supports HTTP/1.1 over TLS (versions 1.2 and 1.3). Newer versions of HTTP present certain improvements that make connection establishment quicker, mitigate head of line blocking, and increase performance significantly while used in non-reliable networks (e.g. wireless and roaming).

Any choice of the technology stack used to implement the NM B2B API is constrained by SWIM compliance as this is mandated by CP1 regulation. The last version (at the time of writing) of the SWIM TI Yellow Profile Specification is v1.1 which mandates the support of version 1.1 of the HTTP protocol but allows supporting higher versions as long as these are backwards compatible or there can be a fallback to HTTP/1.1 through protocol negotiation.

3.2.6.1.2 SOAP, POX, REST

There is no homogeneity in the high-level protocols used by the NM B2B APIs exposed by NM to support Request/Reply exchanges:

- NM B2B exposes SOAP and POX Requests/Replies;

- AIMSL exposes SOAP Requests/Replies.

This heterogeneity is the source of overhead in terms of developer expertise, tooling, and maintenance of multiple technology stacks.

The support of the SOAP protocol by modern programming languages (e.g., Rust, Go, Typescript) is scarce, and often lacking mature, feature-complete and well-maintained libraries. Reliance on SOAP might pose a problem for any new development as it significantly constraints the available programming languages to implement Client Software as well as finding the relevant skillsets in the labour market.

POX remains supported by all, modern or less modern, programming languages. It is also used by a significant portion of the existing NM B2B Clients.

Today, more than 50% of the received requests use SOAP.

In contrast, a different set of technologies that support strongly typed service contract definitions has gained adoption during the last decade and is currently being analysed by the SWIM Yellow Profile working group. These include OpenAPI, gRPC, Avro, Protocol Buffers, JSON Schema, none of which are used or supported by the NM B2B or AIMSL.

Should the adoption of a new (following an update of the SWIM-TI Yellow Profile) protocol be decided and planned, the model centric API design, implemented by the NM B2B, would guarantee the possibility to support it for a reasonable cost for NM and facilitate a smooth transition for the Users.

3.2.6.2 Asynchronous Exchanges

There is no homogeneity in the high-level protocols used by the NM B2B APIs to expose Publish/Subscribe exchanges:

- NM B2B uses AMQP 1.0;
- AIMSL uses WSN.

This heterogeneity is the source of unnecessary extra developments. Moreover, the WS-Notification technology suffers from recognised weaknesses:

- The main open source project that supports WS-Notification has been abandoned and remains unmaintained since 2013;
- WS-Notification has never experienced large-scale adoption;
- Its lack of adoption means expertise and know-how are scarce which makes troubleshooting complicated;
- WS-Notification implementations present technical challenges related to firewall traversal.

3.2.6.3 Data Exchange Formats

Both NM B2B and AIMSL APIs use XML. Moreover, both APIs rely on standard aviation exchange formats (AIXM and/or FIXM) which are also defined in XML.

Other data exchange formats like JSON (most used format) or Protocol Buffers (more performant) have been foreseen as possible alternatives. However, no satisfactory solution was found yet regarding their combined usage with AIXM and FIXM.

3.2.6.4 Exposure of Geographical Feature Services

AIMSL exposes geographical feature services via WFS 2.0.

Whereas like AIMSL, NM B2B exposes airspace data (Airspace Structure service), it does not expose geographical feature services.

The exposure of geographical feature services should be consistent.

3.2.7 Service Consumer Identification

The identification of the service consumer aims at enabling the following capabilities:

- Service and resource access control;
- Usage policy enforcement;
- Runtime user activity monitoring:
- Post-ops user activity reporting.

From the NM B2B perspective, the service consumer is characterised by the following elements:

1) A Customer Organisation
2) An End User
3) A Client Software

Today, NM B2B insufficiently supports these concepts – instead NM B2B relies on the following technical artefacts:

- The X.509 certificate;
- The “default” ANUId associated to the certificate;
- An optional “act on behalf of” ANUId, which if received, overrides the “default” ANUId.

Nothing prevents the same X.509 certificate from being shared by several instances of Client Software. On the contrary, and for legacy scalability constraints, several X.509 certificates can be used by the same Client Software.

ANUId stands for Air Navigation Unit Identifier. However, in practice, the ANUId is nothing else than a string. In some cases, its value allows a non-formal identification of a business actor (for example, ‘KLMAOCC’ identifies KLM Aircraft Operator). In other cases, it is an opaque identifier with no semantic (for example, ‘EH002882’ identifies Sabre Airline Solutions).

In any case, the X.509 certificate and the ANUId do not allow a formal identification of the End User and Client. Consequently, the current NM B2B cannot:

- Assert access rights and enforce usage policy according to the business responsibility of the End User;
- Assert access rights according to the level of validation of the used Client Software;
- Monitor and report about End User / Customer Organisation activities;
- Monitor and report Client Software behaviours.

3.2.8 Security

3.2.8.1 Protocols

The NM B2B relies on TLS (v.1.2 and v.1.3) as its transport layer security protocol, which ensures point to point integrity and confidentiality of the information exchanged. As well as supporting authentication based on X.509 certificates.

SWIM compliance strongly constrains the choice of transport layer security protocol, as it mandates the use of TLS v1.2 (or higher). The NM B2B satisfies this constraint.

3.2.8.2 Network

The NM B2B is offered through two different networks: the Internet, and PENS. At two different sites; Brussels and Bretigny (acting as contingency). The PENS network is isolated from the public Internet as a Multiprotocol Label Switching Virtual Private Network (MPLS VPN). Each endpoint is protected by an independent firewall.

The Internet endpoints, as a public network, may be subject to Decentralized Denial of Service (DDoS) attacks. Given the nature of these attacks there is no perfect protection against them, nor can they be truly avoided. Instead, a defence in-depth approach can help mitigate their impact to a large degree. Given the use of mutual TLS authentication by the NM B2B the reliance on Content Delivery Network (CDN) solutions to mitigate DDoS attacks is constrained to the TCP/IP layers, which sit below the TLS encryption. These solutions can be effective but cannot involve powerful inspection techniques at the application protocol layer as this would require terminating TLS at the CDN.

The PENS endpoints on the other hand have an extra layer of protection as part of a permissioned VPN isolated from the Internet, which would make these types of attacks not feasible.

3.2.8.3 Credentials and Authentication

The NM B2B uses credentials at two different layers: at transport layer, and at message layer.

At transport layer, it relies on mutual TLS authentication based on X.509 certificates. This allows to authenticate the NM B2B to the Client Software, and the Client Software to the NM B2B with very high security guarantees.

At message layer, the ANUId is used as an additional Client credential. The ANUId is used by the NM B2B and the NM backend systems to apply additional business rules and authorization controls.

Mutual TLS authentication based on X.509 certificates as used by the NM B2B provides very strong security guarantees but presents some drawbacks that need to be carefully considered:

- X.509 certificates are complex to set-up and manage for the User. They need to be exchanged off-bound in a secure manner, Users need to be aware of how to set their Client Software implementation to use certificate authentication and know how to store them securely.
- The process of issuing an X.509 certificate has an associated overhead in terms of workload and time to deployment.
- X.509 certificates have a finite lifespan and need to be renewed periodically. Increasing workload in the teams involved and costs long-term.

- X.509 certificates are not suitable for web implementations. An oft-requested implementation pattern Users would like to explore involves the use of a web platform whose backend is connected to the NM B2B and offers a web-based frontend or API to allow Users of the said platform to access NM B2B data or functionality. This type of solution cannot be supported currently because the certificate presented by the platform does not identify the End User, and the ANUId that identifies the End User Organisation can be spoofed.
- Due to the costs and overhead associated to the issuance and management of each certificate, a coarse-grained approach to Client authentication via certificates is often used. Instead of using a fine-grained certificate authentication where each instance or application inside an organization is issued a specific non-shareable certificate, multiple instances and sometimes applications within an organization will often use the same certificate. This approach weakens the monitoring, control of usage quotas, and authorization controls that the NM B2B can apply on its End Users.
- Any endpoint exposed on the public Internet can be subject to DDoS attacks. Content Delivery Network (CDN) providers offer various solutions to mitigate these attacks, but the most sophisticated techniques require TLS termination at the CDN so they can perform packet inspection. TLS termination at the CDN implies that the mutual authentication will be performed between the Client and the CDN provider, instead of the NM B2B. Performing Client authentication outside of the TLS layer can mitigate this issue and enable more sophisticated DDoS protection solutions to be used.

The ANUId usage as message layer credential identifying the business entity presents various problems. The ANUId credential offers poor properties as an authenticator, as it provides no protection against spoofing or impersonation. The ANUIds are not secret, and any system could potentially fill-in a valid ANUId of any other system. In practice, this issue is mitigated in the NM B2B because a mapping between certificates and ANUIds is kept, which limits impersonation risks to the business entities within the same organization sharing the same certificate. But this approach significantly reduces the solution space of Client implementations that the NM B2B can support, preventing cross-organizational middleware infrastructure and SAAS-like Client solutions.

3.2.8.4 Authorization

The NM B2B enforces access control to the operations, topics, queues, datasets, and resources exposed by the NM B2B API on a per client certificate basis. That is, the NM B2B maintains as part of its configuration a mapping of each certificate to the set of operations, topics, datasets, and resources that it has access and enforces access control based on it.

The NM B2B does not provide the means to perform updates to the authorization of an End User during runtime. The access control to the NM B2B is defined statically and modifications require a new deployment of the software. This constraint severely impacts the ability to serve End Users timely, updates to the authorization are treated as software changes and must follow the control management processes and schedule of a release.

The NM B2B would benefit from being able to enforce access control based on configurable assertions on the payload. For instance, an Aircraft Operator may be able to retrieve flights only if some field of its payload matches certain values. Or subscribe

only to flights that match its callsign. The NM B2B does not have the technical means to support this type of access control currently.

The NM B2B authorization *hardcodes* access to each message queue to a single certificate. This implementation pattern severely limits the possible solution landscape on the Client side. The NM B2B would benefit from abstracting the authorization applied to its Publish/Subscribe message queues to enable credential agnostic assertions. This would allow the NM B2B to enforce access controls to the message queues to other credentials or combinations of credentials.

The NM B2B cannot rely on the ANUId for authorization control due to the weak properties it has as an authenticator. This prevents the NM B2B from enforcing access control, usage quotas, and monitoring at the End User identity level and must rely exclusively on the certificate for authorization control.

3.2.9 Quality of Service

3.2.9.1 Performance

The NM B2B provides its services on a *best-effort* basis in relation to the performance Quality of Service.

The NM B2B measures and publishes with its Reference Manuals the response times of each operation exposed by its API at the 50%, 95%, and 99% percentiles. These figures are based on the response times observed on the OPS platform.

Response times are globally satisfactory. However, for large responses (size greater than 1MB), the NM B2B response times are below expectations. Moreover, short periods (between a few seconds and a few minutes) of performance degradation are observed in a recurrent manner (a few times a week).

3.2.9.2 Availability, Scalability and Reliability

The NM B2B provides its services on a *best-effort* basis in relation to availability and reliability Quality of Service.

The NM B2B publishes in its NM B2B Services Portal (Sharepoint) the unplanned service degradations which affect the availability of the B2B. It publishes also when the services return to normal operation. Unfortunately, these publications are not automatic and may miss partial degradations or failures affecting specific sub-systems which only affect some services. Furthermore, the NM B2B does not provide figures of the availability (percentage of time the systems remained available) or of the reliability (time between failures or failure rate) affecting the NM B2B services.

Furthermore, the NM B2B does not publish any information regarding the load or the load growth that it can cope with. The NM B2B does not have any estimates of the impact to its availability and reliability of future demand increase of the services.

Finally, the degradations of performance that are regularly observed can in some case result in rejected requests, therefore affecting the availability of the impacted services.

3.2.9.3 Security

The NM B2B guarantees the confidentiality, integrity, and authenticity of the information it serves through its API. It does so via its use of TLS and X.509 certificates for mutual authentication, which guarantees these properties cryptographically.

The NM B2B does not provide the means to guarantee the non-repudiation of the data exchanged through its API. In concrete terms, it does not provide the means to prove that a particular exchange (e.g., message publication) occurred.

3.2.10 Usage Policy

The NM B2B enforces for each X.509 certificate some quotas in terms of:

- Bandwidth consumption per sliding time interval;
- Request count per sliding time interval;
- Simultaneous (parallel) request count.

This usage policy has limitations that should be addressed:

- The request count quotas apply to request types. However, several request types are typically handled by the same NM resource. As a result, either NM resources are not correctly protected, or they are used in a sub-optimal manner. In both cases, Users can be negatively impacted.
- A single User can monopolize, during a short period, a significant portion of some NM resource, with the risk of preventing Users from accessing this resource.
- The processing of invalid requests consumes NM resources. However, no quota prevents a User for sending too many invalid requests. More generally, the NM B2B is not capable to take measures, in an automated manner, to protect itself against misuse, for example by reducing the priority or by suspending some request type access to some mal-functioning Client Software.
- The usage policy is associated to the X.509 certificate presented by the Client. This credential does not uniquely identify the End User identity, which requires the knowledge of the ANU identifier. This implies that the NM B2B has no way of enforcing quotas at the granularity of the business entity. All End Users coexisting under the same X.509 certificate will compete for the same resource quotas.

3.2.11 API Design Guidelines

No NM B2B API design guidelines exist today, which does not help NM engineers when designing the API, neither to discuss these guidelines with the NM B2B Users.

3.2.11.1 Model Centric API

An API is a contract that formally defines a set of B2B services. This contract is agreed by the API provider (who implements the services) and by the API consumers (who use the services).

Formal API contracts enforce the use of specific protocols and exchange format. API contract definitions rely on an API specification language: SOAP (XML exchanges over HTTP), OpenAPI Specification (RESTful APIs using JSON over HTTP), gRPC framework (Protocol Buffers over HTTP/2). However, from a semantic perspective, there is no significant difference between a SOAP, an OpenAPI or a gRPC API contract.

Today, the NM B2B Requests/Replies are exposed in both SOAP and POX.

This double exposure is enabled thanks to the fact that the NM B2B API is maintained in a technology agnostic model, i.e. the API is not directly maintained as a set of WSDLs and XSDs but as a logical UML-like model. The main requirements that led to this choice are the following:

- Support both SOAP and POX;

- Preserve the possibility to expose the NM B2B API in other ways than SOAP or POX by defining and documenting a logical model rather than the formal contract itself;
- Decide which information must be included in the NM B2B API, including aspects that are not supported by standard languages like SOAP, Open-API or gRPC (for example, any change in the NM B2B API is formally linked to a change request that enables the automated generation of release notes).

A clear benefit of this approach is that the NM B2B API documentation is today articulated and presented to the User as a logical model. Therefore, would NM expose the NM B2B API in gRPC or in Open-API, the current documentation would remain valid.

Today, this model centric approach is not consistently used in NM B2B and AIMSL.

3.2.11.2 Services Organisation

3.2.11.2.1 Context

Today, the NM B2B API is organised in a tree-structure of Service Groups – Services – Service Interactions.

Service groups are the root elements. A 'service group', as the name suggests, groups a collection of services that logically fit together. For example, the 'Flight' service group groups the 'Flight Preparation', 'Flight Filing', 'Flight Management' and 'Flight Safety' services.

A service (aka as a Port Type according to SOAP terminology) exposes a collection of service interactions that support some business use cases. For example, the 'Flight Preparation' service exposes the following service interactions:

- FlightPlanValidationRequest/Reply
- RoutingAssistanceRequest/Reply
- EvaluateFlowImpactRequest/Reply
- ReroutingApplyRequest/Reply

A service interaction allows Client Software to interact with NM B2B interfaces according to one message exchange pattern (Request/Reply or Publish/Subscribe).

Each service group is mapped one-to-one to a SOAP WSDL (for a specific B2B version). For example, the Flow Service Group has a FlowServices WSDL file (for a given B2B version).

Each SOAP WSDL relies on one XSD schema that defines the data types used by the services within the service group. For example, the FlowServices WSDL relies on the FlowServices XSD file.

Each XSD schema may import other XSD schemas (of other service groups). For example, the FlowServices XSD file imports the following other XSDs:

1) CommonServices XSD
2) AirspaceServices XSD
3) FlightServices XSD

So, in IT terms, the FlowServices XSD "depends" on the Common, Airspace and Flight XSDs.

Finally, some XSD also depend on external exchange models' XSDs such as AIXM and FIXM.

3.2.11.2.2 Issues

The following problems have been identified:

Monolithic and constraining service groups

The current service groups were introduced when the NM B2B was initially created and they only contained few services back then. The services grew in number and complexity over the years spanning a wider business scope and adopting external exchange models such as AIXM and FIXM. All this resulted in 'bloated' monolithic service groups. This makes the Client Software development more cumbersome. For example, an Airport only interested in obtaining Passenger Demand Forecast data (i.e. a list of flight identifications with few associated numbers) needs to download and process the full FlightServices XSD, plus the dependent XSDs (Common, Airspace and Flow), plus the AIXM XSD (which is used by Airspace) and generate artefacts for all such data types.

It has to be noted however that there is also some value in the service group categorization because it provides a taxonomy and a way to easily identify groups of services that logically belong to a specific ATFM domain or subdomain. However, a distinction should be made between a flexible "logical" categorization versus a more restrictive and constraining "physical" one.

Misplaced services within service groups

Some services are not defined in their "natural" service group, while some others are unnaturally forced into a service group. For example, the *Tactical Updates* service, that supports the retrieval and update of dynamic airspace data, is defined in the *Flow* service group. Such a service would rather be expected in the *Airspace* service group. On the other hand, the GNSS Interference service, which relates to Communication, Navigation and Surveillance is forcefully placed in the Airspace service group.

This makes it sometimes difficult for a User to locate a service.

Suboptimal service granularity

Although it is not always obvious to define what should constitute a service, the NM B2B strives to offer services according to the following principle:

1) An NM B2B service is a collection of service interactions and data types that combined together provide a well-defined business capability or solves a well-defined operational need;

2) Also, a service is most of the times intended for a well-defined set of Stakeholders, unless the business capability is such to foresee a collaboration of several types of Stakeholders.

There are however cases when this principle is not well applied. For example, the Airspace Availability service combines in fact two services (two different service capabilities intended for different Stakeholders):

1) Airspace Management: Intended for Airspace Management Cells (AMC) for booking or releasing restricted airspaces or conditional routes via the submission of AUP/UUP;

2) Airspace Availability: Intended for Airspace Users to retrieve the opening and closures of restricted airspaces and conditional routes that result from the consolidation of the AMC's input into an EAUP/EUUP.

Cross service group dependencies

The NM B2B API contains bi-directional dependencies between the 'Flight' and 'Flow' service groups, leading to some undesired complexity in the corresponding WSDL's and XSD's.

Overloaded service interactions

Some NM B2B Request/Replies support in practice several usages. For example, the EhelpDeskTicketCreationRequest/Reply supports about ten distinct usages intended for different User types (creation of a ticket to force a flight in a regulation, exclude a flight from a regulation, improve a slot, swap slots, etc.). Another example is the FlightUpdate Request/Reply, that allows sending different types of flight updates such as First System Activations (FSA) from ATC systems, oceanic notifications from Gander and Shanwick, Aircraft Position Reports (APR) from Aircraft Operators, etc. Such overloaded Requests/Replies are difficult to use and to document. Moreover, they create complexity in the access rights management and post-ops reporting.

3.2.11.3 API Design Paradigms

The three most commonly observed API design paradigms are:

1) Resource-oriented: This API design paradigm uses resources as its first level of abstraction on which the API is organized. REST interfaces and graph-based interfaces are examples of this type of design.
2) Remote Procedure Call (RPC): This API design exposes procedures as its first level of abstraction on which the API is organized. SOAP, gRPC, Avro, and WFS APIs fall under this design paradigm.
3) Message-oriented: This API design paradigm places the notion of message at the centre of its abstraction and orchestrate the consumption of the service around it. Topic based Publish/Subscribe APIs are clear examples of this design paradigm.

Today, the NM B2B follows:

1) A Remote Procedure Call (RPC) design paradigm for its Request/Reply API, this choice being strongly constrained by its support of the SOAP protocol;
2) And a message-oriented API design for its Publish/Subscribe API.

The choice of service design paradigm has a direct impact in the way services are consumed and there is no one-size-fits-all design. RPCs are a reasonable choice when the API is enabling the execution of certain actions to the requester. For instance, proposing routes for a flight, validating a flight plan, or evaluating the flow impact of a flight plan are examples of functionality enabled by the NM B2B that fit nicely within the RPC paradigm. Exposing this type of actions through a resource-oriented API design can be cumbersome and results in an impractical API design.

The choice of service design paradigm must balance many factors including expressivity, maintainability, ease of use, but also technological considerations. In this respect, the NM B2B lacks guidelines to help the API designer to make the right choice.

3.2.11.4 Naming Conventions

The absence of naming conventions results in various kinds of inconsistencies that make the API difficult to learn and use.

The following points illustrate, in a non-exhaustive manner, these inconsistencies:

- No rule specifies whether a verb or a noun shall be used to describe the action realised by a request/reply. For example, the *Measure* service exposes a

`RegulationCreationRequest/Reply` and a `RegulationCancelRequest/Reply`.

- No “standard verb” is documented. Hence, nothing ensures that two distinct verbs cannot be used in two Request/Reply names with the same meaning or, the other way around, that the same verb is used by two distinct Request/Reply with a different meaning.
- A case policy is defined but not always respected. As an illustration, the OTMV acronym is written differently in different class/enumeration names: `OTMV`, `OTMVThreshold`, but `OtmvAlert`, `OtmvStatus`. Some automated checking is missing.
- Poor naming, long, and specifying the intended actor:
  `AUPGetManageableRouteSegmentsForAMCAndRouteRequest`

3.2.11.5 Error Reporting

The NM B2B error reporting is complicated to use, heterogeneous, and poorly documented:

- Unstructured errors reported by the backend applications are reported by NM B2B as plain text messages associated with inaccurate error type and without any error location / error parameters. It is not possible for the NM B2B to map those unstructured backend errors into a uniform and structured error model. Therefore, the NM B2B exposes unstructured errors to the Client Software which in turn cannot automate the error handling.
- There is no clear separation between generic errors (possibly reported by any type of Request/Reply) and request type specific errors. For example, the `ReplyStatus` enumeration declares generic errors, e.g. `SERVICE_NOT_AVAILABLE` and specific errors, e.g. `OBJECT_OUTDATED` (typically associated to an update method), or even `INVALID_DATASET` which is service-specific.
- There is no exhaustive documentation of the errors possibly reported by a given Request/Reply. For example, a unique `ErrorType` enumeration declares, in the *Airspace* service group, all the errors or warnings, possibly reported by any Request/Reply of the service group. Obviously, not all these errors can be reported by each request.
- Reported errors do not provide an accurate indication of the error responsibility (Client or NM B2B server).
- The corrective action to be followed by a User / Client on an error reply is insufficiently documented. For example, the documentation does not explain what are the User possibilities in case of an access denied or a usage policy violation.
- In case of error, the NM B2B returns the following HTTP status:
  a) 400 – Bad Request – when the request type could not be recognised;
  b) 404 – Not Found – when the request path is incorrect;
  c) 413 – Request Entity Too Large – if the request payload size is greater than 500 KB;
  d) 200 – Ok – for any other error.

Such an error policy does not facilitate the integration with Client libraries / tools, that are typically capable to understand and take measures, like alerting, based on the returned status. The use of a standard HTTP status might help the development and maintenance of the Client Software.

However, it also happens that no HTTP status correctly reflects the error. More generally, the HTTP status should always be complemented by some structured error details.

3.2.11.6 Usage of Message Properties

HTTP messages support the provision of properties expressed as request or response headers. Similarly, AMQP messages support the provision of AMQP Header, AMQP Message, and Application properties. The NM B2B makes today a limited usage of these properties, whereas in some cases, it might avoid some costly and unnecessary payload processing by the Client Software (e.g. for Client-side filtering and routing).

3.2.11.7 Mitigating Impact of Changes

Even if undesired, it happens that some unplanned change must be applied to an already deployed version:

- An enumeration value can have been forgotten;
- A class attribute can be missing;
- A typedef constraint might be incorrect;
- A class constraint can be missing or incorrect;
- A business rule and its corresponding error code might have to be introduced.

The “natural” datatype correction might result in a backward incompatible change and therefore would theoretically require the deployment of a new NM B2B version, which is a heavy process for NM and for the users. Moreover, such changes are usually very localised and only impact a few users.

Loose enumeration is the only mechanism supported by the NM B2B to mitigate such a situation. A loose enumeration is modelled as a union of a strict enumeration and a string prefixed by `OTHER:`. Such model was designed as an extension placeholder, enabling the addition of free text values in a backward compatible manner.

However, the current loose enumeration pattern is often poorly handled by the XML Schema code generators, resulting in cumbersome and expensive manually maintained code.

Additionally, nothing was foreseen to mitigate other kinds of unplanned changes.

3.3 Service Operational Aspects

The section focuses on issues that were identified with regards to how the NM B2B services are operated today, especially from the User's perspective.

3.3.1 Documentation

The NM B2B documentation is very rich today. Yet, relevant shortcomings have been identified and should be addressed to simplify the use of the NM B2B.

3.3.1.1 Technical and Business Documentation

The NM B2B documentation encompasses both technical and business aspects. Within the NM B2B documentation, the NM B2B Reference Manual addresses the technical aspects.

The API documentation (which is part of the NM B2B Reference Manual) refers sometimes to business concepts and procedures described in documents that are not always publicly accessible (parts of NM or EUROCONTROL internal documentation). As a result, various sections of the NM B2B Reference Manual are (rephrased) copies of these business document parts, which is inefficient as the source text often evolves on its own. Moreover, when referencing is possible, it is limited to the document URL complemented in the best case by some section name, which is not proper inter-document linking and leads indeed to broken links. In summary, both approaches currently followed by the NM B2B Reference Manual to link technical documentation to business documentation is not satisfactory.

The other way around, in most cases, the linking from the business documentation to the corresponding NM B2B technical documentation is absent, so that the business documentation reader has no simple way to know whether and how a business process is supported by the NM B2B API.

3.3.1.2 High Expertise Barrier

Today, using the NM B2B often requires the User to understand in depth the processes and data conventions of the NM system.

For example, a User planning to develop a working subscription to the FFICE_PUBLICATION topic but having no knowledge about ENV data will, in turn, have to consult the "FFICE", "Common", "Essentials" and "Airspace" chapters of the NM B2B Reference Manual, as well as the "Flight Filing Use Cases" document, several AIXM schemas and a download of the Units data.

Such a procedure implicitly assumes a high level of expertise of the User developing the Client Software. This is a major obstacle to the use of the API, particularly for smaller organisations who have limited (if any) access to the experts.

3.3.1.3 Examples of API use

Good quality and up-to-date examples are known to be one of the main factors of the easy adoption and usage of an API.

The examples provided today in the NM B2B documentation are of insufficient quality:

- The Request/Reply examples are presented as a pair of XML payloads without any documentation:
    - No business context / purpose;

- No pre-conditions required by the execution of the example;
- The syntax of the provided payloads is valid but nothing guarantees that these payloads are semantically correct.

- The service interactions (Publish/Subscribe or Request/Reply) often come with options and tuning possibilities of which the usage strongly depends on the business case to realise. But, in general, only one pair of XML payloads illustrates the use of the service interaction and alternative usages are not exemplified.

  For example, the FLIGHT_DATA topic is the corner stone of the future slot message replacement. However, it is deemed too difficult today for a development team to get, by way of the documentation, a fully detailed picture of what they will have to build to implement the future slot message replacement via NM B2B.

  It is also generally admitted that the NM B2B lacks some form of functional documentation packaging, mission-oriented, where Client developers would find for a well identified subset of functionalities the technical elements to rapidly build the corresponding know-how, e.g. a technical overview, the NM B2B interactions, their order, etc.

- Business errors are not exemplified, which often triggers specific support from NM to the Client Software developer, which is inefficient for both NM and NM B2B Users.

3.3.1.4 Migration to NM B2B

The documentation concerning the migration to NM B2B is incomplete.

For example, a User willing to receive the same Flight Plan messages, via the FF-ICE NM B2B service, as it receives today via AFTN will have to read the "Flight Filing Use Cases" document. This document recommends the User to contact the National ENV Coordinator or the NM B2B Office to obtain information relative to the data that shall be used to file the subscription.

By its lack of self-consistency such a documentation is source of extra workload for the User, the National ENV Coordinators, and the NM B2B Office.

3.3.1.5 Integration with Third-Party Documentation (AIXM / FIXM)

Both NM B2B and AIMSL APIs rely on third-party exchange models and formats: AIXM and FIXM for NM B2B, AIXM and GML for AIMSL. The points of junction between the NM API and the third-party exchange models require some specific documentation.

The usage within an API of a third-party exchange model requires the documentation of the interpretation and validation rules applied in that API. For example, a FIXM attribute could be declared as optional in the FIXM documentation but mandatory in the NM B2B API; or some mandatory FIXM attribute could be ignored by the NM B2B API.

In the interest of NM and NM B2B Users, the navigation from the NM B2B API documentation to the third-party documentation should be fluid. But there exists today no harmonised guidelines regarding the documentation of a junction with a third-party documentation. As major examples, the NM B2B API does not document the FIXM and AIXM junctions in the same way, and the NM B2B AIXM junction does not support any kind of navigation from the NM B2B documentation to the AIXM one.

3.3.1.6 Change Tracking

Identifying the changes between two NM B2B versions that might impact a Client is of utmost importance for the User. Considered changes are API changes and documentation changes:

(1) An API change:

- New, updated or removed service interaction;
- New, update or removed data type;
- New, updated or removed third-party exchange model usage rule.

(2) A documentation change:

- The update of a plain documentation section, e.g. the update of the Service Usage section of the NM B2B Reference Manual;
- The update of the documentation of an API element.

Regarding API changes, new, updated or removed service interactions and/or data types are automatically emphasised today in the NM B2B Reference Manual. However, the modifications of third-party exchange model usage rules (FF-ICE usage rules for example) are not covered by this automated process.

Regarding documentation changes, the NM B2B Reference Manual contains change annotations to the modified sections. But these change annotations are not generalised to all NM B2B documents. Inside the Reference Manual, the generation of these annotations is not fully automated. As a result, some modified sections might not be annotated as actually modified. Moreover, a change annotation neither indicates what precise portion of the text was updated nor allows the reader to view the previous text version.

3.3.1.7 NM B2B Release Notes

In preamble, one should not confuse “NM Release Notes” – that document the changes brought in an entire NM release and their impact -- and the “NM B2B Release Notes” that are published together with each new NM B2B release deployment.

The NM B2B Release Notes are organised in four main sections:

1) NM B2B versions – the new version and the list of decommissioned versions;
2) Impact on previous versions – the possible impact of the release deployment on the previously supported version(s);
3) Migration guidelines – guidelines to assist Users in migrating their Client Software code from the previous version to the new one;
4) Version notes – the detailed notes on the new version.

The version notes include exhaustive lists of the impacted NM B2B API elements (data types, request, replies and P/S messages). They also support, by design, a bi-directional navigation between the model changes and the version notes.

However, the version notes do not cover the changes in third-party exchange models and in the associated usage rules. Developers are not informed of the impact of these changes and are not sufficiently assisted in upgrading their Client Software.

3.3.2 User Onboarding

The User onboarding process is a critical pathway that begins with a service access request and culminates in the deployment of the Client Software onto the OPS platform.

The following issues have been identified that compromise the efficiency, transparency, and overall User experience of this process:

Fragmented Entry Points

Currently, there is no unified entry point for User onboarding. The existing web form is outdated and poorly maintained. Consequently, Users resort to multiple channels for onboarding, such as direct emails to Customer Support or personal contacts within the organisation. This fragmentation leads to inconsistent experiences and difficulties in tracking and managing onboarding requests.

Multiple ticketing systems

Different NM departments (Customer Support, B2B Office, OSM) use different systems for handling onboarding-related activities. This lack of uniformity not only hinders effective communication and coordination among teams but also creates inefficiencies and delays in process handling.

Process Visibility and Bottlenecks

It is recognised that Users desire a clearer view of their onboarding journey, including the ability to track the status and progress of their requests. Currently, the onboarding process may not always provide the required level of transparency, which can leave Users feeling out of the loop and uncertain about the timing of their onboarding completion. Additionally, this situation can obscure potential bottlenecks, making it challenging for NM and Users to identify and address delays promptly.

Accountability issues

The current onboarding process lacks a centralized accountability structure. Ideally, there should be a designated point of contact for each User, responsible for overseeing and advancing the onboarding process. The absence of such a role leads to diffused responsibility and potentially prolonged or stalled onboarding experiences.

Lack of mechanism for capturing user feedback

The current onboarding process lacks a comprehensive system for tracking and auditing User feedback, hindering the NM capability to track User experiences and pinpoint areas for enhancement comprehensively.

Scalability concerns

As the User base grows, the current onboarding process may not scale effectively. This lack of scalability could lead to increased bottlenecks, delays, and a decline in service quality.

3.3.3 User OPS Validation

This section covers the processes and methodologies used to ensure that Client Software built on NM B2B Services functions effectively and efficiently in the real operational scenarios/usage.

3.3.3.1 Current Process

Introduction to Operational Validation

The NM B2B Operational Validation is a procedure defined in the Operational Deployment of NM B2B Services, which NM follows prior to allowing access to NM B2B Services on the operational platform, for a new or updated Client Software.

The NM B2B Operational Validation is meant to ensure that the Client Software performs as intended.

Objectives of Operational Validation

The main objective of the Operational Validation is to ensure the functional correctness, reliability, security, and compliance of the Client Software with the NM B2B service usage.

During the Operational Validation procedure, it is essential that the operational procedures are aligned with the requirements set in the Client (or with the Client behaviour).

Methods and Approaches

The Client consuming NM B2B services is operationally validated against business and technical criteria; the two approaches complement each other in ensuring a comprehensive validation.

The Technical Operational Validation Documentation describes the metrics and associated thresholds that a Client that consumes the NM B2B Services must demonstrate compliance with before accessing the operational platform.

The NM B2B WRITE Service Documentation Set describes the Business Acceptance Criteria for each WRITE service, i.e. the criteria that a Client shall demonstrate compliance with during the Operational Access Acceptance Activities prior to accessing the operational platform.

However, different methods can be used prior to the operational validation, such as testing, simulations, audits, and analysis of real-time data.

These methods are applied at the NM B2B candidate's request to access the OPS platform.

Operational Validation

The Operational Validation procedure takes place while the Client is connected to the PREOPS platform. It consists of:

1) Technical Operational Validation: The Client operates under nominal conditions for a predefined period of time in PREOPS and is evaluated against the acceptance criteria established in the Technical Operational Validation Documentation;
2) Connectivity Check: A preliminary connectivity check that verifies the Client is ready to proceed with the Business Operational Validation;
3) Business Operational Validation: The business operational validation where the Client will be evaluated against the acceptance criteria established in the NM B2B WRITE Service Documentation Set.

After performing each of these steps, the User is contacted by NM staff responsible to conduct these activities. The positive outcome of each step is mandatory to move to the next step.

Validation Documentation and Reporting

The Operational Validations report contains:

1) Technical Operational Validation Report: The result of the technical Operational Validation;
2) Connectivity Check Report: The result of the connectivity check;
3) Business Operational Validation Report: The result of the business Operational Validation.

The Operational Validation report records the successful criteria but, as well, any deviations/limitations encountered.

3.3.3.2 Issues

Continuous Improvement and Maintenance of Client Applications

The operational validation largely involves manual procedures and assessment.

The criteria mentioned in Methods and Approaches are verified only during the operational validation procedure.

Prior to the beginning of the Operational Validation procedure, Users do not have any indication if their client applications satisfy the exiting criteria or if the NM B2B services are consumed in an efficient way. Users are not able to self-assess their Client Software. This implies that the Operational Validation procedure introduces a significant schedule risk into User side implementation project plans and therefore, the coordinated deployment of new collaborative Network Management features.

The existing published acceptance criteria are only for the NM B2B WRITE services. Similar acceptance criteria shall be proposed for the NM B2B READ services.

Client Software evolves over time. It is important that periodic re-evaluation and validation are performed automatically to maintain operational efficiency. There are no technical means to oblige Users to re-assess their Client Software after each evolution/enhancement.

Platform Issues

The PREOPS platform does not provide a data feed that is close enough to operations to validate services that rely on real time operational data.

The PREOPS platform currently has a dual purpose; it is the platform used for new developments on one side and used to perform Operational Validations. Both coexisting under the same platform. It is not always possible to obtain a clean view of the nominal usage of a Client because its use in PREOPS may coexist with other applications under development.

3.3.4 User Management

The current User management process and tooling present limitations that make it more cumbersome, non-scalable, and slower than necessary.

3.3.4.1 User Identity Management

Identity fragmentation

During onboarding, the User identity is registered in the Customer Relation Management software used by Customer Support. Once the User is ready to start integrating with the NM B2B, Customer Support registers them in the Identity Management software.

These two applications are independent and hold uncorrelated notions of the User identity. Finally, the runtime system has no notion of User identity, instead relying exclusively on the credentials (X.509 certificate and ANUId) without correlation to the User identity.

Technical debt

The tooling available to perform User identity management is obsolete, which is a pain point of the User management processes.

Normalisation issues

There are no formalised and stable conventions on how to identify a User. For example, there is no normalisation process for the definition of the organisation name, which occasionally results in the same organisation being registered under different names. There is no formal categorisation of the types of Stakeholders. The ANUId (see section 3.2.7 for a more detailed discussion) has no reliable semantic.

These issues make greatly difficult the ability to manage a large User base as the identity information recorded cannot be used in a uniform and coherent manner.

Lack of process documentation

The process followed during User identity management is not formalised or documented. Therefore, the enrolling and training of new staff requires more time than necessary.

3.3.4.2 Credential Management

Tooling deficiencies

The tools used to manage the credentials of the User base are relatively old, lack proper maintenance and present various functional deficits that make credential management unnecessarily difficult.

Lack of credential management portal

The NM B2B does not have a web portal to allow Users to manage and retrieve their credentials. The X.509 certificates that the NM B2B relies on to authenticate a User must be renewed with certain periodicity, when that happens months long campaigns to contact the users are initiated – typically resulting in very significant overheads to the teams involved in the credential management.

Process Overhead

The NM B2B manages a pool of X.509 certificates received from its provider, GlobalSign, and assigns these certificates to its users as needed. This adds overhead to the process of certificate management as NM needs to perform certain duties that are typically handled by the Registration Authority and aggravates the problem of the normalisation issues identified in 3.3.4.1.

Lack of dynamic configuration

The credentials that the NM B2B recognises as valid and their respective mappings to authorization cannot be configured dynamically. Any change to the credentials associated to a User requires the deployment of a software patch.

3.3.4.3 Authorization Management

Technical debt

As the NM B2B API grew in functionality, and the User needs became more varied and heterogenous, the initial Role Based Access Control (RBAC) solution became inadequate. Managing authorization changes has become a time consuming and difficult process.

Functional deficits

The NM B2B would benefit from being able to enforce access controls based on assertions made on the content of the request and reply payload, but the solution in place lacks this capability. For instance, it would be beneficial to be able to enforce access controls based on the value of the airports requested in a *queryFlightsByAerodrome* request or enforce access controls based on the filters applied on a *FLIGHT_DATA* subscription. The NM B2B authorization solution lacks the means to express or enforce this level of access control.

Lack of dynamic configuration

Changes to the authorization associated to a set of credentials cannot be managed dynamically. Approved changes are not implemented immediately, instead they are grouped into a software patch which is deployed during a maintenance window.

3.3.4.4 Usage Policy Management

The configuration of the usage policy associated to a set of credentials cannot be deployed during runtime. The same type of constraints and delays as those detailed for authorisation management apply.

3.3.5 Monitoring

3.3.5.1 System, Services, and Users

By definition, the NM B2B monitoring embraces the following views:

1) System monitoring – monitor the behaviour of the components that participate to the delivery of the NM B2B services: load, memory, connections, etc.
2) Service monitoring – monitor the quality of the delivered NM B2B services: performance, reliability, etc.
3) Client monitoring – monitor the behaviour of the Clients: correctness of the requests, compliance with the usage policy, etc.

Today, the NM B2B system is monitored 24/7. However:

- The alerting focuses on system problems – as an example, an alert is raised when a system component is down, but not when a B2B service is slow;
- No QoS monitoring criteria have been defined. For example, no alert is raised in case of service performance degradation;
- Incorrect request metrics as well as usage policy violation metrics are evaluated and available near real-time – however, no alert is raised if a Client behaves wrongly;
- During interventions, the monitoring is degraded as some service interactions are partially monitored, or in some case, not monitored at all;
- Moreover, the three views listed above are related with each other: a malfunction in a component typically results in some service(s) malfunction and finally impacts Users. The current NM B2B monitoring solution does not allow the navigation between these views, so that identifying the NM B2B services and Users impacted

by a component malfunction may turn to be expensive as it requires a deep NM B2B implementation knowledge.

In addition, it must be noted that there is a recurrent demand from the NM B2B Users to access the service and Client monitoring views.

3.3.5.2 Information about Past Incidents

Today, the NM B2B does not expose to the User any reporting regarding the past incidents and/or interruptions of service(s).

Providing the status of the NM B2B services in the past, e.g. at the time of some problem occurrence, would help the Client Software operators when investigating problems encountered on the Client side.

3.3.5.3 Monitoring Access

The User access to the monitoring is of utmost importance in case of NM B2B malfunction. For this reason, whatever NM B2B monitoring solution is proposed, it should be accessible even if the NM B2B services are not accessible, which is not the case today.

3.3.5.4 Health Check

Today, the NM B2B does not expose any kind of API health check. Consequently, the User is informed of the unavailability of a service only when it sends a request. The only mitigation option supported today consists in sending periodically lightweight requests, e.g. ReleaseRequest. However, the reception of a ReleaseReply only indicates that the NM B2B Platform is reachable. It does not provide any information regarding the availability of a precise service, e.g. Flight Preparation.

3.3.6 Reporting

The following issues have been identified affecting post-ops reporting and analytics capabilities:

- Both internal NM teams (i.e. CSO, OSM, B2B Office) and Users face challenges in obtaining detailed insights into API usage patterns, performance metrics, and error rates;
- Current reporting dashboards do not implement role-based access control to ensure that Users can only access the data they are authorised to see;
- Data related to Users, Clients, authorisation profiles, API usage patterns, etc., are currently available from different sources, which are not compiled today, so that the provision by NM of a comprehensive picture for both internal (issue investigations, auditing, global reporting, etc.) and Users' purposes in a timely and efficient manner is made difficult;
  Example: the "NM B2B Management Board" requires a status report on the integration of a given Stakeholder with the NM B2B Services in order to assess progress and possible consumption optimisation measures – e.g. information regarding the User's departments operating a set of B2B certificates, consuming a set of B2B services/operations, following certain consumption patterns, etc.

3.3.7 Maintenance

NM plans maintenance windows to deploy patches on the NM B2B as well as on the NM backend applications. Even though today NM communicates these planned maintenances to Users, the communication is partial: it indicates which applications are planned to be patched but does not give an accurate picture of the real User impact. For example, in case of an ETFMS planned maintenance, NM does not communicate the exhaustive list of NM B2B services that will not be available.

NM publishes planned maintenance windows 6 months in advance. However, to fix a recurrent problem, e.g. a service handles incorrectly some input values, it might happen that NM plans a patch maintenance window between one and two weeks in advance. NM notifies such patch maintenance windows, via AIM publication, only 3 days in advance. No clear information is exposed to the Users regarding the minimum delay between the notification and the occurrence of a planned maintenance.

In case of critical problem, e.g. a memory leak in some process, it happens that NM must realise some emergency maintenance intervention. Users are not notified about such unplanned maintenance window.

Consequently, the Client Software cannot distinguish between an occurrence of service unavailability due to a planned or emergency maintenance and one caused by a system failure: Users regularly complain about the unexpected errors that they receive during maintenance windows.

Moreover, because the NM B2B does not return today information regarding the status and expected duration of the interruption of service, Users call the NM CSO (and rightly so), whom in turn creates incidents accordingly, that often lead to costly and unnecessary problem investigations.

3.3.8 Disaster Recovery / Contingency

Today's NM B2B is a single large API that is deployed as a whole and is hosted on premises in the EUROCONTROL/Haren (Brussels) data centre.

A second data centre is located in France as a contingency site in case of Disaster Recovery (DR) scenario. This DR site hosts the same NM systems that are deployed in Haren, including the NM B2B infrastructure and data (to some extent), and therefore qualifies as a *"Hot"* Disaster Recovery (using the Cold-Warm-Hot definitions).

The contingency systems are idle and kept in stand-by and ready to take over operations in case of a disaster in the Brussels site.

The current DR scenario has some disadvantages:

System-oriented rather than Service-oriented

The DR scenario must define service continuity requirements for each service, expressed as Recovery Time Objective (RTO) and Recovery Point Objective (RPO), and not in terms of systems (i.e. by blindly replicating all the systems and data). Of course, services require systems, but the definition of what systems, processes, resources and data should come as a consequence of service continuity requirements.

The NM B2B is made of:

(1) *Essential Components*, that form the NM B2B "infrastructure" (e.g. IAM, API Gateways, message brokers, etc.)

(2) *Service Components*, i.e. systems and processes that provide services (e.g. F&F, IDL, CSST, etc.)

While the former are needed as to provide the B2B infrastructure, the latter shall be chosen according to each service's QoS.

Lack of clear definition of QoS in Contingency Mode

Today some of the services offered via NM B2B lack a clear and formal definition of their expected QoS in contingency mode. For example, for some services the required QoS in contingency may be exactly the same as in nominal circumstances, whereas other services may run in "degraded mode", and other services may not be available at all. However, there is no formal definition of what such concepts and policies are and it is often not clear to a User what to expect when NM runs in Contingency Mode.

Cost

Currently, the NM Contingency Site is almost a one-to-one replica of the Operational Site. The full deployment of all NM systems in the Contingency Site on-premise data centre, kept in stand-by, has a significant cost (infrastructure, physical resources and software licences).

Limited testing capability

The complexity of the current DR setup does not cater for frequent switch-over exercises to do full end-to-end testing, i.e. from NM B2B to Client Software.

3.3.9 Incident Management

The NM B2B provides multiple entry points for Users to report incidents.

- For operational emergencies: An email address, a phone number, and a web form. These channels of communication are available 24/7 and operated by the NM CSO team.
- For customer support requests: An email address, and a web form. These channels of communication are operated by the NM Customer Support team during business hours.
- For integration support requests: A web form. This channel of communication is operated by the NM B2B Office team during business hours.

Having different channels of communication exposed to the User implies that, in case of an incident, Users themselves need to judge what is the most appropriate support category to use. This is bound to cause misclassifications, which then need to be forwarded internally to the right team.

Furthermore, the lack of an integrated tooling used by the different teams makes the incident processing difficult and costly to track.

Furthermore, Users have no visibility on the status of their requests. They have to recontact the support team.

3.3.10 Problem Investigation

The problem investigation activity highly relies on the recorded logs.

The NM B2B records structured logs. Each log is a data structure with meaningful attributes. Such approach demonstrated to enable efficient and precise post-processing: log querying, log aggregation, etc.

The NM B2B logs are correlated in the sense that it is possible to identify all the logs that have been recorded during the processing of a single received request. The correlation however is not propagated until the backend system. Therefore, the

investigation of a problem that results from a backend system malfunction can be difficult.

The NM B2B systematically records all received inputs (request payloads) and all returned outputs (response payloads). Over time, the recording of this information also demonstrated to greatly facilitate the problem investigation. However, the P/S messages published to the Users are not recorded, which may be seen as a significant gap in the auditing requirements for the NM B2B.

Problem investigation also relies on the capability to replay the input messages received during a given period. This capability is extremely useful to investigate problems that arise on long periods of time (typically 1 day) and/or result from the combination of multiple causes. However, the replay capability is only partially supported. The investigation of long duration / multi-factor problems happens to be difficult and time consuming.

3.4 Business Scope

As indicated in introduction, this document does not only intend to provide an agreed view on the technical and service operations aspects, but also on the functional scope to be covered by the NM B2B in the future, and the way to do so.

This section intends to list in broad terms the NM B2B gaps and evolutions required to reach the functional goals expressed in the "business" ConOps documents.

The Business Scope remains indeed addressed in broad terms here as their corresponding elaborated requirements will be discussed with concerned Stakeholders in specific fora, and presented in specific documents (like the NM B2B Operational Deployment Plan).

3.4.1 iDL

The Network iDL ConOps describes the following high-level scope, which should all impact one way or the other the NM B2B evolutions:

- System merge for AIM and ATM data definition (basically, merge of EAD and CACD systems)
- Process for the collaborative iDL AIRAC Data (iDLAD) definition
- Airspace Utilisation Rules and Availability (AURA)
- Additional Airport Data (Airport Corner, etc.)
- MET & Natural Hazards
- Aircraft Performance
- Network Events
- Transponder Code Function (TCF) configuration
- Data Harmonisation
- Business Evolutions – Indirect Impact on iDL

Merge of EAD and CACD Systems

As explained in the iDL ConOps, the two systems will be merged into the iDL one, ensuring thereby the single and consistent view on the AIM/ATM data. But today there is no technical or API commonality between the NM B2B Airspace services (serving CACD data) and the AIMSL (serving EAD data), which is ambiguous and highly cost inefficient. It is obviously expected that the exposure of the Network iDL data would be merged too.

Process for the collaborative iDL AIRAC Data (iDLAD) definition

This is the most challenging item for the NM B2B coming from the iDL scope. Indeed, it is where the digitalisation process comes into force, enabling the required level of collaboration for the iDL AIRAC data. Doing so will require the development of new concepts in the first place, like Projects and Branches, and the NM B2B services supporting them, to upload data to elaboration branches, downloading them and properly notifying relevant Users about changes at elaboration time. Whereas the roles and responsibilities of the involved Stakeholders shall not change through this evolution, the interfaces shall necessarily have to change.

The same will apply with permanent branches, namely after integration, as publication, and for late changes in these permanent branches.

Airspace Utilisation Rules and Availability (AURA)

The AURA definitions cannot be proposed via NM B2B by the relevant Stakeholders today, and there exists no electronic process to handle those, as opposed to what iDL foresees today.

Additional Airport Data (Airport Corner, etc.)

Please refer to the iDL ConOps to get the list of "additional Airport Data" applications.

NM B2B requirements for these applications do not exist today.

MET & Natural Hazards

The NM B2B does not expose any MET data today.

Regarding natural hazards, the NM system offers the EVITA application, via HMI only, and limited to volcanic ash.

Another notable issue today is that flight plan revalidations do not take place against MET & natural hazards, and flight planners are therefore not informed accordingly of potential asynchronous flight plan rejections.

Aircraft Performance

Some Aircraft Performance data is exposed today via the NM B2B Airspace Structure service – this service might not be sufficient to meet the iDL requirements.

Network Events

The wide NET event information gathered by NM is only accessible to all via an HMI application, which is not related to any other HMI application (no navigation).

There exists no NM B2B service today to serve Network Events.

Transponder Code Function (TCF) configuration

There exists no NM B2B service today in connection with TCF.

Data Harmonisation

The data harmonisation issues mentioned in the iDL ConOps have essentially to do with the respect of existing rules, and the evolution of these rules. The iDL B2B needs of course to evolve with the agreed rules.

Business Evolutions – Indirect Impact on iDL

The iDL object type catalogue will obviously evolve in support to business evolutions in other iNM domains, e.g. Flight Planning, ATFCM, ASM, CRCOs, etc., will in turn will impact the iDL B2B API. Some of these evolutions are mentioned in the next section.

As mentioned above, business evolutions and their impact on the NM B2B developments will be detailed over time through the NM B2B Operational Deployment Plan.

3.4.2 Flight

The drivers for change are described in the Network 4DT ConOps. An extract of the "Transition Principles" section of the ConOps is reminded in the corresponding section 4.4.2 of this ConOps.

3.4.3 Flow

The list below refers to main changes described in the Flow ConOps, which are expected to impact the NM B2B APIs. This list is aimed at serving as first basis for

change classification to be addressed in the NM B2B Operational Deployment Plan; as seen in section 4.4.3, no solution is proposed today, not even in general terms.

- Harmonised restriction and traffic volume models
- AOP/NOP departure information integrated in eFPL
- Enhanced ATFM slot swapping, UDPP+ (enhancements of User-Driven Prioritisation Process)
- Dynamic Airspace Configurations (DAC)
- Collaborative framework managing delay constraints on arrivals
- Exchange of airport operational information with NM, and Integration of airport operational information into NM systems
- AOP/NOP departure information integrated in eFPL
- DPI and API provision without filed FPL
- Continuous monitoring of data exchange (with alerting service in case data quality is not sufficient for flow management activities)
- Enhanced planning systems for the management of DMAs
- Collaborative framework managing delay constraints on arrivals
- Enhanced local traffic complexity tools
- Meteorological information exchange
- Delegation of ATM services provision among ATSUs

3.4.4 Cross-Service Linking

NM B2B exposes today a wide panel of services. Yet it often does not provide an efficient way to combine these services in a simple way.

For example, a flight profile references aerodromes and points via their ICAO designators, but unfortunately no NM B2B service allows Client Software to retrieve the full details of an aerodrome or a point from its ICAO designator.

3.4.5 Services Only Supported via HMI

Many services and capabilities available via NM HMI applications (CHMI, NOP and NMP) are not available today via NM B2B. Therefore, Users cannot integrate these services and capabilities into their Client-side HMI. The list below is not exhaustive but gives a good idea of the main missing services/capabilities:

- Airspace data Create, Read, Update, Delete (CRUD) service:
  The airspace data CRUD service is exposed by the CHMI only.
  The current NM B2B Airspace API only supports the download of bulk airspace data. It does not expose NM B2B querying and write service interactions.
- RAD service:
  The RAD service enables the collaborative (National RAD Coordinators and NM RAD Team) elaboration and publication of the RAD.
  The RAD service is exposed by the NMP (HMI) only.
  No related NM B2B service is exposed.
- CAL service:
  The CAL service allows the Transponder Code Function (TCF) to manage and publish transponder codes.
  The CAL service is exposed by the NMP (HMI) only.
  No related NM B2B service is exposed.
- Crisis management service:
  The crisis management service is exposed by the NMP (HMI) and the NOP (HMI).
  No corresponding NM B2B service is exposed today.

- Network Event service:
  A Network Event is an activity (or set of activities) which may influence the Network for a given period. The Network Event service enables the gathering, edition and the publication of Network events.
  The Network Event service is exposed by the NOP (HMI) only.
  No related NM B2B service is exposed.
- Daily Network Plan service:
  The daily Network Plan service consists in the daily publication of the set of tactical ATFCM measures (e.g. activation of routing scenarios, regulations, etc.) prepared by the NM and other concerned partners (FAB, FMP) during the planning phase.
  The Daily Network Plan service is exposed by the NMP (HMI) and the NOP (HMI).
  No related NM B2B service is exposed.
- Headline News service:
  The Headline News service is exposed by the NMP (HMI) and the NOP (HMI). It enables the writing and publication of news about events that might impact the Network.
  No related NM B2B service is exposed.
- Call Sign Similarity Tool (CSST) service:
  The CSST allows aircraft operators to detect, then deconflict similar call signs in their flight schedules to reduce the incidence of call sign confusion events and improve the safety of the Network.
  The CSST service is exposed by the NOP (HMI) only.
  No related NM B2B service is exposed.
- Archived data access:
  ATM Stakeholders often need to refer to past information. For example, to build the plan for one day, an ANSP often needs to look at the same weekday in the previous week. Of course, each User can build and maintain a local history of data. However, this forces every ATM Stakeholder to implement the same solution, while it has been expressed (e.g. from ENAIRE) that it would be desirable that NM provides such functionality in a centralised manner, ensuring the correctness of the data.
  Archived data are mainly accessible via the CHMI.
  No NM B2B service exposes archived data.
- Other:
  There exist other HMI applications candidates for NM B2B, to be considered case by case. An example amongst others is MIRROR, a new EUROCONTROL flight visualisation tool enabling operational Stakeholders to better predict delays and take measures to mitigate their impact – improving flight efficiency –partially integrated in the NMP, but not in the NM B2B.

4 TO BE – Solutions

4.1 Introduction

This chapter presents the solutions to the problems identified in the previous chapter (AS-IS – Problem Statement), developed in accordance with the objectives stated at the beginning of this document.

It must be noted that the section structure of chapters 3 and 4 are identical, making it easier to match the proposed solutions with the identified problems.

4.2 Technical Aspects

4.2.1 Consistent B2B

The following needs have been identified:

- Ensure a high level of homogeneity and consistency between all B2B services exposed by NM;
- Share with the Users the main technical aspects that all NM B2B services should respect.

The future NM B2B will define a consistent set of standards, rules, and constraints to which all NM B2B services will conform: the “NM B2B Essentials”.

The “NM B2B Essentials” will address the following topics:

(1) Regulatory context;

(2) Service lifecycle and versioning;

(3) Platforms;

(4) Message exchange patterns;

(5) Exchange protocols;

(6) Service consumer identification;

(7) Security;

(8) Quality of service;

(9) Usage policy;

(10) API design guidelines.

4.2.2 Regulatory Context

4.2.2.1 General

The NM B2B shall comply with the regulatory requirements defined in section 3.2.2.1.

4.2.2.2 SWIM Compliance

The services exposed by the NM B2B need to be compliant with the SWIM Specifications mandated by the CP1 regulation.

To meet this regulatory constraint the NM B2B will incorporate the SWIM Compliance process as an integral part of its service design roadmap. Concretely this implies that:

- During service design the selection of interface protocols used to expose NM B2B services will be chosen in compliance with the latest version SWIM-TI Yellow Profile Interface Bindings Specification.
- The NM B2B Technical Infrastructure will be kept compliant with the latest version of the SWIM-TI Yellow Profile Infrastructure Capabilities Specification.
- The NM B2B will produce as a documentation artefact a service description compliant against the latest SWIM Service Description Specification.
- The NM B2B will produce as a documentation artefact a semantic traceability of its services conformant against the latest version of the SWIM Information Definition Specification.

4.2.3 Service Lifecycle and Versioning

4.2.3.1 Versioning Policy

The following needs have been identified regarding the versioning policy:

- Provide Users with clear expectations of the backward compatibility of a new version.
- Provide Users with clear expectations regarding the support duration of a deployed version;

NM B2B will use a two levels versioning:

1. **NM B2B Version**
   The version that identifies a deployment in the context of the NM B2B Operational Deployment Plan (see section 4.2.3.2). Each NM B2B version aggregates a collection of NM B2B Service Versions and associate them to a deployment and support lifecycle.

   A MAJOR.MINOR sequence identifies an NM B2B version:
   - MAJOR – identifies the lifecycle of the NM B2B version
   - MINOR – identifies the version increment in the context of the NM B2B version lifecycle

2. **NM B2B Service Version**
   The independent version of a service.

   Semantic versioning (see https://semver.org/spec/v2.0.0.html) will be used to version the Services (see section 4.2.11.2). Each Service version number will be expressed as MAJOR.MINOR.PATCH, where:
   - MAJOR - indicates a MAJOR version. A MAJOR version will contain backward incompatible changes with respect to the previous MAJOR version.
   - MINOR - indicates a MINOR version. A MINOR version will only contain backward compatible changes with respect to the MAJOR version. It can be used to expose new service interactions, with no impact on the existing ones.
   - PATCH - indicates a PATCH version. A PATCH version will contain backward compatible API bug fixes. A PATCH version, being a sub-version of a MINOR version, inherits the same backward compatibility features as MINOR versions.

   Each Service, e.g. Flight Preparation, will have its own versioning. Therefore, the User will be informed of the evolution of a Service version in the context of a new NM B2B Version, or new NM B2B Version Increment deployment. This information will help Users to decide on whether their Client Software needs to be upgraded.

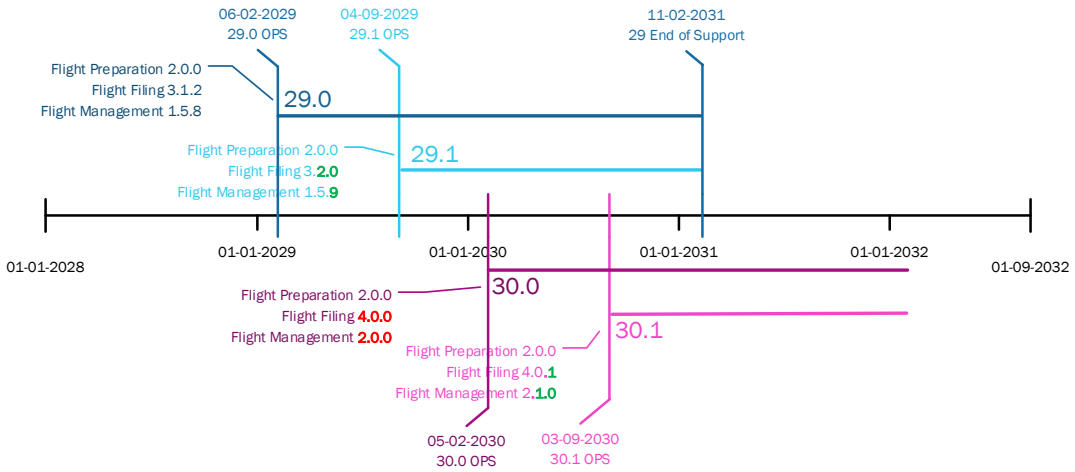

Figure 1: NM B2B Versioning

A NM B2B Version will specify the version of each Service that it aggregates. The above figure illustrates the following scenario:

- 06-02-2029 - NM B2B 29.0 (Version) OPS Deployment
  Contents:
  - Flight Preparation 2.0.0
  - Flight Filing 3.1.1
  - Flight Management 1.5.8

- 04-09-2029 - NM B2B 29.1 (Version Increment) OPS Deployment
  Contents:
  - Flight Preparation 2.0.0 (unchanged)
  - Flight Filing 3.**2.0** (MINOR)
  - Flight Management 1.5.**9** (PATCH)

- 05-02-2030 - NM B2B 30.0 (Version) OPS Deployment
  Contents:
  - Flight Preparation 2.0.0 (unchanged)
  - Flight Filing **4.0.0** (MAJOR)
  - Flight Management **2.0.0** (MAJOR)

- 03-09-2030 - NM B2B 30.1 (Version Increment) OPS Deployment
  Contents:
  - Flight Preparation 2.0.0 (unchanged)
  - Flight Filing 4.0.**1** (PATCH)
  - Flight Management 2.**1.0** (MINOR)

- 11-02-2031 – NM B2B 29 End of support
  - Flight Filing 3.x.x decommissioning
  - Flight Management 1.x.x decommissioning

To prevent any unnecessary software upgrades when a Service MINOR or PATCH version is deployed, each Service will be exposed under a URL that contains the Service name and its MAJOR version. For example, the version 3.1.1, and later the version 3.2.0 of the Flight Filing Service will both be exposed under the same URL: https://www.b2b.nm.eurocontrol.int/FlightFiling/v3. The NM B2B version will not be part of the Service URL.

4.2.3.2 Service Operational Deployment Plan

The solution presented below addresses the following needs:

- Early exposure of the future service API versions to Users;
- Users' involvement during the service API design phase;
- Predictable service lifecycle.

The deployment of a new NM B2B version will be announced in the context of an operational deployment plan. The duration of the plan will depend on the nature of the NM B2B Version: it might be announced a few months before the OPS deployment of an NM B2B Version increment, up to one year in advance, in the case of a new NM B2B Version.

The NM B2B Version Operational Deployment Plan will aggregate the following information:

- The NM B2B Version (or Version increment) OPS Deployment date
- The Service Operational Deployment Plans

Each Service Operational Deployment Plan will specify:

- The nature of the new version to be deployed: MAJOR, MINOR, PATCH, or none.
- A detailed schedule of the deployment plan (see below)
- The old major version(s) of the service that are planned to be decommissioned (old major version(s) can only be decommissioned in the context a new NM B2B Version, an old major version cannot be decommissioned in the context of an NM B2B Version increment).

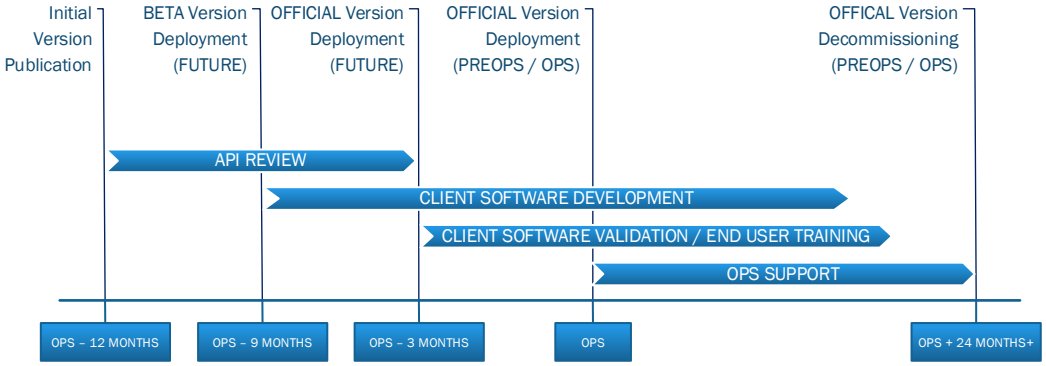

Figure 2: NM B2B Service Operational Deployment Plan

As illustrated by the figure above, the service operational deployment plan will specify the following elements:

NOTE: The periods specified in the figure above and in the text below are still under discussion and will be agreed upon in upcoming versions

Initial API Version Publication

Up to 12 months before the OPS deployment, the initial version of the service API is published. The initial API publication will provide necessary documentation enabling the planification of the client side efforts in terms of development, testing, training, and regulatory needs.

The API Review starts.

API Review

The period during which Users review the BETA version of the service API and provide feedback. Client Software development/prototyping can start. However, the service API is not deployed yet.

BETA Version Deployment on FUTURE Platform

Up to 9 months before OPS deployment, a BETA version of the service API is deployed on a FUTURE platform. The service API Review continues. Client Software development goes on. However, the API might still evolve in parallel according to the received feedback.

Client Software Development

The period during which Users develop and test their Client Software against the BETA version of the service API.

Until the OFFICIAL version deployment, this period is also used to gather final feedback on the service API and to fine-tune it if necessary.

This period extends after the OPS deployment and will terminate only with the decommissioning of the MAJOR version from the OPS platform. Practically, it should terminate as soon as a new MAJOR version of the service API is deployed on the OPS platform.

OFFICIAL Version Deployment on FUTURE Platform

Up to 3 months before OPS deployment, an OFFICIAL version of the service API is deployed on a FUTURE platform.

The service API Review is terminated. The service API version should not evolve anymore until its OPS deployment.

The Client Software Development continues.

Client Software Validation and NM B2B End User Training starts.

Client Software Validation and NM B2B End User Training

The period during which:

- Users validate their Client Software;
- Users organise the training of their End Users.

Like the Client Software Development, this phase officially terminates with the decommissioning of the MAJOR version from the OPS platform. Practically, it should terminate as soon as a new MAJOR version is deployed on the OPS platform.

OPS Deployment

The official version of the service API is deployed on the PREOPS and OPS platforms. From this date onwards, Clients start using the service in an operational context.

The OPS deployment date is set by the NM B2B Version Operational Plan, meaning that all new service versions of the NM B2B Version are deployed on OPS simultaneously.

OPS Support

The official version of the service API is exposed and supported on the PREOPS and OPS platforms.

Decommissioning

A MAJOR version of a service API can be decommissioned from the PREOPS and OPS platforms minimum 24 months after its OPS deployment and minimum 24 months

after the publication of the operational deployment plan of the next MAJOR version of the service API.

4.2.3.3 Urgent MAJOR Service API Deployment

In principle, the deployment of MAJOR (backward incompatible) Service versions will exclusively take place in the context of new (MAJOR) NM B2B version deployments. However, in very exceptional situations, e.g. an operational bug that requires an urgent fix, it might happen that a MAJOR Service version has to be deployed in the context of a (MINOR) NM B2B Version Increment deployment.

In such exceptional circumstances, NM will adopt the following approach:

- Change impact mitigation patterns will be used to ensure the continuity of the current MAJOR service version(s) support. As explained in section 4.2.11.7, these mitigation patterns will rely on the usage on “weakly typed” data structures. A new MINOR or PATCH version of the impacted service will be deployed.
- Simultaneously, a new “strictly typed” MAJOR version of the impacted service will be deployed. The new MAJOR service version will inherit the lifecycle of the version that it corrects.
- A strong effort of communication will be made to inform Users about the impacted interactions, with the objective of giving them the elements to decide if they remain on the former MAJOR version or move to the new one.

It should be noted that, given the service operational deployment plan exposed above, such a bug has virtually no chance to go unnoticed till operational deployment.

4.2.3.4 Support of Multiple Service MAJOR Versions

To allow Users to schedule the upgrade of their Client Software, the NM B2B needs to support simultaneously multiple MAJOR versions of the services that evolve in a backward incompatible manner.

Considering the pattern where future versions will be deployed much earlier, the transition period between two consecutive MAJOR versions of a service will be of at least 12 months.

4.2.3.5 NM B2B Version Publication and Deployment Frequency

As today, a new NM B2B version will be published on a yearly basis.

However, to support a shorter deployment lifecycle for fully backward compatible changes, several NM B2B version increments, containing new services, and/or service MINOR versions, might be published during the year.

4.2.4 Platforms

The solution presented below addresses the following needs:

- Unique OPS platform;
- Isolated development environment for Client Software, supporting automated testing;

- Early exposure of future versions in non-OPS platform(s);
- Protection from unfair usage of the non-OPS platform(s), e.g. using a non-OPS platform to access OPS data in a production context.

4.2.4.1 OPS Platform

The NM B2B will support operations, as today, via the OPS platform.

The OPS platform will expose the operational services in normal and in contingency mode.

The OPS platform will give access to all operational data, including those data that are being elaborated (e.g. future AIRAC data).

The OPS platform will be supported 24/7.

4.2.4.2 Non-Operational Platforms

As today, the NM B2B will also support service exploration, Client Software testing, or OPS validation thanks to non-operational platforms.

On a non-operational platform, the User will have the possibility to work in isolation from other Users. Hence, he will have the possibility to execute automated tests without risking interactions with the tests being performed by other Users.

A non-operational platform will be characterised by the following properties:

1) Supported Versions

   The list of the NM B2B versions supported by the platform.

   A platform that supports the same versions as the OPS platform will allow Users to validate their Client Software before using it to access the OPS platform.

   A platform that supports future versions will typically be used to gather User feedback about future evolutions of the services and to allow Users to develop and test their Client Software before the OPS deployment of these future versions.

2) Enabled Services and Capabilities

   It happened in the past that the access to some deployed service (service exposed by a deployed version) was disabled on the OPS platform. For example, the RADRestrictionActivationsUpdateRequest/Reply was deployed in April 2023 as part of NM B2B 27.0 but should remain disabled until January 2025.

   It will be possible, on a non-operational platform, to specify which services and capabilities are enabled, independently of their OPS enablement status.

   The list of enabled services and capabilities will be communicated to the B2B users.

3) Data Provisioning Policy

   The provision of data to a non-operational platform is essential to support the development and testing activities of the Users. However, there is no single data provisioning policy that would cover all test cases.

   To validate a change in a Client Software before using it on OPS, the User might decide to compare the respective behaviours of the modified Client Software on a non-operational platform and the current Client Software on the OPS platform.

The alignment of the non-operational data to the OPS one is a prerequisite for such a test.

Another User might rather focus on automated regression tests and could prefer to always execute the same tests against the same data, for example a "reference day of operations". Such a "reference day of operations" would ensure that known data (flight plans, flight updates, measures, etc.) are input in the system at known time in the day.

NM will associate to each non-operational platform a data provisioning policy. Such a policy will indicate which data are aligned with the OPS platform, or with another source, e.g. a reference day of operations.

4) Usage Policy

To prevent malicious exploitation of OPS data alignment on a non-operational platform, the NM B2B will assign to NM B2B End Users, distinct usage policies to distinct non-operational platforms. For example, on a platform of which data are aligned with the OPS platform, some specific load quotas could seriously limit the number of requests and/or the consumed bandwidth on a one day period while preserving an OPS-like usage on shorter periods.

5) Support

Depending on their criticality, non-operational platforms will not benefit from the same support. The NM B2B will clearly specify, per platform, the kind of support that the NM B2B User can expect.

For each non-operational platform, the NM B2B will publish the availability periods. Per availability period, it will publish the following information:

- Purpose of the platform;
- Supported versions;
- Enabled services and capabilities;
- Data provisioning policy;
- Usage policy;
- Support.

4.2.4.3 PREOPS Platforms

A PREOPS platform will be a non-operational platform, dedicated to the validation of the Client Software, by the NM B2B Users, before accessing the OPS platform.

A PREOPS platform will expose the same versions as the OPS platform.

A PREOPS platform will enable the same services and capabilities as the OPS platform.

A PREOPS platform will be running 24/7 and supported Office Hours.

To support the different test approaches, several PREOPS platforms will be exposed. For example, one PREOPS platform might ensure the best possible data alignment with the OPS platform, whereas another one might rather daily repeat the same "reference day of operations".

4.2.4.4 FUTURE Platforms

A FUTURE platform will be a non-operational platform, dedicated to the exposure of a future NM B2B (MAJOR or MINOR) version.

A FUTURE platform will be running 24/7 and supported Office Hours.

Such a platform will allow the NM B2B Users to adapt and/or develop their Client Software before the OPS deployment of the B2B version. Additionally, the platform will offer a feedback mechanism, enabling the NM B2B Users to report insights and suggestions for improving the quality of the services prior to their deployment on OPS.

4.2.5 Message Exchange Patterns

4.2.5.1 Supported Patterns

The "NM B2B Essentials" will support at least the following Message Exchange Patterns:

Synchronous Request/Reply (S-R/R)

1) The Client sends a request
2) The NM B2B returns a synchronous reply

Asynchronous Request/Reply (A-R/R)

1) The Client sends a request
2) The NM B2B returns a synchronous request receipt reply
3) The NM B2B publishes an asynchronous reply message

Event Publish/Subscribe (E-P/S)

1) The Client subscribes to a topic
2) The NM B2B publishes messages when topic events occur
3) Note: The E-P/S message exchange pattern will be homogeneously supported across the NM B2B API. The subscription synchronisation (which allows the user to receive the topic messages, recently published, but anterior to the subscription activation) will be supported by all NM B2B E-P/S topics.

Scheduled Publish/Subscribe (S-P/S)

1) The Client subscribes to a topic with a given schedule (e.g. the Client subscribes to the daily publication of the ATFCM situation at 06:00, 12:00 and 18:00)
2) The NM B2B publishes messages according to the subscribed schedule

File Download

1) The Client sends a download request
2) The NM B2B returns a file location from which the user can download the file

File Upload

1) The Client sends an upload request (including a file)
2) The NM B2B uploads the file

4.2.5.2 Guidelines

The "NM B2B Essentials" will provide guidelines for NM B2B service designers. These guidelines will define decision criteria regarding the pattern(s) under which a new service interaction shall be exposed. The following non-exhaustive list of criteria is foreseen:

- Processing duration: asynchronous patterns will be recommended for service interactions that require a long processing duration;

- Data dynamicity: publish subscribe patterns will be recommended for the retrieval of data that evolve frequently;
- Service interaction criticality: asynchronous patterns will be recommended for critical service, e.g. Flight Filing;
- Data volume: asynchronous patterns will be recommended for the retrieval of large amounts of data.

These criteria will be shared with the NM B2B Users.

The "NM B2B Essentials" will also provide guidelines to help the NM B2B Users selecting the right pattern when several possibilities are offered by the NM B2B.

4.2.6 Exchange Protocols

The following needs are identified generically for the selection of exchange protocols:

(1) SWIM Compliance: The services exposed by the NM B2B need to be compliant with the SWIM Specifications mandated by the CP1 regulation. Compliance with the SWIM-TI Yellow Profile significantly constraints the space of exchange protocols. The selection of exchange protocols supported by the NM B2B needs to conform with the SWIM-TI Yellow Profile Interface Bindings Specification.

It must be noted that future proofing is not only aimed at avoiding technical debt but also at protecting the investment from all – ensuring SWIM compliance definitely helps with that latter concern.

(2) Contract Driven APIs: The NM B2B needs to prioritise exchange protocols that enable the definition of contract driven APIs. Given the nature of the information exchanges enabled by the NM B2B safety and correctness play a crucial role in its API design principles, contract driven APIs facilitate correct client implementation.

(3) Future Proofing: The NM B2B needs to ensure its selection of exchange protocols remains future proof. Exchange protocols supported by the NM B2B must benefit from a wide support through an ample selection of programming languages, covering both established programming languages (C, C++, C#, Java…) and languages that have become popular more recently (Rust, Go, Python…). This can ensure new Client Software implementations are unconstrained in their selection of technology stack.

(4) Support for the XMs: The global standards for exchange of flight (FIXM) and aeronautical information (AIXM) only have XML data models as their physical instantiation, at the time of writing. Therefore, the NM B2B needs to select exchange protocols that support the exchange of XML payloads.

(5) Standard Exchange Protocols: The NM B2B needs to select exchange protocols that have been standardised by recognised international standardisation bodies. Selection of Standard exchange protocols prevents vendor lock-in.

4.2.6.2 Synchronous Exchanges

Given the needs and constraints identified, the only exchange protocol that meets these is HTTP/1.1. In particular:

- XML over HTTP/1.1 remains a valid solution that meets all needs identified.
- While SOAP clearly fails the future-proofing criteria, it may still be offered optionally as a convenience solution for legacy programming languages.

The NM B2B will continue to observe the evolution of the SWIM-TI Yellow Profile and reassess its technological selection in accordance with the needs identified and the needs expressed by its users.

4.2.6.3 Asynchronous Exchanges

Given the needs and constraints identified, the only exchange protocol that meets these needs remains AMQP 1.0.

The NM B2B will continue to observe the evolution of the SWIM-TI Yellow Profile and reassess its technological selection in accordance with the needs identified and the needs expressed by its users.

4.2.6.4 Data Exchange Formats

Given the needs and constraints identified, XML remains as an unavoidable serialisation format for the exchange of flight and aeronautical information. Other types of exchanges may be unconstrained by this criterion and favour other serialisation formats (e.g., JSON, Protobuf…) if these are defined and recognised as a Standard.

4.2.7 Service Consumer Identification

The following needs have been identified for the Service Consumer Identification solution:

(1) Identifies the Customer Organisation: The Service Consumer Identity model must be flexible enough to allow the identification of the Customer Organisation at the granularity desired (e.g. Organisation, Unit, Department…).

(2) Identifies the End User: The Service Consumer Identity model must be flexible enough to allow the identification of the End User of the NM B2B from a business perspective at the granularity desired (e.g. function, role, operator...).

(3) Identifies the Client Software: The Service Consumer Identity model must be flexible enough to allow the identification of the Client Software at the granularity desired (e.g. application name, version, site, instance, IP…).

(4) Available during runtime by the NM B2B: The NM B2B needs access to the Service Consumer Identity model during runtime.

(5) Common view: A common view of the Service Consumer identity will be available across different applications and teams.

(6) Credential agnostic: The Service Consumer Identity model will be agnostic of the credentials. It will be possible to flexibly configure different types of credentials to the same User identity. For example, the same End User identity may be linked to a user/password credential, token-based credential, X.509 certificate or combinations of them as needed.

The NM B2B will select an Identity Provision solution that meets the needs and constraints defined above.

4.2.8 Security

4.2.8.1 Protocols

The following needs have been identified for the selection of the security protocols:

(1) The selection of security protocols needs to be conformant with the Service Interface Bindings established in the SWIM-TI Yellow Profile.

(2) The selection of cryptographic algorithms and key-sizes needs to be conformant with the SWIM-TI Yellow Profile requirements.

Based on the needs identified the selection of security protocols is sufficiently constrained. The NM B2B will continue relying on Transport Layer Security (TLS) v1.2 or higher to ensure conformance with the SWIM-TI Yellow Profile. The NM B2B selection of cryptographic algorithms and key-sizes will conform to applicable European recommendations.

4.2.8.2 Network

The following needs have been identified based on the problem statement:

(1) The NM B2B needs to introduce the necessary mitigation measures to protect its infrastructure against DDoS attacks in its public Internet endpoints.

(2) The NM B2B will keep supporting its PENS endpoints to satisfy the regulatory needs of Customer Organisations, and as a fallback network providing a complete mitigation against DDoS attacks.

Based on the needs identified above, the following solutions will be considered:

The NM B2B will apply a defence in-depth approach to protect its public Internet endpoints by combining a firewall with DDoS protection solutions either at the TCP/IP layer or application layer, if needed.

The NM B2B will continue to provide its services via PENS, as this network offers inherent protection against DDoS attacks.

4.2.8.3 Credentials and Authentication

The following needs are identified based on the problem statement:

(1) The authentication solution needs to be able to flexibly customise the appropriate credential or combination of credentials to authenticate the end-user.

(2) The authentication solution needs to be able to authenticate the end-user behind a web platform.

(3) The authentication solution needs to be able to passthrough a CDN while being able to securely authenticate the end user.

Based on the identified needs, the authentication solution of the NM B2B will support authentication with multiple types of credentials, which may be combined between them to ensure that the user can be identified at the right level of granularity.

(1) X.509 certificates will be used to authenticate the machine-to-machine connection with the NM B2B API. A single certificate could be used for an entire organization, significantly reducing the overhead costs associated to their management while benefiting from the very high security guarantees that certificates provide.

(2) Username/Password will be used for web-based authentication to the administration portal which a user may use to manage its account and retrieve an API token.

(3) Token-based authentication will be used for fine-grained authentication of the end-user of the NM B2B API.

The particular combination of credentials that will be used to authenticate a user will be configurable and left as a runtime option. For instance, large Stakeholders may have many different internal end-users and Client Software instances. The NM B2B may use one X.509 certificate for the organization used across all different instances and applications and as many tokens as needed to identify the end-user or instance performing the query. This combination strikes a right balance between keeping very high security guarantees provided by the X.509 certificate while benefiting from the simplified management of tokens, which can be easily generated, refreshed, and deleted to support as many end-users as needed.

This flexibility also enables the NM B2B to support web-based platforms. The provider of the web-based platform is authenticated via an X.509 associated to its organization while the end-users of the platform are authenticated via token-based authentication. Unlike the ANUId the token is non-spoofable, secret, and can be refreshed often to increase security.

Flexibly combining two authenticators like described above also can enable TLS termination at a Content Delivery Network (CDN) as the NM B2B will still have an authenticator exchange at message layer (the token) which it can use to verify the user identity securely. This solution can be useful to mitigate potential DDoS attacks on the public Internet endpoint of the NM B2B.

In essence, introducing a message layer credential (token-based authentication) can provide the flexibility needed to ensure that the NM B2B can identify the user identity with as much granularity as needed while keeping the overhead associated with X.509 client certificates under control.

4.2.8.4 Authorization

The NM B2B will implement an authorization mechanism that satisfies the following requirements:

(1) The authorization assigned to a credential will be manageable during runtime by the NM B2B Office, without requiring a new software deployment to change the authorization of a user.

(2) The NM B2B will enforce authorization to its Request/Reply interactions at the following levels of granularity, at a minimum:

a) Based on the type of request;

b) Based on assertions on the payload of the request;

c) Based on assertions on the state of the accessed resources.

(3) The NM B2B will enforce authorization controls to its Publish/Subscribe interactions at the following levels of granularity, at a minimum:

a) Based on the topic (e.g., the authorization will check if a User can subscribe to a topic).

b) Based on assertions on the payload of the message publication. (e.g., only messages that match the assertion will be published to the User).

c) Based on assertions on the message queue (e.g., the authorization will check if a User can connect to a particular queue).

The NM B2B will select an Authorization Server solution that meets the aforementioned needs.

4.2.9 Quality of Service

4.2.9.1 Performance

The following needs have been identified for the performance Quality of Service.

(1) Observability: Users need real time monitoring of the response times experienced by its services.

(2) Statistics: Users need access to the statistical figures experienced by the NM B2B services on a predefined set of Service Level Indicators during a representative past time interval (e.g., 3 months, 6 months, 1 year). Statistics shall include traffic statistics (bandwidth, throughput).

(3) Target figures: Users have expressed the need to define target figures for the response times of the NM B2B services.

(4) Critical services: The NM B2B needs to be able to meet the minimum response times figures required for these services.

To achieve the performance needs identified, the NM B2B will make available through an API and through a web interface (see section 4.3.5) the following aspects of the Performance Quality of Service:

- Real time monitoring of the response times observed by the NM B2B services;
- Response time statistics of the NM B2B Services during a representative reference period;
- Reference target values of the response time.

To ensure the target values of the response time are met, the NM B2B may introduce various techniques to reduce response times, particularly when handling large payloads.

- Caching: Certain queries return a response that remains static for a sufficient amount of time to benefit from caching. In such cases the NM B2B may introduce cached responses at an API gateway or CDN level, removing load from the systems and reducing response times.
- Load Balancing: Spikes in response times may be due to overbooked resources in the NM B2B backend systems. When this is identified as the source of spikes in the response time of a service, introducing load balancers and horizontally scaling across workers may alleviate the underlying issue.
- Vertical scalability: Complex queries require large computational resources and may not always be parallelisable. In such a case, profiling the execution path and identifying whether additional hardware resources are needed can alleviate the problem.
- Elasticity: Demand peaks may require dynamically scaling the available resources either horizontally or vertically. Elastic scalability could be used to tackle seasonal load and demand spikes.

The NM B2B will profile the system performance to identify the root causes of performance degradation and apply the right combination of techniques to mitigate them.

4.2.9.2 Availability and Reliability

The following needs have been identified for the availability and reliability Qualities of Service.

(1) Observability: The NM B2B users need real time monitoring of the availability status experienced by its services.

(2) Statistics: The NM B2B users need access to the statistical figures experienced by the NM B2B services on a predefined set of Service Level Indicators during a representative past time interval (e.g., 3 months, 6 months, 1 year).

(3) Target figures: The NM B2B users have expressed the need to define target figures for the availability and reliability Service Level Indicators.

(4) Critical services: The NM B2B needs to be able to meet the minimum availability and reliability figures required for these services.

To meet the aforementioned needs, the NM B2B will make available through an API and through a web interface (see section 4.3.5) the following aspects of the Availability Quality of Service:

- Real time monitoring of the service availability.
- Statistics observed during a representative reference period of the following Service Level Indicators by the NM B2B services:
  - Availability:
    - Uptime with and without planned maintenance windows.
    - Time To Repair.
  - Reliability:
    - Time Between Failures.
- Reference target values of the SLIs.

In addition, to ensure the target SLIs are met, the NM B2B will introduce the necessary redundancies in its architecture to minimise single points of failure.

4.2.9.3 Scalability

The following needs have been identified for the scalability Quality of Service.

(1) The NM B2B needs to be able to scale to keep with the increased demand of its services driven by the nominal growth trends driven by increased digitalisation of ATM and the adoption mandated by the CP1.

To achieve the scalability needs identified the NM B2B will implement the following solutions:

- Minimise Bottlenecks: Identify and minimise single points of failure that act as bottlenecks in the NM B2B architecture.
- Stateless design: Prioritize a stateless design to enable horizontal scalability and load balancing.
- Elasticity: Demand peaks may require dynamically scaling the available resources either horizontally or vertically. Elastic scalability could be used to tackle seasonal load and demand spikes.

4.2.9.4 Security

The following needs are identified for the Security Quality of Service of the information exchanges.

(1) The NM B2B will continue to ensure the confidentiality and integrity of its information exchanges at transport layer.

More explicitly, neither the non-repudiation of the exchanges nor message-layer confidentiality or integrity are identified as a need.

Therefore, the NM B2B will continue relying on TLSv1.2 (or higher) which guarantees the confidentiality and integrity of the information exchanges at the transport layer.

4.2.10 Usage Policy

The following needs have been identified for the Usage Policy solution:

- Ensure an equitable access to the Services to all End Users;
- Protect the NM B2B against malfunctioning Client Software;
- Inform the User about its recent usage.

To ensure an equitable access, the NM B2B will, as today, enforce the compliance with load quotas. The current quotas should remain in application:

- Bandwidth consumption per sliding time interval;
- Request count per sliding time interval;
- Simultaneous request count.

To protect itself against incorrect requests, the NM B2B will also enforce the compliance with quality criteria, e.g. rate of incorrect requests per sliding time interval. Note that the automated estimation of the quality of the received requests will allow each Customer Organisation to validate at any time (and on any platform) the level of quality of its Client Software and/or End Users.

The NM B2B will support flexible quotas enforcement at Client Software, Customer Organisation, and End User levels. For example, it will be possible to assign load quotas to End Users, independently of the Client Software that they use to connect the NM B2B and/or independently of the Customer Organisation that proxies the NM B2B. It might also be possible to enforce quality criteria to a Customer Organisation and/or to its End Users.

In case of quota exceeded, the NM B2B will first warn the Customer Organisation and/or End User. In a second time, if no correction is observed, the NM B2B might temporarily suspend the access, until its usage metrics come back to acceptable values.

Each Customer Organisation will be informed about its own status regarding the usage policy but also about the status of its Client Software and End Users.

4.2.11 API Design Guidelines

4.2.11.1 Model Centric API

All NM B2B services will be designed and documented through a model centric approach with the purpose of:

- Harmonising the NM B2B artefacts: documentation and API definition documents such as OpenAPI documents, XSD or JSON schemas, etc.;
- Preserving a technological agnostic documentation, enabling the future adoption of new exchange protocols or new exchange formats;
- Ensuring a strict adequacy between the exposed services, the documentation, and the implementation;

- Ensuring a fine traceability of the API changes and automating the generation of the release notes.

4.2.11.2 Services Organisation

The proposed solution addresses the following needs:

- More flexible and meaningful organisation of the services;
- Simplified Client Software development, avoiding the download of unnecessary dependencies.

Flat service organisation

The NM B2B will drop the strict service groups / services organisation and will adopt a flat organisation of the services. The main objectives of this change can be summarised as follows:

- Simplified Client Software development
  Client Software that uses a unique service will depend on a lighter OpenAPI document and/or XSD or JSON schema.
- Provide a more flexible categorisation of the services
  The NM B2B will allow to tag a service. Therefore, it will be possible to associate a service with several tags. For example, the Filing Service (today included in the FF-ICE service group) will be marked as a Flight and as an FF-ICE service.
  This categorisation will also be used to associate the services to the business use case(s) that they support.
- Align to the SWIM registry organisation
  The SWIM registry already adopted such a flat organisation.

Refined service / service interaction granularity

To improve the usability of the NM B2B, a strong effort will be made to associate a more clear and precise scope to each service. This clarification aims at improving the usability of the API, facilitating the management of the access rights, and improving the quality of the post-ops reporting.

For example, the current Airspace Availability service will be split in two services:

- Airspace Management: Intended for Airspace Management Cells (AMC) for booking or releasing restricted airspaces or conditional routes via the submission of AUP/UUP;
- Airspace Availability: Intended for airspace users to retrieve the opening and closures of restricted airspaces, conditional routes, and restriction activations, that result from the consolidation of the AMC's input into an EAUP/EUUP.

This effort will also target the interactions that today mix several usages, for example, the FlightUpdate and EHelpdeskTicket Requests/Replies.

Modular exchange model

The exchange model contains the definition of the datatypes used to compose the exchanged messages (including the message datatypes themselves).

A datatype can be used by:

- one service interaction only;
- several service interactions of the same service;
- several service interactions belonging to distinct services.

Datatype definitions will be organised in packages (or modules). The granularity of the NM B2B datatype packages will realise the right balance between:

- The legitimate demand of the users to not pull useless datatypes when using only a few interactions of a service. Pulling unnecessary datatypes results in a huge number of useless generated lines of code.
- The risk of package proliferation that can lead to a complex dependency management for the Users and for NM.

The exchange model will be organised as an oriented graph of datatype packages, meaning that any datatype package will possibly depend on other datatype packages but no bi-directional, and more generally no cyclic dependency, will be allowed.

The datatype package graph is not yet available. However, this graph will be extensible to comply, along the time, with the need to incorporate new services in the NM B2B. It should be articulated around:

- One *Common* datatype package
  The *Common* datatype package will encapsulate the most used datatypes. The following non-exhaustive list illustrates the common package contents:
  - Messaging support datatypes, e.g. Request, Reply, PSMessage, etc.
  - Time related datatypes, e.g. Date, Time, Duration, etc.
  - Geographical datatypes, e.g. Latitude, Longitude, etc.

- *Resource* datatype packages
  A *Resource* datatype package will encapsulate the datatypes related to one or a (logical) group of resource types. For example, the *Measures* datatype package will contain all the datatypes related to regulations, regulation proposals, and re-routings.

- *Service* datatype packages
  A *Service* datatype package will encapsulate the datatypes that are specific to a service. Hence, there will be one service package per service. Such a datatype package will contain at least all message data types (requests, replies and P/S messages).

- *Third Party* datatype packages
  A *Third Party* datatype package will encapsulates the datatypes that ensure the integration of the third party datatypes, e.g. AIXM or FIXM, within the NM B2B exchange model.

4.2.11.3 API Design Paradigms

The following needs are identified for the selection of API design paradigms in the NM B2B APIs:

(1) Usability: NM B2B APIs need to be expressive and easy to use, fulfilling user needs.

(2) Maintainability: NM B2B APIs need to be maintainable, and easy to evolve as new functional needs arise. This consideration includes both the server and client sides.

(3) Homogeneity: A homogeneous look and feel across the NM B2B APIs improves usability and facilitates development work.

(4) User Feedback: User feedback is critical to meet user needs. The NM B2B needs to involve user feedback early-on through the design phase to ensure API design is aligned with user needs.

To meet these needs the following high-level solutions are proposed:

The NM B2B will develop API design guidelines that help service designers meet the needs identified above, in the selection of API design paradigms.

For instance, these design guidelines will prescribe the adoption of REST APIs as a service design paradigm for Request/Reply interactions. REST APIs will help us achieve our identified needs for usability, maintainability, and user feedback much better than the existing SOAP/POX model, while remaining compliant with the SWIM-TI Yellow Profile.

To this end we aim to target Richardson's Maturity Model level 2 which provides a good balance between usability and maintainability. And we will leverage HTTP's content-negotiation to support multiple data serialization formats where needed. This will allow the NM B2B to support XML payloads where does are required by external constraints (e.g. support for FIXM, AIXM, WXXM…) but gives us freedom to also support JSON format if these become available. Leaving the choice of which one to use for our stakeholders.

The NM B2B will also involve user feedback early-on in the design process of a service to ensure the design meets users' needs.

4.2.11.4 Naming Conventions

To harmonise the design of the API, and to facilitate its usage, the "NM B2B Essentials" will define, and share with the Users, naming guidelines.

The naming guidelines aim at addressing the following aspects:

- Case policy, including a consistent treatment of the acronyms;
- Request, reply, and operation naming, clarifying the form (verb or noun), and the position of the various elements that compose their respective names;
- Attribute or choice naming, clarifying for example which of `asmScenario`, `asmScenarioReference`, `asmScenarioUuid`, or `asmScenarioUUID`, should be the name of an attribute that contains a reference (expressed as a UUID) to an ASM scenario.

4.2.11.5 Error Reporting

The following needs have been identified for the Error Reporting solution:

- Enable and facilitate the automation of the error processing by the Client Software;
- Provide a detailed documentation of the reported errors to the Users.

The NM B2B will use a clear, consistent, and homogeneous error model. All NM B2B Requests/Replies will report errors according to this model.

The error model will distinguish two categories of error types:

- Standard errors: errors that are possibly returned by any Request/Reply;
- Specific errors: errors that are possibly returned by a specific Request/Reply.

The documentation of each Request/Reply will indicate:

- The exhaustive list of specific error types that it can raise;

- The exhaustive list of specific warning (error types) that it can raise.

Each error type (standard or specific) will be documented as follows:

- Meaning and detection condition of such an error;
- Error parameter list, including, the documentation and processing instructions of each parameter;
- Default retry policy.

At the current stage of analysis, the following standard error types have been identified (this list may evolve as the NM B2B solution is refined):

- INTERNAL_ERROR: The request processing failed due to an internal error.
- SYSTEM_OVERLOAD: The request processing failed due to some temporary overload of the system.
- ACCESS_DISABLED: The service/resource access is disabled for all users.
- ACCESS_DENIED: The service/resource access is not authorised to the user.
- USAGE_REJECTED: The request could not be processed due to a violation of the usage policy.
- MALFORMED_REQUEST: The request could not be processed due to some invalid syntax.
- INVALID_REQUEST: The request is well-formed but could not be processed due to some violated request constraints.

Any returned reply will contain a summary status with possible values:

- OK: the request processing was successful;
- Any standard error type identifier (INTERNAL_ERROR, SYSTEM_OVERLOAD, etc.): the request processing failed due to some standard error;
- REQUEST_SCECIFIC_ERROR: the request processing failed due to some request specific error(s).

To facilitate the automated processing, the summary status will be expressed as an HTTP status: 200 for OK, 500 for INTERNAL_ERROR, 503 for SYSTEM_OVERLAOD, etc.

In case of successful processing, the reply might contain a list of warnings.

In case of error, the reply will contain:

- The list of errors that were detected during the processing.
  The objective is to reduce the number of consecutive retries that might result from returning only the “first discovered error”. Unfortunately, an error might hide subsequent errors by preventing the execution of deeper validations. Therefore, when a request contains several errors, the NM B2B will return an “as exhaustive as possible” error list.
- A description of the retry policy that should be implemented by the Client. The retry policy will respond to the following questions:
  - Shall the Client re-submit the request or not?
  - If yes, how much amount of time shall the Client wait before re-submitting?
  - How many times should it re-submit?

  The retry policy recommendation will be computed dynamically, based on the detected error(s) and the Client Software / End User recent activity.

Each reported error will contain:

- A structured description;

- A textual description.

The structured description aims at enabling the automated processing by the Client Software. It will contain:

- Error type: The error type identifies the nature of the error. It also indicates to the Client Software how to interpret the error parameters.
- Error parameters: The error parameters provide additional information about the error, e.g. the path, in the request, of an object reference that could not be found.

The textual description aims at providing an informal description of the error to the User.

4.2.11.6 Usage of Message Properties

Message properties are key-value pairs that are added to the message being exchanged to facilitate its processing by the receiver (e.g. routing).

Message properties are particularly useful in asynchronous messages (e.g. publish/subscribe pattern) when the client software may need to dispatch the received messages to different processes based on some properties.

> The NM B2B makes use of message properties in its AMQP messages (AMQP Header properties, AMQP Message properties and Application Properties) to convey useful information about the nature of the message (e.g. the type of message) but does not provide sufficient information about the content of the message to support routing decisions, or when it does, it is via an informal way. For example, the Application Property NM_BUSINESS_ID is documented as follows:*This is a more humanly readable identifier that provides information about the nature of the message. For example, for a FlightDataMessage it can look like "ifplId:AA00311500 acId:AFR1144 adep:LFPG ades:UUEE divertedAdes:null eobt:2017-09-11 17:05 evt:CNC". It was introduced for NM's internal use. However, it may be useful for logging purposes but the client application should not parse it because the format may change at NM's discretion*.

The NM B2B will introduce new message properties to support message routing (to be decided whether to use standard property such as "subject" or custom property such as NM_SUBJECT). The values of such properties will be formalized and duly documented. As an example, it is foreseen to add the following properties: service name, service namespace.

Such properties will not be limited only to AMQP messages but might prove useful also in HTTP responses.

4.2.11.7 Mitigating Impact of Changes

Mitigating unplanned changes by means of weakly typed structures, e.g. using `OTHER:…` values in loose enumerations, will never be totally satisfactory. However, such a solution demonstrated its utility in the past, e.g. by allowing a smooth introduction of new `FlightEventType` values.

The NM B2B will continue to support a concept of loose enumeration. However, it is understood that the implementation pattern shall better integrate with the usual XML schema parsers / code generation tools, keeping in mind that in some longer term future XML might disappear from the technological horizon. The pattern that will be used is not decided yet. The following options are considered, for discussion:

- Current AIXM like pattern
  A loose enumeration is modelled as a union of:
  - a strict enumeration;
  - a string prefixed by `OTHER:`.
- FIXM like pattern
  A loose enumeration is modelled as a choice between two elements:
  - a strict enumeration;
  - a string.
- Combined pattern
  A loose enumeration is modelled as a pair of elements:
  - a strict enumeration containing an `OTHER` value;
  - a string whose presence is conditioned by the usage of the `OTHER` value.

In the future, he NM B2B will support additional mitigation patterns. For example, it could declare in each class a list of key-value pairs that could serve as placeholder to transport missing attribute values. Alternatively, the NM B2B could generalise, like FIXM, the support for data type extensions. At the stage of writing this document, no decision is taken yet.

In any case, the use of such mitigation measures shall remain exceptional. If any unplanned change must be implemented, the NM B2B will adopt the following approach:

- If the strictly typed implementation of the change is backward compatible, e.g. a new enumeration value only used in input:
  - NM will publish and deploy a new PATCH version of the impacted service.
  - The User will decide when he adopts this new version.
- If the strictly typed implementation of the change is backward incompatible, e.g. a new enumeration value only used in output:
  - NM will continue to support the MAJOR version(s) of the impacted service, making use of the mitigation patterns, e.g. `OTHER:…` values in loose enumerations.
  - Simultaneously, NM will publish and deploy a new MAJOR version of the impacted service (which will inherit the current NM B2B version lifecycle) that will include strictly typed corrections.
  - The User will decide if he remains on the former MAJOR version of the service, or if he upgrades its Client Software to the new MAJOR version.

4.3 Service Operational Aspects

4.3.1 Documentation

The following needs have been identified for the documentation:

- Improve the NM B2B usability;
- Simplify the NM B2B adoption, typically when NM B2B is recommended the replacement for an outdated exchange solution;
- Improve the documentation integration and navigability;
- Improve the accuracy, reliability, and coverage of the NM B2B Release Notes and documentation change tracking.

The NM B2B User will have access to the following documentation:

1) Operational documentation
The operational documentation will describe, as today, the operational procedures, the Stakeholders that participate to these procedures, and the business data that are exchanged. This documentation should remain agnostic of the communication channel: HMI or B2B.

2) Technical documentation
As today, the technical documentation will be composed of:
   - The SWIM Conformance Assessment documents;
   - The NM B2B Reference Manual:
     - The NM B2B Revision Notes – the changes delivered by a version
     - The NM B2B Essentials – the technical aspects;
     - The NM B2B Services – the exposed services and the exchange model.
   - Some annex technical documents, e.g. the NM FIXM Extension documentation.
   - The OpenAPI documents, XSD schemas, and/or any other kind of formal document corresponding to the solution retained by the API Design Guidelines.

3) Implementation guide
The implementation guide will be organised around business use cases, with the purpose of federating the operational and the technical documentation, offering therefore a place where the User will find all relevant information. The documentation of each business use case will contain:
   - References to the corresponding operational documentation;
   - References to the technical documentation of the service interactions used in the context of the use case;
   - The nominal and the main alternative workflows;
   - Message examples for all steps of the documented workflows;
   - Detailed test case which will help the Client Software developer in testing and validation activities.

   For example, this is the place where a User will find the detailed information and examples on how to use the FLIGHT_DATA topic to implement the future slot message, or to extract the ATFCM information from NM B2B Flight data It is expected that the writing of the Implementation Guide will also facilitate discussions via the NM CDM Process in order to rationalise the supporting APIs. Special attention will be placed on documenting the migration process from legacy exchange solutions, e.g. AFTN network to NM B2B. This documentation will serve

as a comprehensive guide to ensure a smooth transition and mitigate any potential risks associated with the migration.

A unique publication point for the consolidated NM B2B Documentation will be defined. The reader will have the possibility to navigate fluently trough all parts of the documentation. For example, the EarlyDPIRequest/Reply is today used by the Advanced Tower and A-CDM business use cases. Its technical documentation (including the corresponding formal documents like XSD schemas or OpenAPI documents) will expose links to the implementation guide, and more precisely to the documentation of the Advanced Tower and A-CDM business use cases. In turn, the documentation of the Advanced Tower and A-CDM business use cases will expose links to the EarlyDPIRequest/Reply the technical documentation (NM B2B Reference Manual and formal API documents).

The integration of third-party exchange models, e.g. AIXM or FIXM, will respect the following principles:

- Document and publish the model extensions according to the third-party model recommendation. For example, the NM FIXM Extension will be published, as today, as a pair of documents: the Reference UML Model and the XSD Schema Documentation.
- Document in a homogeneous manner the additional rules that NM applies to a third-party model.
- Ensure a fluent navigation from the NM B2B documentation to the third-party model documentation. Note that the precision of the navigation will be constrained by the possibilities offered by the third-party model documentation.

An effort will be made to extend the coverage of the change tracking to all parts of the technical documentation and implementation guide. For example, the following changes will be emphasised:

- Change in the documentation of a business use case;
- Change in an implementation example;
- Change in a third-party model extension;
- Change in the interpretation or usage rule of a third-party model.

At the same time, the navigability between the changes in the documentation and the NM B2B Release Notes will be improved. The reader will be correctly informed about the reason for a documentation change, and in turn, will have the possibility to navigate from one NM B2B Release Note entry to all related model and documentation changes.

4.3.2 User Onboarding

Based on the concerns highlighted in the analysis of the current NM B2B user onboarding process, the following solutions are proposed aiming to improve the journey for new users.

- A unified onboarding platform, serving as the sole entry point for all new NM B2B users, replacing fragmented entry points and outdated web forms. It will feature an intuitive interface, a description of the process and the information required, a repository of all business objects (e.g. forms, agreements, certificates, reports, complementary information, etc.), and the possibility to track the onboarding status.
  Such a solution would reduce confusion and enable better tracking and management of the onboarding process, resulting in an improved overall efficiency and user experience.

- An integrated ticketing and communication system consolidating various current tools into a single, unified workflow, improving coordination, response time and ensuring accountability through clear task allocation.
- A dedicated onboarding PoC for each user/organisation, guiding users through the process, addressing queries and ensuring a smooth transition.
  Such an approach would enhance accountability and avoid bottlenecks due to distributed responsibility along the process.
- A structured feedback mechanism within the onboarding platform, enabling users to provide both immediate and post-onboarding feedback. This input will be systematically reviewed to identify improvement opportunities and implement enhancements.
- Any Customer Organisation of which NM B2B Access request is eligible, will have access to the consolidated NM B2B Documentation.

4.3.3 User OPS validation

The following needs are identified based on the problem statement:

(1) The NM B2B needs to provide a reproducible environment such that the evaluation of an Operational Validation can be automated and its results reproduced under the processes of post-ops monitoring;

(2) The NM B2B systems needs to ensure that the technical verifications performed during an operational validation are enforced during runtime;

(3) The operational validation needs to be able to cover all the interactions (READ and WRITE) of the B2B API;

(4) The Operational Validation needs to be able to be executed by each NM B2B User prior to the official request for evaluation;

(5) The NM B2B needs to be able to identify any divergence from the validated pattern of use of a Client Software.

The combination of the following solutions is proposed to address the needs identified above:

Isolated Environment: The NM B2B Operational Validation will use an isolated environment with a configurable data provisioning policy (see section 4.2.4.2). This solution will address the need for reproducibility identified and will enable the validation of specific operational scenarios, testing a patch of a client application before deployment, or reproducing issues triggered under special conditions.

Integration Tests: The NM B2B will formalize a battery of integration tests to be executed against its API. For each interaction offered by the NM B2B API, a number of tests that verify the technical and business correctness of the client application will be defined. These integration tests will enable a high level of automation in the execution of the Operational Validation and provide a clear expectation for the software developer of the intended and correct behaviour of a client implementation.

Error Quotas: The NM B2B will introduce error quotas to ensure the NM B2B systems are protected during runtime from client errors (see section 4.2.10). This measure will ensure that the verifications performed during an Operational Validation in terms of correct technical implementation of the B2B API are actively enforced during operations.

Monitoring and Alerting: The NM B2B will introduce monitoring and alerting of client applications. The Operational Validation will be used to calibrate the expected pattern

of usage in terms of interactions of the B2B API used, usage levels, and acceptable error rates. The monitoring and alerting solutions will be used in the OPS platform to identify deviations from the calibrated Operational Validation levels.

4.3.4 User Management

4.3.4.1 User Identity Management

The following needs are derived directly from the discussion of problems and limitations presented in section 3.3.4.1 and partially related to 3.3.4.2.

(1) The NM B2B needs to support the adoption the European Aviation Common PKI (EACP) as mandated by the CP1.

(2) The NM B2B needs to streamline the process of user identity management and ensure a formal registration process is followed.

(3) The NM B2B needs a single source for the identity provision accessible across the different teams and applications.

Need (1) is straightforward to support, PKI relies on highly standardised protocols and the choice of PKI provider is relatively transparent for both client and server. In practical terms, the trust-store of Customer Organisations will need to include the certificate bundle of the EACP Certification Authority trust chain. And the NM B2B will update its server certificate to a new one issued by the EACP.

The adoption of the EACP can equally serve to meet need (2). As discussed in section 3.3.4.2, the NM B2B currently manages a pool of certificates issued by GlobalSign. The adoption of the EACP as the common PKI for European aviation will enable Customer Organisations to retrieve directly from the EACP their own certificates. Removing the NM B2B from these duties, which alleviates the overhead it causes and solves the normalisation issues experienced with identity registration. This will ensure a formal registration process is followed and enforced by the EACP Registration Authority.

Need (3) requires adopting a single Identity Provider solution that can be relied on as the single source for the NM B2B. This Identity Provider solution must integrate adequately with the Customer Relations Management software in use, and the Incident Management system.

4.3.4.2 Credential Management

The following needs are identified for the Credential Management solution of the NM B2B:

(1) The NM B2B needs to be able to support X.509 client certificates. Including certificates emitted by the current Certificate Authority (GlobalSign) and the European Aviation Common PKI (EACP).

(2) The NM B2B needs to be able to support username/password. Including the ability to manage them dynamically (e.g., update password and user registration).

(3) The NM B2B needs to be able to support two-factor authentication (2FA).

(4) The NM B2B needs to be able to support token-based authentication. Including the ability to manage them (create, revoke, refresh…) dynamically.

(5) The NM B2B needs to be able to associate one or more credentials to an identity and manage this mapping during runtime, without requiring a new deployment of its software.

The needs identified in this section establish a baseline of user requirements that the Identity and Access Management solution and Secrets Management solution of the NM B2B will satisfy.

The NM B2B will additionally provide a User management portal to enable its Users to manage their credentials dynamically.

4.3.4.3 Authorization Management

The following needs are derived directly from the discussion of problems and limitations presented in section 3.3.4.3.

(1) The NM B2B needs to be able to manage the user authorization during runtime without requiring a new software deployment.

(2) The NM B2B authorization solution needs to be able to define access control assigned to a credential to match its business needs at the level of the interaction, resource, and queue of the B2B API.

(3) The NM B2B authorization solution needs to be able to enforce access control based on assertions on the content of the payload.

(4) The end-user will have the ability to retrieve the authorization assigned to its credentials via a secure web interface.

Need (1) requires segregating the authorization configuration from the static configuration of the NM B2B and persist it in a runtime accessible solution.

Need (2) requires extending the authorization model from the current role-based access control to support the high level of customisation required. This might involve the adoption of an Attribute-Based Access Control authorization model substituting or enriching the current Role-Based Access Control.

Need (3) requires adopting a solution that can parse the payload of the NM B2B interactions.

Need (4) requires exposing a secure web portal for user management. Where users of the NM B2B can view their authorization and request authorization changes.

The NM B2B will select an Authorization Server solution that can support these requirements.

4.3.4.4 Usage Policy Management

(1) The NM B2B needs to be able to manage the usage policy of its users during runtime without requiring a new software deployment.

(2) The NM B2B needs to flexibly customise the usage policy assigned to a credential to match its business needs at the level of the NM B2B interaction.

Need (1) requires segregating the usage policy configuration from the static configuration of the NM B2B and persist it in a runtime accessible solution.

Need (2) requires that the solution chosen can parse the payload to retrieve the operation invoked.

The NM B2B will select an API Gateway solution that can support these requirements.

4.3.5 Monitoring

The solution presented below addresses the following needs:

- Inform the Users about:
  - the availability of the services;
  - the on-going issues;
  - the planned events;
  - the past events (planned or unplanned);
- Ensure the User access to the monitoring via HMI and via API;
- Ensure the User access to the monitoring in case of NM B2B malfunction – such periods are typically the ones during which the NM B2B users need a precise information about the NM B2B status.

The NM B2B monitoring will be exposed as:

- An API;
- A Web application.

The NM B2B monitoring will expose the list of available (OPS and non-operational) platforms. For each platform, it will expose the following information:

- **Support:**
  The platform support: 24/7 or Office Hours.

- **Status:**
  The status of the platform (overview), of each service, and of each business use case.
  The API will expose the status of the services via Scheduled P/S. For example, a Client will be able to subscribe to the periodic publication (e.g., every 5 seconds) of the Flight Filing Service status.

- **Quality of Service:**
  The historical statistical figures of the Quality of Service of each service (see section 4.2.9).

- **Issues:**
  The list of known and on-going issues, including planned and unplanned maintenance windows. Each issue will document the impacted services and business use cases.

- **Planned events:**
  The events that are planned to occur on the platform (the list might not be exhaustive) and their respective impacts in terms of services and business use cases availability:
  - NM Release deployment;
  - NM planned maintenance window;
  - NM failover / contingency exercise;
  - NM B2B Version deployment / decommissioning;
  - NM B2B Business Use Case deployment.

- **History:**
  The events that occurred in the past on the platform and that impacted the availability of the services:
  - Planned event;
  - Unplanned event / incident.

For reliability purpose, NM will host the NM B2B monitoring API and Web application on a distinct domain name. In this way, NM will ensure that the NM B2B monitoring remains accessible even if there are issues with the `eurocontrol.int` domain.

To proactively detect possible issues, the NM B2B monitoring will be deployed as an external NM B2B Client. The NM B2B monitoring will evaluate the status of each platform/service by periodically connecting to them and assessing the platform/service responses.

Finally, the NM B2B monitoring will provide navigation facilities:

- From a platform/service/business use case to its corresponding documentation.
- From a planned event to its announcement, e.g. from a NM Release Deployment event to the NM Release Notes.

4.3.6 Reporting

Based on the concerns highlighted in the analysis of the current NM B2B reporting function, the following solutions are proposed aiming to improve its reporting capabilities.

- Analytics dashboards consolidating data from various sources in order to provide both NM internal teams and B2B users with in-depth insights into API usage patterns, performance metrics, error rates, as well as client certificate and user access control information.
  Such a solution would facilitate efficient access to comprehensive data, streamlining issue investigations, auditing, and reporting processes.
- Role-based access control within the analytics dashboards to ensure users can access only the data for which they are authorised.
  This approach would allow to protect sensitive information and comply with data segregation policies.
  Finally, relevance and usability of data and insights would also be improved as a result of tailoring information to the specific needs and authorisations of different user roles.
- Data integration and aggregation processes compiling data from different sources into a comprehensive reporting framework.
  This solution would enable the provision of holistic insights into NM B2B API usage for both internal and external Stakeholders and simplify the process of generating reports.
- Custom report generation features within the analytics dashboard would enable users to create tailored reports based on specific parameters, such as API service consumption, user department activities, Client usage, and more.
  Such an approach would empower users to generate reports that meet their actual needs.

4.3.7 Maintenance

The solution presented below addresses the following needs:

- Inform the Users about the maintenance windows, planned and unplanned;
- Inform the Users about the impacted services;
- Report to the Users that a service is under maintenance via a specific error.

The three main new concepts in the solution are:

1. The traceability between B2B services and systems/applications
2. The notification and publication of all maintenance events
3. The introduction of a *Maintenance Mode*

The final maintenance process shall be as follows:

1. As today, a planned maintenance will usually be notified 6 months in advance. However, it might happen that a serious problem requires the quick deployment of a patch, e.g. a service handles incorrectly some input values. In such a case, an exceptional planned maintenance can be applied but must be notified at least 2 weeks in advance.
2. Sometimes a critical problem requires an urgent fix, e.g. a process running out of memory requires an urgent restart. In such a case, an emergency maintenance window will be opened.
3. In all cases, the maintenance window will be notified to the points of contact and will remain exposed in the monitoring (see section 4.3.5).
4. The maintenance event will contain the following information:
    a. Reason for the maintenance
    b. Start datetime, expected duration, and actual end datetime
    c. List of the impacted services
5. When the time comes for the maintenance to take place, the team will put the impacted B2B services in *Maintenance Mode*.
6. When in *Maintenance Mode*, the impacted services will return a dedicated structured error message that the client application can use to inform its own users.
7. Once the maintenance window is finished, the team will set the B2B services back to *Nominal Mode* (i.e. normal operations).

The monitoring solution will track all maintenance windows to properly compute the availability of the services.

4.3.8 Disaster Recovery / Contingency

Disaster Recovery (DR) is the ability to reestablish normal operations after an unexpected disaster, failure or comparable event that caused a significant system, network or data failure, with subsequent loss of service.

Service Oriented

With respect to business functionality, the NM B2B API shall be seen as a collection of services and not as a whole.

Each business service shall clearly specify its Quality of Service (see above). This shall include:

(1) The expected objectives in nominal circumstances, i.e. when the systems are running normally,

(2) Whether or not the service should be available even in case of disaster, and in such case, whether it is foreseen to run in some sort of “degraded mode”, and if so, what would be the objectives in such degraded mode.

(3) The recovery objectives in case of disaster. Such objectives shall be specified as:

- Recovery Time Objective (RTO), i.e. the maximum acceptable time that the service can be down after a disaster
- Recovery Point Objective (RPO), i.e. the maximum amount of data that can be lost during the recovery from a disaster.

Failover testing

Disasters are adverse events that may cause total system failures for which we prepare but may never happen.

If the disaster recovery procedure is never applied, how can one trust that it will work flawlessly when needed?

To be able to trust the disaster recovery procedures, they need to be tested frequently.

The NM B2B technical solution shall enable frequent testing of disaster recovery scenarios (which may include failover switching, activation of contingency systems, degraded modes, etc.), and it should be possible to do so per service (i.e. apply disaster recovery to some specific services without affecting others).

It shall be possible to plan regular failover exercises on one or more B2B services, during which client systems would consume the services from the DR solution. This will build a trust on the DR solution and will keep the personnel well trained. The date of such exercises will be communicated via the monitoring solution.

Optimization of resources

The NM DR must deploy the essential components and only the services and processes required by the agreed DR scenario necessary to support the services according to their required Quality of Service in contingency mode (which may differ from the QoS on nominal circumstances).

What if PENS fails?

In line with the recommendations of the Future IP Needs Task-Force (FIN-TF), endorsed by NDTECH/13 (June 2024), the PENS Governance is seeking to establish a dual-core sourcing strategy for the next generation of PENS (PENS 3.0) to ensure a more sustainable, resilient, and cost effective solution than the combination of existing regional IP-connectivity solutions. Related activities will be initiated post summer 2024.

4.3.9 Incident Management

Based on the problem statement the following needs are identified for the incident management capabilities of the NM B2B.

(1) Unified Entry-Point: The NM B2B will provide a single, web-based entry-point to report incidents.

(2) 24/7 Support for Operational Emergencies: Operational emergencies need 24/7 support, the NM B2B will continue to offer this support via the unified web-based entry-point plus a phone line.

(3) Cross-Team Integration: The internal incident management tooling should facilitate seamless communication and transfer of incidents between teams (CSO, Customer Support, B2B Office).

(4) Incident Tracking: Users should be able to track the status of their incident reports autonomously via a web-based interface.

(5) Incident Registration and Analytics: The incident management system will register the history of incidents, resolution, milestones, timestamps, and teams involved. To enable post-incident analytics, identify bottlenecks, and improve the performance of the incident management processes.

To meet these needs and solve the problems identified the NM B2B will implement the following solutions:

(1) A web-based portal that allows its users to register their incidents and requests for support. Replacing the multiple email addresses and web-forms currently available, providing a unified entry-point to receive support for the NM B2B.

(2) Integrated with a unified ticketing system shared across the different teams inside EUROCONTROL dealing with the different aspects of Incident Management, Customer Support, and Integration Support. Enabling seamless routing between departments, a single view of the status of a request, prioritisation, and dispatching across teams.

(3) The web portal will expose the means for the user to track the incident resolution and interact with the NM B2B support specialists.

(4) The web portal may be integrated with the monitoring portal described in section 4.3.5.

(5) In addition, CSO will maintain a phone number available 24/7 for operational emergencies.

4.3.10 Problem Investigation

The solution presented below addresses the following needs:

- Complete the recording of the NM B2B activities;
- Simplify the replay of the NM B2B activities;
- Improve the analysis tooling.

The NM B2B will record sufficient information to re-build any published P/S Message. This feature will ensure to NM the possibility to reconstruct, at post-operation time, the exhaustive list of messages exchanged via NM B2B with any User, Request / Reply or Publish / Subscribe Topic.

The NM B2B will ensure that all components involved in the treatment of a request correctly correlate the information (logs) that they record. This feature will ensure to NM the possibility to reconstruct, visualise, and analyse, the detailed processing sequence of any received NM B2B request.

To ensure a complete replay capability, the same approach will be applied to the treatment of the activity triggered by the NM HMI users. Indeed, NM HMI and NM B2B activities are intimately correlated as they are finally handled by the same components. The recording of the NM HMI activity is a pre-requisite to a complete replay solution, which in turn, is required by the long term / multi-factor problem investigation.

The replay of a period of NM system activity will be simplified. Ideally, the post-operation replay of one hour of recorded NM system activity shall not require more than a few minutes of effort.

The recording of the NM system activity (including the recording of the exchanged message payloads required by the replay) will be retained during a minimum period of three months.

Finally, the NM B2B will continuously improve its analysis tooling, giving a particular attention to the upcoming challenges. Priority will be given to:

- Log aggregation and analysis tooling – extend the current solution to newly available information like published P/S Messages;

- Performance bottleneck tracking – develop NM system integrated views in order to localise the latencies;
- Memory usage - detect insufficient capacities.

4.4 Business Scope

4.4.1 iDL

Merge of EAD and CACD Systems

From a business point of view, the main impact on NM B2B of this merge will be that the entire data associated with past, present and future states of an ATM entity (e.g. an Airspace/Aeronautical entity) will be stored and accessible in a single, consistent object, hence having a single lifecycle. The CDM process described below (iDLAD) will make sure that all operational Stakeholders involved in the management of aspects of the said object will have agreed upfront upon the object definition.

Further details are to be found in the iDL ConOps. Some topics must be further discussed via the NM CDM Process, for example (not exhaustive, far from there):

(1) Accepting some differences within the description of such objects, for example to accept that an Airspace object would come with a "publication geometry" (for AIP publication, potentially more textual) and an "operational geometry" (purely formal, geometrical, targeted to efficient computer processing). Some Stakeholders commented that this might not be the best solution, so that the best solution is not known yet and will be discussed via dedicated Collaborative Arrangements meetings.

(2) A main difference that exists between EAD and CACD, which is the use of Airblocks to define Airspace geometries, where it could be expected that the potential use of Airblocks in that context would rather be seen as an internal, private NM structure, and not exchanged via NM B2B as it is today. Again, further analysis of this topic will be better realised via dedicated expert group meetings.

From a technical perspective, the existing NM B2B Airspace services and AIMSL will be entirely aligned so as to become a single, consistent API complying with the solutions proposed in the technical sections above. Doing so will not only rationalise and modernise the access to AIM/ATM data and thereby reduce discrepancies and NM and NM Stakeholders costs on the long term, but also imply useful evolutions in terms of services, for example the generalisation of WFS services (not limited anymore to AIS data) or of the creation of Request/Reply services on AIM/ATM data (which exist today in AIMSL but not in NM B2B Airspace services).

Process for the collaborative iDL AIRAC Data (iDLAD) definition

This is the most challenging item for the NM B2B coming from the iDL scope. Indeed, it is where the digitalisation process comes into force, enabling the required level of collaboration for the iDL AIRAC data. Doing so will require the development of new concepts in the first place, like Projects and Branches (see iDL ConOps), and the NM B2B services supporting them, to upload data to elaboration branches, downloading them and properly notifying concerned NM B2B users about changes at elaboration time. Whereas the roles and responsibilities of the involved Stakeholders shall not change through this evolution, the interfaces shall necessarily have to change.

The same will apply with permanent branches, namely after integration, as publication, and for late changes in these permanent branches.

The NM B2B Airspace and EAD AIMSL services API will not only change because of their merge, but also – and most importantly – because of the introduction of the digitalised collaborative AIM/ATM data building and validation processes taking place in preparation to the coming AIRAC cycles.

Airspace Utilisation Rules and Availability (AURA)

The AURA definitions shall be supported (read/write and proper validations) will be supported via the iDL NM B2B API. The overall RAD/restriction model will be reworked so as to automate as much as feasible the mapping from the RAD restrictions and their grammar onto proper operational restrictions, while ensuring the tracing of this "translation" process. In some cases, the NM B2B API for AURA might have to support some human-attended mapping feature.

Additional Airport Data (Airport Corner, etc.)

From the various Airport application mentioned in the iDL ConOps, one of them has been released as part of the NM-MAINT-2 release, namely the passenger demand prediction service, including an NM B2B API.

The decision of what additional Airport Data (and when) will be exchanged via NM B2B API should be derived from discussions in the NM CDM Process.

MET & Natural Hazards

It is likely that the iDL NM B2B will serve as a broker for MET data, in accordance with regulatory rules. Because local State regulations may enforce to use "trustful sources of MET data", any solution in this area will address this requirement for diversity and choice.

In the Flight Plan domain, flight plan revalidations will take place versus MET & natural hazards, and flight planners will be informed of potential asynchronous flight plan rejections due to weather.

Regarding natural hazards, the future EVITA service will cover missing kinds of natural hazards (see iDL ConOps) and be supported via NM B2B.

Aircraft Performance

Some Aircraft Performance data is exposed today via the NM B2B Airspace Structure service – this service might not be sufficient to meet the iDL requirements: to be discussed via the appropriate NM Working arrangements

Network Events

With iDL, the wide NET event information gathered by NM will remain accessible to all via HMI, but additional efforts will be brought to make it possible to refer to these NET events, in two ways:

- Since Network Events will become part of the iDL data, it will now be possible to refer to events data from other components of the iDL domain (such as ATFM regulations, scenarios, etc.), as well as in any other iNM context;
- Users will have the possibility to get Network Event information from NMUI and B2B, to refer to Network Events in their local context, and possibly to contribute to the definition of Network Events via NMUI and NM B2B.

Transponder Code Function (TCF) configuration

Today, the CCAMS service requires an AFTN connection, but this connection capability may be expanded as the NM distribution services evolve. The future NM systems will maintain a back-up communication mechanism for local contingencies at ATSUs. SSR codes assigned by CCAMS will have to be also provided via NM B2B.

In addition, the implementation of new user interfaces will likely require the extension of current interfaces to B2B technology – please refer to the iDL COnOps.

Data Harmonisation

As explained in the iDL ConOps, the two EAD and CACD data sources will become one, so that the entire iDL data will go through the same validation rules, hence solving the current discrepancies. In addition, a number of system rules will be corrected and evolved, to further ensure the iDLAD adherence to the appropriate regulations. The definition of common validation rules will be developed in coordination with affected stakeholders in the relevant NM working arrangements.

Clearly enough, the application of these validation rules will have an impact on the iDL B2B API.

Business Evolutions – Indirect Impact on iDL

Same as in Chapter 3.

4.4.2 Flight

This is an extract of the "Transition Principles" of the Network 4DT ConOps.

"The transition of the current fragmented trajectory management process to the Network 4D trajectory management will be gradual and will happen in different steps within 2029 time horizon. It should be recognized that not all Operational Stakeholders can progress with the same pace, mostly depending on their operational needs and expected operational benefits of 4D trajectory management enhancements. Therefore, within this period a broad co-existence of different modes of flight plan, flight data and trajectory exchanges will be in place and all of them need to be considered for the network 4D trajectory prediction/negotiation and sharing. Although the FF-ICE R1 services are most likely to be deployed by the majority of Operational Stakeholders by 2029, the ICAO 2012 flight planning will still exist and the Network 4D trajectory management processes will be able to support them. Different formats of flight plan/flight data exchanges (ICAO, ADEXP, FIXM) will coexist for substantial time as there is no indication that ICAO intends to phase out ICAO FP 2012.

The transfer and coordination process will be enhanced by deploying the additional OLDI message exchanges, enabling OLDI multi-cast functionalities via SWIM YP or FO IOP implementation. There will be no uniformity in the coordination and transfer process exchanges and each operational Stakeholder will select the most appropriate mechanism in accordance with their operational/technical context, identified operational needs and cost/benefit analyses. OLDI messages will be exchanged via FMTP or SWIM YP.

The airport exchanges (DPI, FUM) will progressively move from AFTN to NM B2B. It is expected that by transition of airport exchanges with NM via NM B2B to be finalized within the 4DT CONOPS time horizon and Network Manager can decommission the AFTN/AHMS exchanges with airports, however they might be kept as a back-up communication means.

The exchanges with Airspace User will be gradually enhanced towards NM B2B and some of them might be phased out (EFD) by 2028.

The legacy exchanges for the provision of trajectory updates gradually moved over SWIM YP (FSA, AFP, APL, ACH) and depending of the pace of implementation it is foreseen that NM B2B for trajectory updates/revision will be dominant by 2029, but none of these legacy messages is planned to be decommissioned. Therefore, the

legacy and NM B2B based exchanges will coexist and NM and respective Operational Stakeholder need to take into account both modalities. The exchanges stemming from FF-ICE R2 might complement the trajectory revisions, but they will come on top of legacy ones and NM B2B.

An operator that is unable to submit FF-ICE flight plan data shall continue to submit current flight plans (FPL) and associated ATS messages (CHG, DLA, etc.) in accordance with the procedures described in PANS-ATM chapter 4.4 and Appendices 2 & 3. ANSPs that have implemented FF-ICE i.e., ANSPs are obliged to continue their support of FPL and associated messages as long as the mixed-mode environment exists.

NM will continue to use CPRs and ADS-B reports for trajectory updates while ANSPs will continue to use a variety of surveillance inputs for trajectory updates. No substantial change is foreseen in this area.

The Network Manager will offer the NM Trajectory service for the construction of ATC local trajectory, but still some Operational Stakeholders might rely on their own systems for the complete Trajectory Prediction process.

[…] The flow exchanges will continue to be done using XML format.
Special considerations should be taken for the trajectory updates/revision of IFPZ neighbouring ATS units, as some legacy exchanges that will not exist within IFPZ (like OLDI via X.25) may still need to be supported by Operational Stakeholders bordering non-IFPZ. It is expected by 2029 that some of the North-Atlantic traffic trajectory revisions could gradually move to FF-ICE R2.”

4.4.3 Flow

No solution is proposed today as the requirements will have to be further developed in the first place – the NM B2B Operational Deployment Plan will serve as the planning tool for both NM B2B technical and business-related evolutions.

4.4.4 Cross-Service Linking

The general rule will be that the reference information will be systematically passed so as to be able to resolve it easily, as well as the required retrieval services.

The exact way of facilitating the retrieval of referenced information (from one object to the other) will be defined on a case-by-case basis.

As an example, objects of the Airspace Structure model will be referenced from the many other services using them through an “identification” structure (ICAO, IATA, UUID, …) that will allow to unambiguously retrieve these objects from the Airspace Structure API.

4.4.5 Services Only Supported via HMI

All NMUI services will also be rendered via NM B2B. The priorities of such developments will be analysed in time via the NM CDM Process.

As said in Chapter 3, the list below is not exhaustive but gives a good idea of the main missing services/capabilities:

- Airspace data Create, Read, Update, Delete (CRUD) service:

The full NM B2B API for the Airspace/Aeronautical CRUD will be developed in the context of the iNM iDL project, together with the merge of the EAD and CACD systems and the creation of the digital CDM process for the iDL AIRAC Data definition.

- RAD service:
  The RAD service will be entirely supported (read and write) via an NM B2B API of the iNM iDL component.
- CAL service:
  The iDL scope includes the CAL, and more generally improvements to the TCF configuration, which are foreseen to be made available via NM B2B. This will be addressed as part of the iDL developments.
- Crisis management service:
  The crisis management service will be exposed via NM B2B, including the support of definition and publication of danger areas and danger area forecasts.
- Network event service:
  The Network event service will be fully supported via NM B2B API, as part of the iNM iDL component.
- Daily Network Plan service:
  The NM B2B API for the Daily Network Plan service will be provided as part of the iNM/Flight and Flow developments.
- Headline News service:
  The NM B2B API for the Headline News service will be provided as part of the iNM/Flight and Flow developments.
- Call Sign Similarity Tool (CSST) service:
  The NM B2B API for the CSST service will be provided as part of the iNM/Flight and Flow developments.
- Archived data access:
  This gap must be addressed in the overall context of iNM developments, on a case-by-case basis – the general technical case of exchanging massive data amounts should also be addressed in this context, as a prerequisite.
- Other:
  MIRROR and other HMI applications that do not have their NM B2B counterpart could be supported via NM B2B in the future, depending on needs expressed via the NM CDM Process.

5 Transition to Future NM B2B

The approach is to progressively reach the full coverage of the agreed changes at the end of the transition period, around 2030. During this transition, improvements will be deployed in parallel along the three axes: technical aspects, service operational aspects, and business scope.

This chapter describes how NM intends, in practice, to deliver over time the planning elements needed by B2B Stakeholders to build their own related plans.

The Chapter 5 does not expose the transition plan to the future NM B2B; it has been preferred to maintain a rolling "NM B2B Operational Deployment Plan", as the NM B2B ConOps and such a rolling document do not (and should not) share the same lifecycle. However, the first version of the NM B2B Operational Deployment Plan comes together with the first full official version of this ConOps, namely version 1.0.

5.1 NM B2B Operational Deployment Plan Publication

Applying the Service Lifecycle and Versioning solution, starting from 2024, NM will publish at least once a year the NM B2B Operational Deployment Plan. The plan will initially cover the whole transition period, until end 2030. It will be extended beyond this date in the next years.

Each version of the plan will be organised as follows:

Detailed planning for the current (Y) and next year (Y+1)

- Detailed description of the planned changes including, per change or group of changes:
  - Expected impact
    - What services are impacted, MAJOR or MINOR version
    - What Stakeholders and use cases are impacted
  - Delivered value
  - Specific information regarding the regulatory aspects
- Detailed deployment plan
  - Publication date of API change, and subsequent exchanges with Stakeholders via the NM CDM Process
  - Date of API beta version deployments on FUTURE platform
  - Date of API official version deployments on FUTURE platform
  - Date of API official version deployments on OPS platform
- Service version decommissioning plan
  - Date of deprecated API version decommissioning

Draft planning for the year Y+2

- Planned changes, with further plan elaboration where possible
- Planned API version decommissioning

High level planning for further future Y+N (where N>2)

- Planned changes

5.2 Technical and Service Operational Priorities

The following high-level priorities are proposed for the technical and service operational changes (i.e. all changes but business scope).

The introduction of new API design paradigms and guidelines is clearly the most User impacting technical change proposed in this document. Therefore, the publication of the API Design Guidelines is considered as a prerequisite to the publication of any new NM B2B API. In addition, the compliance of an NM B2B API to the API Design Guidelines is considered as a prerequisite to its publication and operational deployment.

During the transition, users will have to adapt their client software(s) to the delivered changes. Therefore, the delivery of the technical or service operational aspects that can enable and/or facilitate the transition are considered as having high priority. In particular:

Any solution element that improves the NM B2B services usability inherently facilitates the migration:

- Service lifecycle and versioning
- API Design Guidelines
- Documentation

Any solution element that facilitates the development, testing, and runtime monitoring of the client software inherently facilitates the transition:

- Platforms, and more precisely:
  - FUTURE platform(s) used to expose early the planned changes
  - Availability of predictable data to enable the automated testing on read interactions
- Quality of service / monitoring, and more precisely:
  - Performance API and Web interface
  - Availability and reliability API and Web interface
  - Request quality monitoring API and Web interface

5.3 Business Scope

The iNM Roadmap foresees the OPS deployment of business services in 2025. Some of these services will be exposed through a new B2B API, e.g. eEAD Digital NOTAMs. Such NM B2B changes are therefore and necessarily seen as having a high priority.

Regarding further business scope, the NM B2B transition plan will align with the iNM Roadmap deployment dates, and conversely. This will follow, as today, the discussions taking place within the context of the NM CDM Process, and the subsequent NM release definition process. Clearly, the earlier planned B2B API deployments will be considered with higher priority.

Again, the plan for business-driven evolutions of the NM B2B will be exposed via the NM B2B Operational Deployment Plan.

5.4 Backward Compatibility – NM B2B Service Lifecycle

The NM B2B deployment plan will strictly follow the lifecycle described in Chapter 4 of this document.

5.5 Deployment Plan Information Per Change

This section sketches the minimal information per change exposed in the NM B2B Operational Deployment Plan.

Value

A customer organisation needs to be informed about the value of a planned change. The transition plan shall provide accurate answers to the following questions:

- In what general context does the change take place?
- Does a change improve the quality of service? How?
- Does a change improve the usability of the service? How?
- Does a change support a new/updated business use case? Which?
- Is a change final or is it an intermediate step in a sequence of changes that will be completed in a future deployment?

Impact

A customer organisation needs to know how much a change will impact them. The deployment plan shall provide accurate answers to the following questions:

- Which business use case(s) / service(s) will be impacted by a change?
- What will be the nature of the impact? Client software? Client software development? Client software operation? Regulatory? Organisational? The plan for change will include a general idea (as NM does not know the client specifics) of the change on the client side.

Planning

A customer organisation needs to know what the planned changes are and when they are planned to be deployed. The transition plan aims at providing accurate answers to the following questions, on a per change basis (or grouping of changes):

- What are the topics “in the pipe”? Those are all kinds of subjects, technical or business, which are at that moment under discussion at NM and/or with Stakeholders.
- When will a description of the NM B2B change be published, e.g. when will a new API version be published? From that point on, detailed discussions about the API change are expected to take place (see Chapter 4) via the NM working arrangements.
- Importantly, the plan will also detail how the change will be implemented across releases, as it is sometimes needed, for backward compatibility reasons, to support an intermediate API version.
- When will a beta version of the change be usable for development and testing purpose? This will come with a last opportunity for Stakeholders to influence the API change.
- When will a change be deployed to operations?
- How long will the pre-change versions remain supported in operations?

Regulatory Context

A customer organisation needs to be informed of the regulatory aspects of a planned change. The deployment plan shall provide accurate answers to the following questions:

- Is a change related to some regulatory aspect, and in what way?
- What should customer organisations know about a change to help them in their discussions with their regulator? This is an essential item, to come early in the process, as it may have a strong influence on the chosen solution.

A. Abbreviations

Abbreviations

Term	Description
AFTN	Aeronautical Fixed Telecommunication Network
AIM	Aeronautical Information Management
AIMSL	Aeronautical Information Management Service Layer
AIS	Aeronautical Information Services
AIXM	Aeronautical Information Exchange Model
AMQP	Advanced Message Queuing Protocol
ANU	Air Navigation Unit
API	Application Programming Interface
ASM	Airspace management
ATM	Air Traffic Management
AURA	Airspace Utilisation Rules and Availability
B2B	Business to Business
CACD	Central Airspace and Capacity Database
CAL	Code Allocation List
CDM	Collaborative Decision Making
CDN	Content Delivery Network
CHMI	Collaboration Human Machine Interface
CRCO	Central Route Charges Office
CSO	Customer Support Office
CSST	Call Sign Similarity Tool
DDoS	Distributed Denial of Service
DR	Disaster Recovery
EAD	European AIS Database
ETFMS	Enhanced Tactical Flow Management System
FAAS	Flight Assessment and Alerting System
FIXM	Flight Information Exchange Model
gRPC	Google Remote Procedure Call
HTTP	Hyper Text Transfer Protocol

HTTPS	Hyper Text Transfer Protocol Secure
IAM	Identity and Access Management
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
iDL	integrated Data Layer
iDLAD	iDL AIRAC Data
JSON	JavaScript Object Notation
LoA	Letters of Agreement
NM	Network Manager
NMP	Network Manager Portal
NOP	Network Operations Portal
POC	Point of Contact
QUIC	Quick UDP Internet Connections
RAD	Route Availability Document
RFC	Request For Comment
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SESAR	Single European Sky ATM Research
TCF	Transponder Code Function
TLS	Transport Layer Security
UDP	User Datagram Protocol
XML	Extensible Markup Language
WFS	Web Feature Service
WSN	Web Services Notification

1

1

2

SUPPORTING
EUROPEAN
AVIATION

www.eurocontrol.int