0.   Cover

ORIGINATOR:	ISSUE DATE:	VERSION:
TAXUD/R5	01.06.2012	1.00

**ANNEX II.C - CCN2 PLATFORM SPECIFICATIONS
AND REQUIREMENTS**

Invitation to tender TAXUD/2011/AO-013

**Specification, development, maintenance
and 3rd level support of CCN and CCN2**

(CCN2-DEV)

Typographic conventions

The following typographic conventions are used in this document:

- The following convention indicates a link.

Draws attention to important information

Indicates definitions or reference information

Indicates that this requirement must be clearly addressed in the tender

0.1.   Table of Contents

0.2. Table of Tables

0.3. Table of Figures

0.4.   Introduction

> *i* In this document, the Directorate-General Taxation and Customs Union of the European Commission, which is the contracting authority, will be further referred to as "the Commission" or "DG TAXUD".

> *i* "Tenderer" is to be understood as an economic operator who has submitted a Tender with a view to concluding a contract. In this Call for Tenders, "Tender" and "Bid" are used as synonyms.

0.4.1. *Purpose*

This document is an Annex to the ITT TAXUD/2011/AO-013 and provides the **CCN2-DEV** CCN2 Platform Specification and Requirements.

0.4.2. *Overview*

This "Annex II.C - CCN2 Platform Specifications And Requirements" document has the following structure:

SECTION	DESCRIPTION
Chapter 0	Provides a list of acronyms, definitions and reference documents used in this document.
Chapter 1	Introduces the key design principles around which the CCN2 Platform should be developed.
Chapter 2	Introduces the CCN2 Platform, explains the functional break-down of the CCN2 Platform and provides all functional requirements.
Chapter 3	Explains the non-functional requirements of the CCN2 Platform.
Chapter 4	The migration from the current CCN/CSI to the CCN2 Platform will be an essential element of the requested services. This chapter introduces requested migration vision and approach.

Table 1: Document structure

0.5.   Acronyms and definitions

An extensive list of abbreviations can be found in "Annex II.E - List of Abbreviations and Definitions".

1. Design Principles

1.1. Overview

The implementation of the CCN2 Platform will be required to conform to certain key design principles. These design principles are required to ensure that the CCN2 Platform:

- Is fit for purpose;

- Allows seamless interaction with the CCN/CSI stacks providing the equivalent level of service as is currently provided;

- Is flexible to meet future development requirements;

- Is scalable to meet projected volumes;

- Is operable and maintainable in a cost effective volume;

- Is upgradable on a regular basis in a cost effective manner.

The initial implementation of the CCN2 Platform:

- Provides a generic SOA backplane for further use as DG TAXUD develops applications around the SOA paradigm;

- Allows applications using the CCN/CSI stacks to interoperate seamlessly with the CCN2 Platform. Thus it should be totally transparent to the existing applications as to whether they are interoperating either via the CCN2 Platform or via the existing CCN/CSI.

> The Tenderers in their response must clearly specify their overall design and indicate how it confirms to the design principles. Conformance with the design principles is a key part of the technical award criteria.

1.2. Definitions

NAME	DESCRIPTION
Partner	A Partner is an entity participating in the CCN2 Platform either by offering services to the CCN2 Platform or by consuming services offered by the CCN2 Platform.

Table 2: Definition of "Partner"

Currently, Partners are National Administrations (NA) in Member States (MS), Candidate Countries (CC), EFTA countries, internal EC Directorates such as DG TAXUD, DG AGRI, DG MARE and OLAF, and EC contractors such as the **ITSM2** contractor. Other types of partners could be introduced in the future.

NAME	DESCRIPTION
Access Point (AP)	Logical interface to the CCN2 Platform, providing all external communications to and from it.

Table 3: Definition of "Access Point"

NAME	DESCRIPTION
Main Hub (Hub)	The Main Hub is the physical location of the CCN2 Platform hosting complete set of CCN2 Platform functionalities. It is designed to allow multiple physical instances both in active / active and active / passive mode.

Table 4: Definition of "Main Hub"

NAME	DESCRIPTION
Platform	A Platform is a combination of hardware, software and possibly appliances and network equipment intended to fulfil specific requirements.

Table 5: Definition of "Platform"

NAME	DESCRIPTION
Component	A Component is a basic building block such as a software package, a Web service, or a hardware appliance that encapsulates a set of related functions (or data).

Table 6: Definition of "Component"

NAME	DESCRIPTION
Module	A Module is a collection of Components that provides a set of logically related functionalities of the Platform.

Table 7: Definition of "Module"

The following figure shows a potential conceptual architecture of the CCN2 Platform.
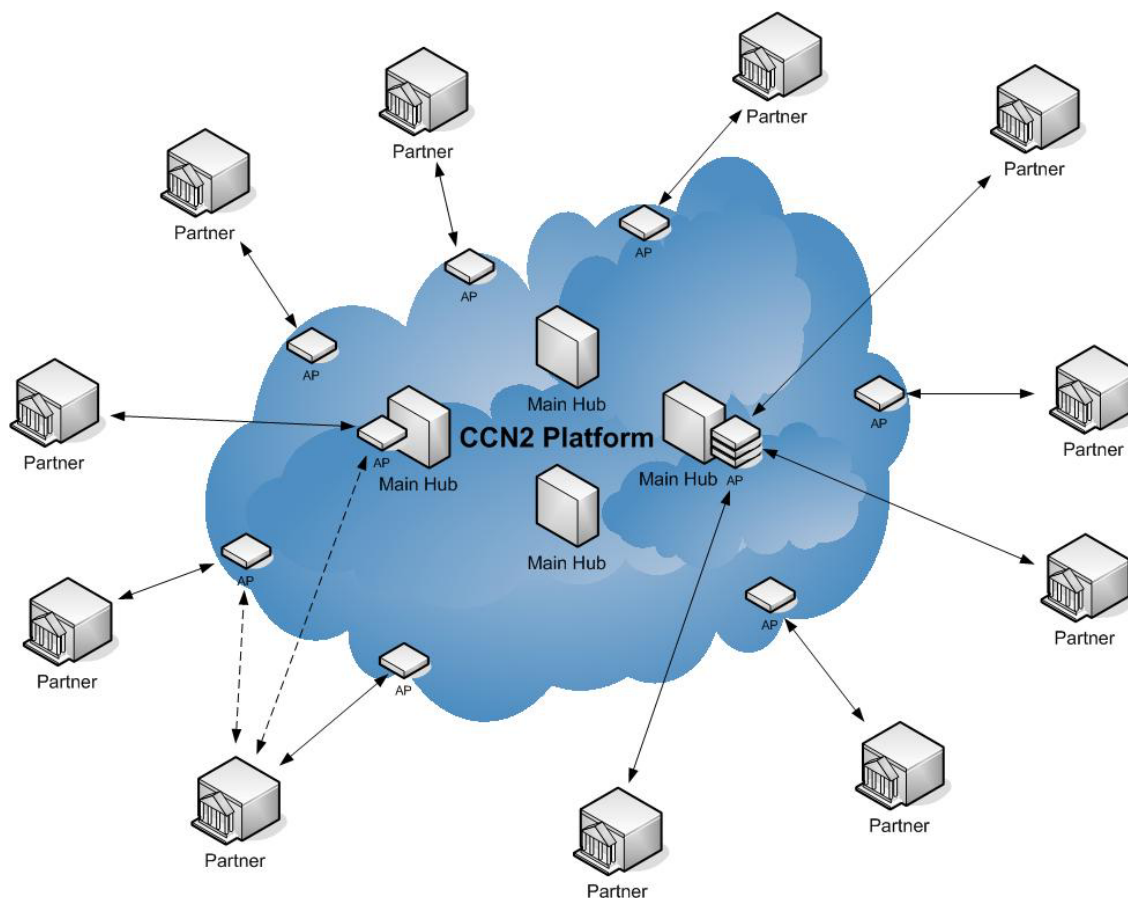
Figure 1: Potential Conceptual Architecture of the CCN2 Platform

Depending on the design, in case of non-availability of an AP hosted in one Partner it may allow connecting to an AP hosted in another Partner or to the AP hosted in one of the Main Hub data centres (as depicted by the dotted lines in Figure 1 above). In such a case it may be required a network equipment or any other equipment able to do the switch.

The proposed CCN2 Platform topology (centralised, distributed or meshed) is a Tenderer design decision based on reliability and other various parameters such as governance, performance etc. vs. the TCO over the framework contract duration.

The minimum set of functions for the AP is defined further in this document. However, the distribution of functionality between an AP and a Main Hub is a Tenderer design decision based on a trade-off between reliability and global TCO over the framework contract duration.

It is preferred that a "cloud-like" management solution be provided. This should allow ease of reconfiguration, dynamic instantiation and logically centralised management functions for the management of all CCN2 Platform components (particularly the AP).

The backup solution for an AP may vary depending on Tenderer design decisions. This could vary from a backup AP solution in a Main Hub to a situation where any AP may serve as a backup AP (e.g. in a purely meshed topology), as long as the requirements are met. It is assumed that the link between a local AP and the Partner is a dual Ethernet connection (2 times 1GB link).

In this document, the following wording is used to denote the importance of requirements:

CLASSIFICATION	DESCRIPTION
MUST	It is mandatory for a solution proposed by the Tenderer to comply with the requirement, feature or behaviour.
SHOULD	The requirement is recommended but it is not mandatory. However, it is a Tenderer's decision whether to propose or not a solution depending on various factors such as cost, complexity, reliability, availability of the features in the products, and amount of custom development involved. As part of the questionnaire the Tenderer will be asked to justify the decision taken.
MAY	The requirement is optional (nice to have). The Tenderer can comply with the requirement, but it should be provided out of the box or with minimum effort required. It is a Tenderer's decision whether to propose or not a solution depending on various factors such as cost, complexity, reliability, availability of the features in the products, and amount of custom development involved.

Table 8: Wording for the requirements

1.3. Detailed Design Principles

The detailed design principles are outlined in this chapter. They have been grouped into the following categories:

- Architecture

- Cost

- Maintainability

- Scalability

- Reliability

- Security

- Supportability

1.3.1. *Architecture*

#	DESCRIPTION	CLASSIFICATION
DP1.1	The CCN2 Platform is designed with the major goal of providing interoperability between Partners as well as between Partners and DG TAXUD.	**MUST**
DP1.2	The CCN2 Platform tries to avoid bespoke development as much as possible through the use of COTS (Commercial Off-The Shelf) products.	**MUST**
DP1.3	The CCN2 Platform offers the possibility to deploy APs where required (e.g. in most Partners) with no limitations on the number of APs that are deployed.	**MUST**
DP1.4	The interoperability provided by the CCN2 Platform to Partners is as far as possible independent from the availability of an individual data centre. In case of non availability of the Partners' Data Centre, the Partner must be able to switch to another Access Point located in a different Data Centre (e.g. in case of disaster or maintenance). Accordingly, the same switching between two Data Centres applies for the Main HUBs.	**MUST**
DP1.5	The CCN2 Platform design is based on best practices and industry standards as much as possible.	**MUST**
DP1.6	The CCN2 Platform supports the SOA design paradigm[1].	**MUST**
DP1.7	The CCN2 Platform supports new integration paradigms using synchronous communications based on SOAP / REST Web Services[2], etc.	**MUST**
DP1.8	The CCN2 Platform offers the asynchronous communication paradigm. The asynchronous paradigm supports existing CSI facilities and provides additional interfaces for Partners using standard interfaces including Web Services, JMS or other technologies.	**MUST**
DP1.9	The CCN2 Platform supports the existing Partner applications with no redevelopment from their side (particularly any change in the CSI API is backward compatible).	**MUST**
DP1.10	The boundaries of the CCN2 Platform are designed to use open standards (as defined in the Commission Communication COM(2010) 744[3]) as far as possible.	**MUST**

---

[1] SOA Reference Architecture
https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12490

[2] Representational State Transfer (REST) http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm

DP1.11	The CCN2 Platform is designed in such a way that it is capable of operating in a shared resource environment with dynamic allocation of resources. For software, this usually means the use of various virtualisation capabilities.	**MUST**
DP1.12	The CCN2 Platform software runs in a virtualised environment.	**SHOULD**
DP1.13	The design of the CCN2 Platform and the proposed software modules have a strong focus on the use of open standards (as defined in the Commission Communication COM(2010) 744[4]).	**SHOULD**
DP1.14	The CCN2 Platform is designed in a way that individual components can run independently of each other on separate systems, as required.	**SHOULD**
DP1.15	The CCN2 Platform is able to support federated SOA domains which are interconnected and capable of operating independently of each other.	**SHOULD**
DP1.16	Simplicity is an architectural goal of the CCN2 Platform and therefore it should be easy to learn for all those involved.	**SHOULD**

Table 9: Design Principles for architecture

1.3.2. *Cost*

#	DESCRIPTION	CLASSIFICATION
DP2.1	The CCN2 Platform is designed in a cost effective manner in order to reduce the total cost of ownership (TCO) – e.g. by using commodity hardware, open source software, etc.	**MUST**
DP2.2	The CCN2 Platform is designed in such a way as to minimise the TCO of the Platform.	**MUST**

Table 10: Design Principles for cost

1.3.3. *Maintainability*

#	DESCRIPTION	CLASSIFICATION
DP3.1	The CCN2 Platform is designed in such a way that it is composed of discrete components such that a change to one component has	**MUST**

---

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Towards interoperability for European public services COM(2010) 744 (http://ec.europa.eu/idabc/servlets/Doca2cd.pdf), page 9

[4] *ibid*

#	DESCRIPTION	CLASSIFICATION
	minimal impact on any other component (modularity).	
DP3.2	The CCN2 Platform is designed in such a way that its components can be easily upgraded or replaced.	**MUST**
DP3.3	The CCN2 Platform is designed is such a way that it is easily extensible with additional components.	**MUST**
DP3.4	The CCN2 Platform is designed to consolidate data used for the operation of the Platform into a single location with no logical duplicates. If it is not feasible to completely consolidate the information, a single source must be identified as the master data and controlled replication must be in place.	**SHOULD**

Table 11: Design Principles for maintainability

1.3.4. *Scalability*

#	DESCRIPTION	CLASSIFICATION
DP4.1	The CCN2 Platform is designed so that there are no inherent limitations in either horizontal[5] or vertical scalability[6].	**MUST**
DP4.2	The CCN2 Platform is designed in a way that there are no limitations in the number of services registered in the SOA registry that can be supported.	**SHOULD**
DP4.3	The CCN2 Platform is designed in a way that there are no limitations on the asynchronous messages' size that can be transported and processed.	**SHOULD**
DP4.4	The CCN2 Platform is designed in a way that there are no inherent limitations in the number of Partners.	**MUST**
DP4.5	The CCN2 Platform is designed in a way that there are no inherent limitations in the number of managed users.	**SHOULD**

Table 12: Design Principles for scalability

---

[5] Horizontal Scalability: The process of adding multiple logical units of resources and making them work as a single unit.

[6] Vertical Scalability: The process of adding a resource within the same logical unit to increase capacity.

1.3.5. *Reliability*

#	DESCRIPTION	CLASSIFICATION
DP5.1	The CCN2 Platform is designed using products that have a proven track record of maturity.	**MUST**
DP5.2	The CCN2 Platform is highly available with no single point of failure within the Platform architecture.	**MUST**
DP5.3	The CCN2 Platform is designed in a fault tolerant manner so that it continues its operations despite the presence of hardware or software faults within the Platform.	**MUST**
DP5.4	The CCN2 Platform is designed is such a way that in any event of interruption or failure the CCN2 Platform can recover in terms of functionalities and data integrity without data loss.	**MUST**
DP5.5	The CCN2 Platform is designed for continuous availability so that scheduled downtime for maintenance or upgrades is reduced as much as possible and ideally is nil. Updates must be possible without interruption of the services offered.	**MUST**
DP5.6	The availability of the Main Hubs is ensured by design and guarantees the end-to-end CCN2 Platform availability (e.g. active-active mode). The target reliability prevents accidental interruption of the exchange capability between any two Partners.	**MUST**
DP5.7	The CCN2 Platform is designed to support release toleration (i.e. the next level of the software/hardware and its prior release levels can coexist.	**SHOULD**
DP5.8	The CCN2 Platform is designed to be tolerant of the unavailability of 3rd party systems and networks and should recover automatically (i.e. re-establishing connections, processing queued messages, synchronisation of data, etc.) when these systems are available again.	**SHOULD**
DP5.9	The CCN2 Platform is designed in such a way that the failure of any component does not prevent management (including problem resolution) continuing on those components still functioning.	**SHOULD**

Table 13: Design Principles for reliability

1.3.6. *Security*

#	DESCRIPTION	CLASSIFICATION
DP6.1	The CCN2 Platform is designed in such a way that prevents unauthorised access to the CCN2 Platform and guarantees data integrity.	**MUST**

DP6.2	The CCN2 Platform is designed in such a way that ensures data and services are accessible only to those authorised to have access (confidentiality).	**MUST**
DP6.3	The CCN2 Platform is designed in such a way that it provides evidences that actions or events have taken place, so that the events or actions cannot be repudiated later (non-repudiation). The evidences shall be persistently stored data.	**MUST**
DP6.4	The CCN2 Platform is designed in such a way that it traces actions of an entity uniquely to this entity (accountability).	**MUST**
DP6.5	The CCN2 Platform is designed in such a way that the identity of a subject or resource is proven to be the one claimed (authenticity). The evidences of the authentication must be persistently stored data.	**MUST**
DP6.6	The secure communications provided by the CCN2 Platform are designed to be independent from the level of security of the underlying transport networks.	**MUST**
DP6.7	The security policy [R101] currently used is carried over by the CCN2 Platform.	**MUST**

Table 14: Design Principles for security

1.3.7. *Supportability*

#	DESCRIPTION	CLASSIFICATION
DP7.1	The design of the CCN2 Platform aims at minimising the learning effort for its deployment and operation, thus reducing the operational cost.	**SHOULD**
DP7.2	The design of the CCN2 Platform aims at minimising operations, number of tools, procedures and timing needed to test the Platform, thus reducing the testing effort.	**SHOULD**
DP7.3	The CCN2 Platform is designed so that it can be monitored and managed using user friendly tools that include a logically centralised management console for all operations, logging and reporting. Thereby reducing the operational cost.	**SHOULD**
DP7.4	The CCN2 Platform is designed so that Partners can easily connect and develop CCN2 Platform compliant applications. Thereby reducing the Partners' development and operational cost related to the CCN2 Platform.	**SHOULD**

Table 15: Design Principles for supportability

2. Functional Requirements

This chapter introduces the functional requirements of the CCN2 Platform:

1. Introduction of the modules that will be used as a basis for the requirement specification;

2. Explanation of the baseline functions of the CCN2 Platform;

3. Description of the detailed requirements for each module;

4. Presentation of a standards' summary that the CCN2 Platform must adhere to.

2.1. Introduction of modules

This section introduces the high-level functions of the CCN2 Platform. The envisioned functional break-down of the CCN2 Platform is provided in Figure 2 below.
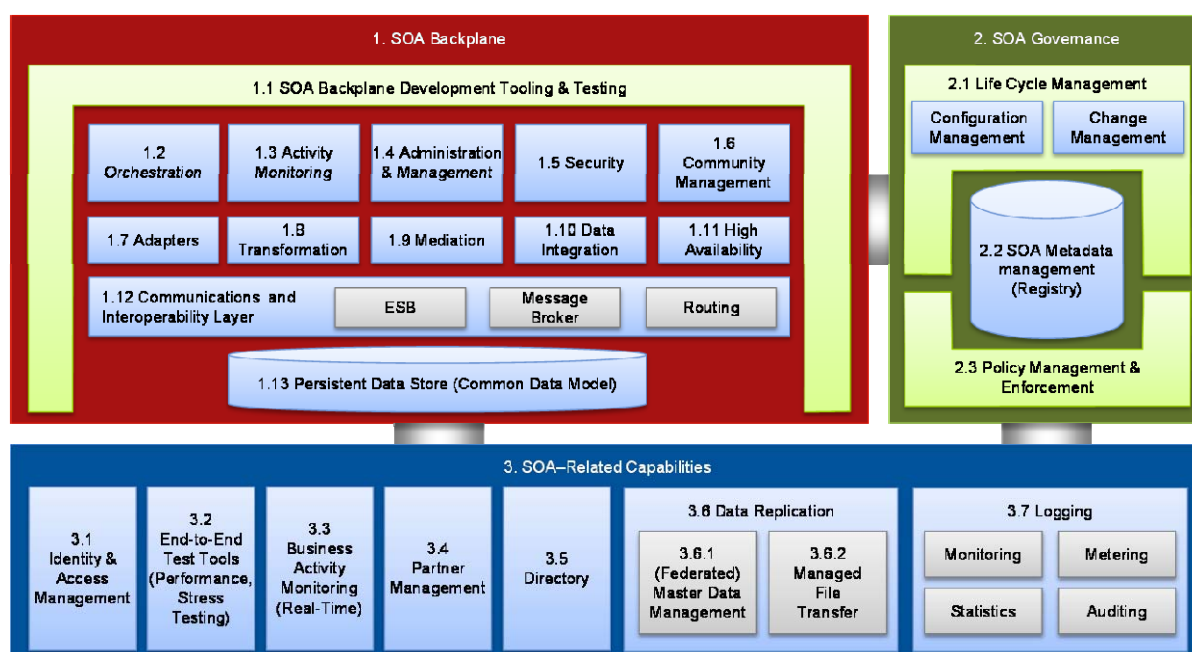
Figure 2: Envisioned CCN2 Platform Functional Break-Down

The following are the three key areas where functionality is required for the CCN2 backplane:

- SOA Backplane – which incorporates the functionalities needed to enable any-to-any, secure, reliable, scalable, manageable and high-performance communication across composite applications and processes, service provider applications and external domains in a technologically heterogeneous environment;

- SOA Governance – which includes the functionalities required to support the governance processes associated with that particular SOA initiative, including a registry/repository and SOA life cycle management tools;

- SOA-Related Capabilities – which are functionalities required to support advanced requirements of the SOA Backplane and SOA Governance, such as BAM, master data management and management of partner communities.

An introductory description of each of the functional areas is given in the sections below (requirements for each module are presented in the section 2.4 Detailed Requirements).

2.1.1. *SOA Backplane (FR1)*

FR1.1 SOA Backplane Tooling and Testing

An environment (preferably GUI based) for:

1. Designing the service interfaces, the rules (transformation, routing), the orchestration flows and the adapter configurations required to implement services using existing assets.

2. Compositing applications using existing IT assets.

3. Testing the applications and system established by the SOA infrastructure, and the applications deployed using that infrastructure.

Some parts of the Tooling will be made available to other DG TAXUD contractors such as ITSM2 and CUSTDEV2, FITSDEV2 (through appropriate means). This will allow them to develop components such as business services, flows, reports, etc...

FR1.2 Orchestration

Technology that hosts the execution of process logic spanning multiple back-end services or applications — typically for short-term (seconds or minutes) processes that can occasionally also be long term (hours, days, weeks) — with the aim of implementing composite services or automated system-to-system processes. The state should be maintained for the duration of the logic (for example, a partner interface process for EDI). Only basic support for human-based activities is required, primarily aimed at exception handling and error recovery.

FR1.3 Activity Monitoring

It refers to functionality that monitors messaging traffic, process state and behaviour, application and service parameters and behaviour for all nodes in a LAN or WAN. It is used to monitor the "health" of the overall system (services, applications, processes and application infrastructure), and to collect events and usage information aimed at populating technical key performance indicators of the deliverables supported by the SOA Backplane and of the SOA Backplane modules themselves.

FR1.4 Administration & Management

Features that assist users in deploying services and keeping the resultant system (applications, services and infrastructure) running at peak efficiency at all times by enabling the remote

monitoring and management of distributed applications, services and information sources, and by enabling the automated resolution of predefined conditions and events[7].

FR1.5 Security

Tools and technologies required to implement the necessary authentication and authorisation to control access to the services and the connected resources (for example, other services, databases), as well as the SOA Backplane functionality.

FR1.6 Community Management

It refers to Low-level B2B connection provisioning capabilities (e.g. configuration of IP addresses, AP names or locations) for protocols such as AS2 or Web services to support connections with the Partners.

FR1.7 Adapters (incl. Legacy support)

Technology that combines design tools and runtime software to implement programs that act as "glue," transforming among protocols, connecting to databases and linking pre-SOA application programming interfaces (APIs) to the SOA Backplane. This includes functionality that will allow existing Member State applications using the CCN/CSI stack to interact with the CCN2 Platform in a bi-directional manner. For example, a bespoke adapter developed using an Adapter SDK or the SOA tooling.

FR1.8 Transformation

Technology to perform syntactic and semantic hub-based transformation of messages, supporting easy-to-use development and reuse of transformation rules, numbers of built-in functions, ease of extending the transformation function with custom-coded logic.

FR1.9 Mediation

It refers to features that enable in-flight message manipulation, such as transformation (typically XML based), intelligent routing, naming and addressing.

FR1.10 Data Integration

It refers to technology that implements processing logic that directly manipulates data values and the representation of those values for storage, transport or presentation purposes. This processing logic is used to establish common access to data sources.

FR1.11 QoS/High Availability

This includes load balancing, high availability and transaction support. Functionality that provides to different applications, services, users or message flows reliability, different execution priorities, in-order delivery, transaction integrity and guarantees of a certain level of performance and availability in case of system/application failures, or when performing maintenance/upgrades of the backplane.

---

[7] For instance, automatic failover within a cluster of application servers, RAID-type functionalities

FR1.12 Communications and Interoperability Layer (ESB, Message Broker, Routing)

A platform that establishes an interoperability layer that supports interactions among components via a variety of protocols (HTTP/plain old XML [POX], SOAP, Internet Inter-ORB Protocol [IIOP], .NET remoting, message-oriented middleware [MOM] protocols, file transfer protocols and others) and interaction styles (request/reply, conversational, publish and subscribe, asynchronous messaging and others). Reliable, once-only delivery of messages should be available.

FR1.13 Persistent Database Store

Database engine to support features such as a common data model, transformation maps and guaranteed message delivery. This engine should support all CCN2 Platform modules.

2.1.2. *SOA Governance (FR2)*

FR2.1 SOA Life Cycle Mgt (Including change and configuration Mgt)

Functionality that manages the development, versioning and deployment of assets (for example, service implementations or Web Services Description Language (WSDL) files, orchestrations) used in implementing SOA-style applications. It publishes the information to the appropriate parties (architects, analysts, developers and IT operations) so that assets can be reused, and it provides traceability and impact assessment. This also includes:

1. Change management functionality to manage the change process where new versions of SOA artefacts are introduced;

2. Configuration management to support a CMDB to allow all relevant configuration details of SOA artefacts to be stored. CMDB tool should maintain an IT service configuration view that depicts the peer-to-peer and hierarchical relationships among the infrastructure components and the services.

FR2.2 SOA Metadata Mgt (Registry/Repository)

Metadata management functionality that provides the following:

1. An online catalogue of services and associated artefacts such as WSDL files;

2. A single point of access for cataloguing, promoting and publishing information about services and applications;

3. Cross-referencing information; statistical information tracking usage, performance, availability and other aspects of the services life cycle;

4. Metadata that enables an ESB to find, bind to and invoke the execution of a service implementation;

5. Metadata that enables access control for all these features.

Metadata management provides the foundation repository for both life cycle management (LCM) and policy management and enforcement.

FR2.3   Policy Management and Enforcement

It refers to technology that enables development, deployment and management of policies that externalise some aspects of SOA governance, such as access control, identity management and performance, and service-level agreements. It provides the foundation for the governance of business services.

2.1.3. *SOA Related Capabilities (FR3)*

FR3.1 Identity and Access Management

IAM technologies can be categorised into four functional classes:

1. Identity intelligence (focused on audit and assurance);

2. Identity administration (focused, prosaically enough, on administration);

3. Identity verification (focused on authentication);

4. Access management (focused on authorisation).

The first two categories can be grouped together as identity management; the latter two can be grouped together as access control.

FR3.2 End-to-End Test Tools

The Test Tools will allow:

*   the CCN2 Platform functionality to be tested end – to – end;

*   to ensure that Partners applications interoperate according to the defined technical specifications of the Platform.[8]

This would also include the ability to carry out performance and stress testing on the CCN2 Platform by injecting transactions to simulate expected and abnormal loads.

FR3.3 Business Activity Monitoring

BAM technology enables real-time monitoring of critical business performance indicators to improve the speed and effectiveness of business operations by intercepting business events being exchanged through the SOA Backplane in the form of messages. At its broadest level, BAM is the convergence of operational business intelligence and real-time application integration.

FR3.4 Partner Management

It refers to services such as partner on-boarding and provisioning that are not part of the SOA Backplane but are required for partner management. Typically used for the management of large number of partners but may have limited applicability in terms of 27 Member States

---

[8] Testing of the specific business flows is not requested.

plus a small number of additional countries. This may be interesting in terms of managing a large number of external partners (traders) - B2B feature.

FR3.5 Directory

Directory services represent an information source for identity. Identity sources include a variety of repositories; directory services provide the capability to collect, transform, manage, and publish identity information across these repositories in response to varied requirements.

FR3.6 Data Replication

FR3.6.1 Federated Master Data Management

Tooling that consistently defines and manages data that applies to high-value business entities of an organisation. MDM technology has the objective of providing processes for collecting, aggregating, matching, consolidating, quality assuring, persisting and distributing such data throughout an organisation to ensure consistency and control in the ongoing maintenance and application use of this information (management of TARIC data, CSRD data).

FR3.6.2 Managed File Transfer

Managed file transfer (MFT) features help companies control all aspects of the movement of data (frequently, but not limited to, large bulk data) internally among applications, or between internal systems and external business partners. MFT functionality usually comprises four discrete functionalities including MFT clients and servers, MFT proxies (for demilitarised zone [DMZ] security) and various plug-ins.

FR3.7 Logging (Monitoring, Metering, Statistics, Auditing)

It refers to the functionality that allows all messages that flow across the CCN2 Platform to be stored in a persistent data store and to allow subsequent analysis for trend monitoring, metering, statistics and audited. NB. "Near real time" activity monitoring is seen as a key part of the SOA Backplane and not as a separate SOA related capability.

2.2.   Baseline Requirements

REFERENCE	REQUIREMENT	CLASSIFICATION
BR-1	The CCN2 Platform provides full integration with the existing Partner applications which use the CSI API. In other words the Partner will not be required to carry out any application redevelopment to link to the CCN2 Platform (except possibly limited technological updates, such as using new versions of the CSI stacks).	**MUST**

REFERENCE	REQUIREMENT	CLASSIFICATION
BR-2	The specific functionality of the existing HTTP/HTTP(S) exchange features currently used in CCN/CSI will be supported in the CCN2 Platform (See [R229], [R381] and other related documents).	**MUST**
BR-3	The CCN2 Platform is integrated with the SPEED2[9] platform using a standard protocol available on both systems.	**MUST**
BR-4	The CCN2 Platform IAM module must provide fine grained roles and responsibilities defining access rights so that specific functions (i.e. IAM, SOA metadata management/service registry, MDM, Monitoring/Statistics etc.) can be delegated to the Partners.	**MUST**
BR-5	The CCN2 Platform must provide at least the same level of reporting and statistics as currently provided by CCN/CSI.	**MUST**
BR-6	The CCN2 Platform must record events for auditing and statistic purposes and export the events using flat files in existing CCN/CSI proprietary formats (See [R165] and other related documents) so that they can be used by the existing CS/MIS and CS/MISE application.	**MUST**
BR-7	The CCN2 Platform operates on the existing CCN network topology (as described in [R171]).	**SHOULD**

Table 16: Baseline requirements

2.3. Access Point (AP) Requirements

The AP provides the following minimum as outlined in the table below:

REFERENCE	REQUIREMENT	CLASSIFICATION
APR-1	Message persistency until the message has been successfully processed (no message is lost).	**MUST**
APR-2	Security (controlled access to the CCN2 Platform)	**MUST**
APR-3	Simple routing (to any of Hub, depending on availability and load).	**MUST**
APR-4	Provide CCN2 Platform interfaces (including the CCN/CSI interfaces as described in the Baseline).	**MUST**
APR-5	Monitoring, Auditing, Logging with support for non-	**MUST**

---

[9] SPEED2 is described in [R374], [R375] and [R376]

REFERENCE	REQUIREMENT	CLASSIFICATION
	repudiation.	
APR-6	The implementation of the Access Point should be as independent as possible of the Partner specific particularities so as to reduce the management of the AP.	**MUST**
APR-7	The CCN2 Platform is accessible with open protocols.	**MUST**
APR-8	The CCN2 Platform supports integration with COBOL programs running on IBM Mainframes currently used in some MS (today supported by the COBOL CSI stack).	**MUST**
APR-9	Direct Access Point to Access Point communication (not going through a Main Hub) is supported. The decision to implement direct communication mechanisms does not restrict the Access Point functionalities. (The direct AP to AP communication can be for instance based on routing decisions, on the type of technology of the interaction (e.g. simple HTTP traffic, REST web services, etc.), and various other parameters.)	**SHOULD**
APR-10	The Access Point stores Partner specific configuration, if needed.	**SHOULD**
APR-11	The Access Point provides storage / "cache" information for other services (e.g. service registry, MDM, etc.).	**SHOULD**
APR-12	The Access Point provides conversion of the CSI API message to formats and structure used in CCN2 Platform.	**MAY**
APR-13	The Access Point provides simple transformation.	**MAY**

Table 17: Access Point requirements

2.4. Detailed Requirements

2.4.1. *SOA Backplane (FR1)*

2.4.1.1. FR1.1 SOA Backplane Tooling and Testing

#	REQUIREMENT	CLASSIFICATION
FR1.1-1	The SOA Backplane has an integrated service environment (ISE) for component-based development assembly, discovery, composition and orchestration.	**MUST**
FR 1.1-2	The ISE provides revision control functionality.	**MUST**
FR 1.1-3	The ISE provides defect tracking support.	**MUST**

#	REQUIREMENT	CLASSIFICATION
FR 1.1-4	The ISE must support a Web Services Interoperability Organisation (WS-I)-compliant implementation of basic Web services standards, including SOAP, WSDL and Universal Description, Discovery and Integration (UDDI), as well as higher-level Web services standards, such as WS-Security.	**MUST**
FR 1.1-5	The ISE supports RESTful services.	**MUST**
FR 1.1-6	The ISE provides a modern interface surface supporting the graphical composition of flows and services.	**MUST**
FR 1.1-7	All modules of the CCN2 Platform will have a development toolset.	**MUST**
FR 1.1-8	The ISE supports an execution environment (e.g. support for running code without leaving the ISE).	**SHOULD**
FR 1.1-9	The ISE provides visually oriented tools for creating software systems and components.	**SHOULD**
FR 1.1-10	The ISE provides the ability to compile individual source files, larger components or modules, and an entire project via built-in commands.	**SHOULD**
FR 1.1-11	The ISE has the ability to connect to one or more software configuration management (SCM) system (e.g. as a built-in feature).	**SHOULD**
FR 1.1-12	The ISE supports the plug in of application and component frameworks (including open source).	**SHOULD**
FR 1.1-13	The ISE supports unit testing.	**MUST**
FR 1.1-14	The ISE supports unit testing by including Consoles for viewing detailed test output.	**SHOULD**
FR 1.1-15	The ISE supports unit testing by support for executing tests in a runtime container, such as an integrated application server.	**SHOULD**
FR 1.1-16	The ISE has functionality to support component and integration testing.	**SHOULD**
FR 1.1-17	The ISE supports interoperability testing, .for instance between the SOA Backplane and the applications (for instance, XML message injection, SAML proxying, dummy SOA services).	**SHOULD**
FR 1.1-18	The ISE provides root-cause analysis.	**SHOULD**
FR 1.1-19	The ISE provides regression test tools that enable functional tests to be executed as a part of build, test management, and life cycle management tools and processes.	**SHOULD**
FR 1.1-20	The ISE provides simulation tools to test atomic and	**SHOULD**

#	REQUIREMENT	CLASSIFICATION
	composite services.	
FR 1.1-21	The ISE provides modelling tools to support data architecture design.	**SHOULD**
FR 1.1-22	The ISE supports other service encapsulation mechanisms (e.g. CORBA, EJB).	**MAY**
FR 1.1-23	The ISE has or integrates with static and dynamic code analysis functionality, such as that which ensures proper code formatting and style and exposes common programming errors.	**MAY**
FR 1.1-24	The SOA Backplane supports the integration of external integrated development environment (IDE) (i.e. the external development environments such as Eclipse are capable of being used as the development environment for the SOA Backplane).	**MAY**
FR 1.1-25	All CCN2 Platform development toolsets will be integrated.	**MAY**

Table 18: SOA Backplane requirements

2.4.1.2.FR1.2 Orchestration

#	REQUIREMENT	CLASSIFICATION
FR 1.2-1	The Orchestration Module of the SOA Backplane has the ability to execute compensating transactions.	**MUST**
FR 1.2-2	The Orchestration Module of the SOA Backplane supports Microflow (i.e. fast executing (sub second/seconds), short living (seconds) "microflows").	**MUST**
FR 1.2-3	The Orchestration Module of the SOA Backplane provides a flow design tool where the process flow and conditional rules can be developed for execution at runtime or the creation of compiled modules.	**MUST**
FR 1.2-4	The Orchestration Module of the SOA Backplane provides Flow monitoring, tracking and diagnostics functionality (i.e. The ability to monitor, track and manage the service flows at runtime).	**MUST**
FR 1.2-5	The Orchestration Module of the SOA Backplane supports graphical design interface for specifying process flows.	**SHOULD**
FR 1.2-6	The Orchestration Module of the SOA Backplane provides the capability to Integrate the Flow monitoring, tracking and diagnostics functionality with external monitoring and	**SHOULD**

#	REQUIREMENT	CLASSIFICATION
	management systems.	
FR 1.2-7	The Orchestration Module of the SOA Backplane can be Integrated with workflow and business process management tools which allow human interaction.	**MAY**

Table 19: Orchestration requirements

2.4.1.3.FR1.3 Activity Monitoring

#	REQUIREMENT	CLASSIFICATION
FR 1.3-1	The Activity Monitoring Module of the SOA Backplane provides monitoring tools to view, control and monitor the availability of resources on the SOA Backplane.	**MUST**
FR 1.3-2	The Activity Monitoring Module of the SOA Backplane is capable of monitoring message traffic on a continual basis.	**MUST**
FR 1.3-3	The Activity Monitoring Module of the SOA Backplane is capable of monitoring service usage on a continual basis.	**MUST**
FR 1.3-4	The Activity Monitoring Module of the SOA Backplane is capable of providing metrics in terms of service usage (performance, utilisation, errors, and resource usage).	**MUST**
FR 1.3-5	The Activity Monitoring Module of the SOA Backplane is capable of monitoring process state and behaviour.	**MUST**
FR 1.3-6	The Activity Monitoring Module of the SOA Backplane provides functionality to define key performance indicators (KPIs) and alerts on events failing KPIs.	**MUST**
FR 1.3-7	The Activity Monitoring Module of the SOA Backplane provides tools for tracing/debugging levels of the various modules of the SOA Backplane.	**MUST**
FR 1.3-8	The Activity Monitoring Module of the SOA Backplane provides tools that can proactively predict future failures by analysing error trends or similar behaviour.	**SHOULD**

Table 20: Activity monitoring requirements

2.4.1.4.FR1.4 Administration & Management

#	REQUIREMENT	CLASSIFICATION
FR 1.4-1	The Administration and Management Module of the SOA Backplane provides rules for automated system monitoring where thresholds are set on which alerts are generated (i.e. resource consumption, errors).	**MUST**
FR 1.4-2	The Administration and Management Module of the SOA Backplane is capable of Integration with external monitoring systems.	**SHOULD**
FR 1.4-3	The Administration and Management Module of the SOA Backplane provides a console that enables a filtered management console based on defined criteria such as a specific Partner or a business domain.	**SHOULD**
FR 1.4-4	The Administration and Management Module of the SOA Backplane provides the functionality for automated message repair and resend. These messages, which are received in an incomplete or inaccurate state, can be analysed against reference data contained within the backplane and corrected and resend without further reference to the originator.	**MAY**

Table 21: Administration and management requirements

2.4.1.5.FR1.5 Security

#	REQUIREMENT	CLASSIFICATION
FR 1.5-1	The Security Module of the SOA Backplane provides authentication functionality.	**MUST**
FR 1.5-2	The Security Module of the SOA Backplane provides authorisation functionality.	**MUST**
FR 1.5-3	The Security Module of the SOA Backplane provides access control functionality (authorisation granting and check) to verify that systems/users are allowed to perform the requested operations.	**MUST**
FR 1.5-4	The Security Module of the SOA Backplane is integrated with the IAM module within the CCN2 Platform to provide authentication functionality.	**MUST**
FR 1.5-5	The Security Module of the SOA Backplane integrates with the IAM module within the CCN2 Platform to provide authorisation functionality.	**MUST**
FR 1.5-6	The Security Module of the SOA Backplane integrates with	**MUST**

#	REQUIREMENT	CLASSIFICATION
	the IAM module within the CCN2 Platform to provide access control functionality to verify that systems/users are allowed to perform the requested operations.	
FR 1.5-7	The Security Module of the SOA Backplane provides functionality for logging of any detected violation attempt (authentication, integrity, confidentiality etc).	**MUST**
FR 1.5-8	The Security Module of the SOA Backplane provides Message level encryption/decryption.	**MUST**
FR 1.5-9	The Security Module of the SOA Backplane provides transport / session / message / payload level encryption/decryption.	**MUST**
FR 1.5-10	The Security Module of the SOA Backplane provides guaranteed message integrity.	**MUST**
FR 1.5-11	The Security Module of the SOA Backplane supports digital signatures.	**MUST**
FR 1.5-12	The Security Module of the SOA Backplane supports credential mapping for the SOA Backplane.	**MUST**
FR 1.5-13	The Security Module of the SOA Backplane supports credential mapping for services.	**MUST**
FR 1.5-14	The Security Module of the SOA Backplane supports credential propagation for services.	**MUST**
FR 1.5-15	The security model of CCN/CSI is carried over.	**MUST**

Table 22: Security requirements

2.4.1.6. FR1.6 Community Management

#	REQUIREMENT	CLASSIFICATION
FR 1.6-1	The Community Management Module of the SOA Backplane provides functionality for connectivity/communications setup for entities that use the CCN2 Platform.	**MUST**
FR 1.6-2	The Community Management Module of the SOA Backplane provides functionality for billing for service usage for partners who use the CCN2 Platform.	**SHOULD**
FR 1.6-3	The Community Management Module of the SOA Backplane provides functionality to manage the provisioning of entities who will communicate using the CCN2 Platform.	**MAY**

Table 23: Community management requirements

2.4.1.7.FR1.7 Adapters (Including Legacy support)

#	REQUIREMENT	CLASSIFICATION
FR 1.7-1	The Adapters Module of the SOA Backplane provides legacy adapters - (Pre SOA API Adapters). The SOA Backplane Adapters module must have the ability to develop integration adapters to legacy systems which are not based on SOA encapsulation of logic but which have a defined low level application programming interface. The existing CCN/CSI would be an example of a low level API.	**MUST**
FR 1.7-2	The Adapters Module of the SOA Backplane provides a JDBC adapter.	**MUST**
FR 1.7-3	The Adapters Module of the SOA Backplane provides an ODBC adapter.	**MUST**
FR 1.7-4	The Adapters Module of the SOA Backplane provides an SMTP adapter.	**MUST**
FR 1.7-5	The Adapters Module of the SOA Backplane provides an adapter to the CCN Mail III platform that is based on a Microsoft Exchange infrastructure.	**MUST**
FR 1.7-6	The Adapters Module of the SOA Backplane provides an FTP/SFTP/FTPS adapter.	**MUST**
FR 1.7-7	The Adapters Module of the SOA Backplane provides an SNMP adapter.	**MUST**
FR 1.7-8	The Adapters Module of the SOA Backplane provides an LDAP adapter.	**MUST**
FR 1.7-9	The Adapters Module of the SOA Backplane provides an adapter software development kit to develop custom adapters.	**MUST**
FR 1.7-10	The Adapters Module of the SOA Backplane provides an EDIFACT adapter.	**MUST**
FR 1.7-11	The Adapters Module of the SOA Backplane provides a generic and configurable XML adapter.	**MUST**
FR 1.7-12	The Adapters Module of the SOA Backplane provides interoperability with CICS and IMS (as used by the CSI stacks) running on IBM platforms in some MS (today supported by the COBOL CSI stack).	**MUST**
FR 1.7-13	The Adapters Module of the SOA Backplane provides other Database adapters (DB2, SQL-Server or equivalent).	**SHOULD**
FR 1.7-14	The Adapters Module of the SOA Backplane provides a Tuxedo adapter.	**SHOULD**

#	REQUIREMENT	CLASSIFICATION
FR 1.7-15	The Adapters Module of the SOA Backplane provides an MQ-Series adapter.	**SHOULD**
FR 1.7-16	The Adapters Module of the SOA Backplane provides an adapter to MOM protocols (e.g. AMQP).	**SHOULD**
FR 1.7-17	The Adapters Module of the SOA Backplane supports .NET adapter.	**SHOULD**
FR 1.7-18	The Adapters Module of the SOA Backplane provides an AS/2 adapter.	**SHOULD**
FR 1.7-19	The Adapters Module of the SOA Backplane provides an AS/3 adapter.	**SHOULD**
FR 1.7-20	The Adapters Module of the SOA Backplane provides a RosettaNet adapter.	**SHOULD**
FR 1.7-21	The Adapters Module of the SOA Backplane provides packaged application adapters. That is prebuilt adapters which have defined integration points with commercial of the shelf software packages such as packaged Customs or Taxation specific software or other generic software (such as ERP).	**MAY**
FR 1.7-22	The Adapters Module of the SOA Backplane provides packaged composite applications and packaged integrating processes.	**MAY**
FR 1.7-23	The Adapters Module of the SOA Backplane provides an AS/1 adapter.	**MAY**

Table 24: Adapters requirements

2.4.1.8. FR1.8 Transformation

#	REQUIREMENT	CLASSIFICATION
FR 1.8-1	The Transformation Module of the SOA Backplane provides built-in transformation functions (for example, sum, average, concatenation).	**MUST**
FR 1.8-2	The Transformation Module of the SOA Backplane provides rules engine based transformation.	**MUST**
FR 1.8-3	The Transformation Module of the SOA Backplane provides a scripting and/or programming language to support transformation.	**MUST**
FR 1.8-4	The Transformation Module of the SOA Backplane validates the message structure against predefined format.	**MUST**

#	REQUIREMENT	CLASSIFICATION
FR 1.8-5	The Transformation Module of the SOA Backplane supports EDIFACT to XML transformation and XML to EDIFACT Transformation.	**MUST**
FR 1.8-6	The Transformation Module of the SOA Backplane supports character set conversion to and from Unicode.	**MUST**
FR 1.8-7	The Transformation Module of the SOA Backplane supports ASCII – encoded data conversion.	**MUST**
FR 1.8-8	The Transformation Module of the SOA Backplane supports EBCDIC – encoded data conversion.	**MUST**
FR 1.8-9	The Transformation Module of the SOA Backplane supports UTF-8 – encoded data conversion.	**MUST**
FR 1.8-10	The Transformation Module of the SOA Backplane supports pre-defined transformations to and from B2B formats and protocols (e.g. EDI and RosettaNet, or equivalent).	**SHOULD**

Table 25: Transformation requirements

2.4.1.9. FR1.9 Mediation

#	REQUIREMENT	CLASSIFICATION
FR 1.9-1	The Mediation Module of the SOA Backplane supports In-flight message manipulation (i.e. the ability to transform the message while being processed by the SOA Backplane).	**MUST**
FR 1.9-2	The Mediation Module of the SOA Backplane supports Intelligent routing (i.e. the ability to route messages based on rules as well as the content).	**MUST**
FR 1.9-3	The Mediation Module of the SOA Backplane supports service virtualisation (i.e. the capability of the SOA Backplane, during operations, to assist service consumers by finding, binding to and invoking the execution of service providers).	**MUST**
FR 1.9-4	The Mediation Module of the SOA Backplane provides supports for message aggregation.	**MUST**
FR 1.9-5	The Mediation Module of the SOA Backplane supports message splitting and reassembly for final delivery (configurable at run time).	**MUST**
FR 1.9-6	The Mediation Module of the SOA Backplane provides semantic validation of the messages against predefined rules.	**MUST**

Table 26: Mediation requirements

2.4.1.10. FR1.10 Data Integration

#	REQUIREMENT	CLASSIFICATION
FR 1.10-1	The Data Integration Module of the SOA Backplane provides data source connectivity to multiple data source types via adapters and other mechanisms.	**MUST**
FR 1.10-2	The Data Integration Module of the SOA Backplane provides an Extraction, transformation and loading (ETL) tool.	**MUST**
FR 1.10-3	The Data Integration Module of the SOA Backplane supports caching (i.e. the ability to cache federated results and various subsets of the source data to improve performance).	**MUST**
FR 1.10-4	The Data Integration Module of the SOA Backplane supports data access tooling that enables the recording (storage) or retrieving (reading) of information (data) from data stores (i.e. distributed query functionality against multiple data sources).	**MAY**
FR 1.10-5	The Data Integration Module of the SOA Backplane provides semantic/logical Tooling (i.e. data infrastructure tooling that enables users to represent semantic models, identify model-to-model relationships, and execute the necessary translations to reconcile data with differing semantic models).	**MAY**
FR 1.10-6	The Data Integration Module of the SOA Backplane provides the functionality to split processing of large files into multiple parallel streams of operation.	**MAY**

Table 27: Data integration requirements

2.4.1.11. FR1.11 QoS/High Availability

#	REQUIREMENT	CLASSIFICATION
FR 1.11-1	The CCN2 Platform is capable of operating in a load balanced configuration in an active/active mode without modification.	**MUST**
FR 1.11-2	The CCN2 Platform is capable of operating in a high availability configuration (e.g. clustering, active/active mode, horizontal scale-out).	**MUST**
FR 1.11-3	The CCN2 Platform support processing prioritisation based on priority rules (e.g. message processing).	**MUST**
FR 1.11-4	The Quality of Service can be maintained using dynamic resource allocation.	**MUST**

#	REQUIREMENT	CLASSIFICATION
FR 1.11-5	The CCN2 Platform supports message prioritisation based a configurable business rules engine with at least ten priority levels.	**MUST**
FR 1.11-6	The CCN2 Platform supports message prioritisation based on the message contents.	**MUST**
FR 1.11-7	The Quality of Service can be maintained by throttling when resource thresholds are exceeded.	**SHOULD**

Table 28: QoS/High availability requirements

2.4.1.12. FR1.12 Communications and Interoperability Layer (ESB, Message Broker, Routing)

#	REQUIREMENT	CLASSIFICATION
FR 1.12-1	The Communications and Interoperability Layer supports configurable message queues.	**MUST**
FR 1.12-2	The Communications and Interoperability Layer supports a message catalogue (i.e. SOAP message schemas).	**MUST**
FR 1.12-3	The Communications and Interoperability Layer supports message correlation.	**MUST**
FR 1.12-4	The Communications and Interoperability Layer supports reliable messaging with guaranteed delivery.	**MUST**
FR 1.12-5	The Communications and Interoperability Layer guarantees In-order delivery of messages.	**MUST**
FR 1.12-6	The Communications and Interoperability Layer supports the production of delivery notifications (e.g. when message is delivered to a queue; confirmation of arrival, confirmation of delivery).	**MUST**
FR 1.12-7	The Communications and Interoperability Layer supports message compression/decompression.	**MUST**
FR 1.12-8	The Communications and Interoperability Layer supports end-to-end tracking of data and messages.	**MUST**
FR 1.12-9	The Communications and Interoperability Layer supports message ordering for given message sets (messages will be processed in the defined order irrespective of when they are received).	**MUST**
FR 1.12-10	The Communications and Interoperability Layer supports message Re-sequencing.	**MUST**

#	REQUIREMENT	CLASSIFICATION
FR 1.12-11	The Communications and Interoperability Layer supports one way messaging.	**MUST**
FR 1.12-12	The Communications and Interoperability Layer supports Request/Reply Interaction Style.	**MUST**
FR 1.12-13	The Communications and Interoperability Layer supports the request/call-back interaction style.	**MUST**
FR 1.12-14	The Communications and Interoperability Layer supports conversational Interaction Style (i.e. non-blocking).	**MUST**
FR 1.12-15	The Communications and Interoperability Layer supports synchronous Interaction.	**MUST**
FR 1.12-16	The Communications and Interoperability Layer supports Asynchronous Interaction.	**MUST**
FR 1.12-17	The Communications and Interoperability Layer supports address based routing (i.e. the ability to route a message to multiple destinations based on a message attribute described in the subject area of the message).	**MUST**
FR 1.12-18	The Communications and Interoperability Layer supports content based routing (i.e. the ability to route a message based on a value or values within a message).	**MUST**
FR 1.12-19	The Communications and Interoperability Layer supports header based routing.	**MUST**
FR 1.12-20	The Communications and Interoperability Layer supports E-mail (e.g. an e-mail can be routed across the backplane or where the contents or attachment of the e-mail can be used by the SOA Backplane to deliver messages or execute transactions with specific entities).	**MUST**
FR 1.12-21	The Communications and Interoperability Layer supports message routing based on a business rules engine.	**MUST**
FR 1.12-22	The Communications and Interoperability Layer supports reliable messaging (e.g. Once and Once Only Delivery).	**MUST**
FR 1.12-23	The Communications and Interoperability Layer supports varying message payloads.	**MUST**
FR 1.12-24	The Communications and Interoperability Layer supports store and forward messaging (i.e. the ability to persist a message and then send it to destinations).	**MUST**
FR 1.12-25	The Communications and Interoperability Layer supports request-driven RPC services-style interfaces.	**MUST**

#	REQUIREMENT	CLASSIFICATION
FR 1.12-26	The Communications and Interoperability Layer supports Web services interfaces which conform to the WS* specifications (as stated in 2.5 CCN2 Platform required standards).	**MUST**
FR 1.12-27	The Communications and Interoperability Layer provides the ability to post events to event sinks (both internal and external to the CCN2 Platform).	**MUST**
FR 1.12-28	The Communications and Interoperability Layer provides the ability to listen to events and carry out defined actions of the receipt of these events.	**MUST**
FR 1.12-29	The Communications and Interoperability Layer supports distributed transactions for the internal backplane communication in order to guarantee no data loss or no data duplication.	**MUST**
FR 1.12-30	The Communications and Interoperability Layer supports distributed transactions for interactions between the CCN2 Platform and Partners systems using widely accepted standards. (e.g. XA protocols)	**SHOULD**
FR 1.12-31	The Communications and Interoperability Layer provides Error handling (i.e. Functionality to report and carry out actions on faulty messages).	**MUST**
FR 1.12-32	The CCN2 Platform must support the POX and REST application interaction paradigms.	**MUST**
FR 1.12-33	The Communications and Interoperability Layer supports Subscribe/Publish Style based on a configurable rules engine (to determine the distribution of messages).	**SHOULD**
FR 1.12-34	The Communications and Interoperability Layer supports batch processing.	**SHOULD**
FR 1.12-35	The Communications and Interoperability Layer supports a job scheduling.	**SHOULD**
FR 1.12-36	The Communications and Interoperability Layer supports multi-tenancy (to deploy as a cloud service).	**MAY**

Table 29: Communications and Interoperability layer requirements

2.4.1.13. FR1.13 Persistent Database Store

#	REQUIREMENT	CLASSIFICATION
FR 1.13-1	The CCN2 Platform provides a persistent data store. Providing typical DB features.	**MUST**
FR 1.13-2	The Access Point will provide data persistence in the event that the central SOA Backplane is unavailable.	**MUST**
FR 1.13-3	The persistent data store supports remote access via common standards (e.g. ODBC, JDBC).	**MUST**

Table 30: Persistent Database Store requirements

2.4.2. *SOA Governance (FR2)*

2.4.2.1. FR2.1 SOA Life Cycle Mgt (Including change and configuration Mgt)

#	REQUIREMENT	CLASSIFICATION
FR 2.1-1	The SOA Governance Module supports service Lifecycle Management -to control service or artefact from one stage to the next via policy compliance testing and/or approval processes.	**MUST**
FR 2.1-2	The SOA Governance Module supports Life Cycle Process Specification which is customisable in the form of a process model.	**MUST**
FR 2.1-3	The SOA Governance Module supports version control functionality controlling multiple versions of a services asset.	**MUST**
FR 2.1-4	The SOA Governance Module supports functionality to support the release management process.	**MUST**
FR 2.1-5	The SOA Governance Module supports dependency tracking with the means to identify dependencies and relationships among services, service artefacts, and service consumers.	**MUST**
FR 2.1-6	The SOA Governance Module supports audit trail functionality to maintain a history and audit trail of the lifecycle of a service or artefacts. This supports compliance with the LAT policy of DG TAXUD.	**MUST**
FR 2.1-7	The SOA Governance Module's asset publication functionality supports the import/export of data so that it can be shared with other assets tools such as **ITSM2** DML and CMDB tools (Clear Case, ClearQuest, HP Service Centre CMDB module) as specified in "Annex II.B - Technical Annex".	**MUST**

#	REQUIREMENT	CLASSIFICATION
FR 2.1-8	The SOA Governance Module supports functionality to notify and publish asset changes to the appropriate actors (architects, analysts, developers and IT operations roles) in parties such as Partner, DG TAXUD and its contractors.	**SHOULD**
FR 2.1-9	The SOA Governance Module's life cycle management functionality can be integrated with current ITIL V2/V3 processes.	**SHOULD**
FR 2.1-10	The SOA Governance Module supports impact Assessment in terms of the functionality to identify the impact of changes, including the dependencies on other software (services and partners), as well as the dependence of other software on the changing component (service or partner).	**MAY**

Table 31: SOA Life Cycle Management requirements

2.4.2.2.FR2.2 SOA Metadata Mgt (Registry/Repository)

#	REQUIREMENT	CLASSIFICATION
FR 2.2-1	The SOA Governance Module has a Metadata repository which is Integrated with the SOA Backplane providing tools and applications to manage the life cycle of service artefacts and to group and manage metadata.	**MUST**
FR 2.2-2	The SOA Governance Module has a Metadata repository which supports web service definitions and type descriptions.	**MUST**
FR 2.2-3	The SOA Governance Module has a Metadata repository which supports Interface descriptions.	**MUST**
FR 2.2-4	The SOA Governance Module has a Metadata repository which supports binding descriptions.	**MUST**
FR 2.2-5	The SOA Governance Module has a Metadata repository which supports endpoint[10] descriptions.	**MUST**
FR 2.2-6	The SOA Governance Module has a metadata repository which supports service name and description.	**MUST**
FR 2.2-7	The SOA Governance Module has a metadata repository which supports type of service (application, data, composite, process, and infrastructure).	**MUST**
FR 2.2-8	The SOA Governance Module has a metadata repository which supports organisational entities (consumers, providers	**MUST**

---

[10] As defined by the W3C (see http://www.w3.org/TR/ws-gloss/)

#	REQUIREMENT	CLASSIFICATION
	etc.), Key stakeholders (roles and responsibilities), and contact information (business owner and technical owner).	
FR 2.2-9	The SOA Governance Module has a metadata repository which supports service version information.	**MUST**
FR 2.2-10	The metadata repository provides functionality for discovery in terms of browsing the service catalogue or searching for information that matches specific criteria.	**MUST**
FR 2.2-11	The metadata repository has a security module to control access to service information integrated with the IAM module.	**MUST**
FR 2.2-12	The metadata repository supports an online catalogue of services and associated artefacts such as WSDL files, XSDs, BPEL files.	**MUST**
FR 2.2-13	The metadata repository provides a single logical point of controlled access for cataloguing, promoting, publishing and searching for asset information.	**MUST**
FR 2.2-14	The SOA Governance Module supports software has a service registry (as an integral part of the repository) providing the functionality to locate a specific service endpoint at run time.	**MUST**
FR 2.2-15	The SOA Governance Module supports software has a service registry (as an integral part of the repository) providing the functionality to retrieve service metadata and policies associated with a service endpoint and dynamically bind to the service at run time.	**MUST**
FR 2.2-16	The service registry is not to be restricted to the management of web services only.	**MUST**
FR 2.2-17	The metadata repository and service registry are integrated with the CCN2 Platform development environment.	**MUST**
FR 2.2-18	The SOA Governance Module has a metadata repository which supports defining runtime policies (routing, transformations, security, reliability, transactions, service level objectives [SLOs], etc.).	**SHOULD**
FR 2.2-19	The SOA Governance Module has a metadata repository which supports defining Service level agreements (SLAs, availability, capacity, responsiveness, transaction rate, etc).	**SHOULD**
FR 2.2-20	The SOA Governance Module has a metadata repository which supports defining utilisation contracts (terms and conditions between consumer and provider).	**SHOULD**
FR 2.2-21	The service registry is capable of synchronisation with other	**SHOULD**

#	REQUIREMENT	CLASSIFICATION
	service registries, such as registries in Partners' infrastructure.	
FR 2.2-22	The SOA Governance Module has a metadata repository which supports code samples and tests.	**MAY**
FR 2.2-23	The SOA Governance Module supports the management of pre SOA API sets.	**MAY**

Table 32: SOA Metadata Management requirements

2.4.2.3.FR2.3 Policy Management and Enforcement

#	REQUIREMENT	CLASSIFICATION
FR 2.3-1	The SOA Governance Module provides policy lifecycle support.	**MUST**
FR 2.3-2	The SOA Governance Module supports Runtime Policy Enforcement to ensure that policies are properly enforced at runtime.	**MUST**
FR 2.3-3	The SOA Governance Module has the ability to produce reports on key metrics such as: • Number of services by lifecycle stage • Number of consumers using a service • Average number of consumers per service • Number of services using a schema type • Total number of policy violations • Number of policy violations • Number of policy waiver requests • Number of policy waiver approvals • Number of enhancement requests • Number of versions of a service or artefact • Number of services meeting or not meeting SLAs • Number of security violations	**MUST**

#	REQUIREMENT	CLASSIFICATION
	• Number of faults	
FR 2.3-4	The SOA Governance Module provides contract management functionality in terms of contract definition between the consumer and the provider.	**SHOULD**

Table 33: Policy Management and Enforcement requirements

2.4.3. *SOA Related Capabilities (FR3)*

2.4.3.1. FR3.1 Identity and Access Management

#	REQUIREMENT	CLASSIFICATION
FR 3.1-1	The IAM Module provides user-provisioning or account-provisioning to creates, modify, disable and delete user accounts and their profiles.	**MUST**
FR 3.1-2	The IAM Module features a graphical user interface accessible remotely and securely.	**MUST**
FR 3.1-3	The IAM Module has user accounts associated with each user/subject.	**MUST**
FR 3.1-4	The IAM Module supports authentication credentials for information system access.	**MUST**
FR 3.1-5	The IAM Module supports RBAC and/or ABAC to provide the functionality to grant, resolves, enforces, revoke and administer fine-grained access entitlements (i.e., privileges, access rights based on various attributes such as country or business domain, permissions, time constraints and/or rules).	**MUST**
FR 3.1-6	The IAM Module is capable of managing group membership or role assignments, from which entitlements may flow.	**MUST**
FR 3.1-7	The IAM Module supports user profile attributes (for example, name, address, phone number, title and department).	**MUST**
FR 3.1-8	The IAM Module supports the definition and enforcement of access policies or rule sets (for example, time-of-day restrictions, password management policies, how business relationships define users' access resources and SOD).	**MUST**
FR 3.1-9	The IAM Module supports delegated administration of the user-provisioning system to Partners and/or domains (for instance to create users, unblock users, set the number of password attempts before account blocking, etc.).	**MUST**

FR 3.1-10	The IAM Module supports user provisioning Workflow — Provisioning and approval. (e.g. registration, re-certification, revocation etc.)	**MUST**
FR 3.1-11	The IAM Module supports automated disablement on defined criteria.	**MUST**
FR 3.1-12	The IAM Module supports user provisioning reporting functionality to allow for the listing, reporting and printing of user, role and group information.	**MUST**
FR 3.1-13	The IAM Module supports credential management.	**MUST**
FR 3.1-14	The IAM Module supports knowledge based authentication (i.e. username/password).	**MUST**
FR 3.1-15	The IAM Module supports X.509 v3 certificate based authentication (i.e. PKI).	**MUST**
FR 3.1-16	The IAM Module supports single sign-on/single sign-off.	**MUST**
FR 3.1-17	The IAM Module should have the capability to synchronise user profile and security attributes among multiple repositories (e.g. Partners, business domains, etc)	**MUST**
FR 3.1-18	The IAM Module provides interfaces and functionalities that are typically used for federated identity management to manage federated identity information from different Partner domains and entities. E.g. the module supports synchronization of the changes in Partner's system(s) such as additions, changes and deletions of user IDs, roles, attributes etc.	**MUST**
FR 3.1-19	The IAM Module features services interface which allows its functionality to be accessible from other modules of the CCN2 Platform (i.e. the SOA Backplane, MDM module, etc.).	**MUST**
FR 3.1-20	The IAM Module must manage all users, roles, profiles and access rights for all CCN2 Platform modules and also for services offered over the CCN2 Platform.	**MUST**
FR 3.1-21	The IAM Module provides log management functionality for the collection, reporting and analysis of log data on security events.	**MUST**
FR 3.1-22	The IAM Module supports one time password tokens.	**SHOULD**
FR 3.1-23	The IAM Module supports user self-service technologies for password retrieval.	**SHOULD**
FR 3.1-24	The IAM Module supports user self-service technologies for password reset.	**SHOULD**
FR 3.1-25	The IAM Module supports user self-service technologies for password changes.	**SHOULD**

FR 3.1-26	The IAM Module supports the export of data to external entities or systems.	**SHOULD**
FR 3.1-27	The IAM Module supports smart cards with PK credentials.	**MAY**

Table 34: Identity and Access Management requirements

2.4.3.2. FR3.2 End to End Test Tools

#	REQUIREMENT	CLASSIFICATION
FR 3.2-1	The Test Tooling provides end to end testing across all modules in the CCN2 Platform.	**MUST**
FR 3.2-2	The Test Tooling provides a test design workbench.	**MUST**
FR 3.2-3	The Test tooling supports automated testing.	**MUST**
FR 3.2-4	The Test Tooling provides Service/Message load generators for load/performance/stress/endurance testing.	**MUST**
FR 3.2-5	The Test Tooling provides test analysis tools and automated test report production.	**MUST**
FR 3.2-6	The Test Tooling provides traceability and defect tracking.	**MUST**
FR 3.2-7	The Test Tooling provides management of test data sets.	**MUST**
FR 3.2-8	The Test Tooling provides support to test process flows.	**MUST**
FR 3.2-9	The Test Tooling facilitates the testing of web services, business logic, data services and implementation layers to ensure that components in those layers are working correctly (validation) and that specified requirements are met (verification).	**MUST**
FR 3.2-10	The Test Tooling provides automated generation of test data sets.	**SHOULD**
FR 3.2-11	The Test Tooling provides enhanced support for CCN/CSI testing.	**MAY**
FR 3.2-12	The Test Tooling provides tuning recommendations for the SOA Backplane.	**MAY**
FR 3.2-13	The Test Tooling provides vulnerability testing support.	**MAY**
FR 3.2-14	The Test Tooling provides reliability and availability testing support.	**MAY**
FR 3.2-15	The Test Tooling supports anonymisation of production data used in testing.	**MAY**

Table 35: End-to-End Test Tools requirements

2.4.3.3.FR3.3 Business Activity Monitoring

#	REQUIREMENT	CLASSIFICATION
FR 3.3-1	The BAM Module provides real time event monitoring (or near real-time with low latency).	**MUST**
FR 3.3-2	The BAM Module provides the ability to hook into the CCN2 Platform and listen for events.	**MUST**
FR 3.3-3	The BAM Module provides event Filtering capability that captures events that meet certain criteria.	**MUST**
FR 3.3-4	The BAM Module provides functionality for defining events, thresholds and actions.	**MUST**
FR 3.3-5	The BAM Module provides a continuous flow rule engine (i.e. the capability to apply a processing rule to each event that has been successfully passed through a filtering layer. The rules look for patterns, metric thresholds and anomalies).	**MUST**
FR 3.3-6	The BAM Module provides temporal rules support (i.e. the ability to analyse a stream of time-stamped events which may be correlated).	**MUST**
FR 3.3-7	The BAM Module provides configurable event dashboards	**MUST**
FR 3.3-8	The BAM Module provides the capacity to store and retrieve data from a persistent data store.	**MUST**
FR 3.3-9	The BAM Module provides the capacity to provide historical comparisons against current data.	**MUST**
FR 3.3-10	The BAM Module provides functionality to receive events from systems outside of the CCN2 Platform via a wide range of connectors.	**MUST**
FR 3.3-11	The BAM Module provides functionality to transform or enrich events for user analysis (i.e. change of country code to country names).	**MUST**
FR 3.3-12	The BAM Module provides functionality to detect abnormal situations.	**MUST**
FR 3.3-13	The BAM Module supports event correlation.	**MUST**
FR 3.3-14	The BAM Module supports configurable alerts at predefined thresholds.	**MUST**
FR 3.3-15	The BAM Module supports E-mail/messaging interfaces to propagate alerts.	**MUST**
FR 3.3-16	The BAM Module must provide the capability to provide a filtered read only view to the Partners in relation to their business domains.	**MUST**
FR 3.3-17	The BAM Module provides the capability to define Partner specific, business specific dashboards, thresholds, events and	**MUST**

#	REQUIREMENT	CLASSIFICATION
	alerts etc.	
FR 3.3-18	The BAM Module provides an end-user tool for defining and maintaining dashboards.	**MUST**
FR 3.3-19	The BAM Module supports predefined pattern matching functionality.	**SHOULD**
FR 3.3-20	The BAM Module supports Complex-Event Processing (i.e. Rules can be nested and based on a sequence of events from multiple sources).	**MAY**
FR 3.3-21	The BAM Module provides functionality to provide impact analysis when abnormal situations are detected.	**MAY**

Table 36: Business Activity Monitoring requirements

2.4.3.4.FR3.4 Partner Management

#	REQUIREMENT	CLASSIFICATION
FR 3.4-1	The Partner Management Module provides partner On-boarding.	**MAY**
FR 3.4-2	The Partner Management Module provides partner provisioning.	**MAY**
FR 3.4-3	The Partner Management Module provides partner profile management (multiple profiles per partner should be supported).	**MAY**
FR 3.4-4	The Partner Management Module provides partner Portal for collaboration, support and self provisioning.	**MAY**
FR 3.4-5	The Partner Management Module provides partner score carding and dashboard functionality.	**MAY**

Table 37: Partner Management requirements

2.4.3.5.FR3.5 Directory

#	REQUIREMENT	CLASSIFICATION
FR 3.5-1	The CCN2 Platform provides a Directory Module that will support other CCN2 Platform modules.	**MUST**
FR 3.5-2	The Directory Module provides interfaces to LDAP.	**MUST**

Table 38: Directory requirements

2.4.3.6.FR3.6 Data Replication

2.4.3.6.1. *FR3.6.1 Federated Master Data Management*

#	REQUIREMENT	CLASSIFICATION
FR 3.6.1-1	The MDM Module provides data modelling tools supporting formal data modelling techniques (conceptual, logical and physical schemas).	**MUST**
FR 3.6.1-2	The MDM Module supports processing routines that provide data manipulation for data storage, access and delivery.	**MUST**
FR 3.6.1-3	The MDM Module provides Data Integration Tools. I.e. extraction, transformation and loading (ETL), data federation, virtualisation, messaging and data replication/synchronisation.	**MUST**
FR 3.6.1-4	The MDM Module provides Multi-Directional Support. The functionality provided to transfer data from partner to partner, from partner to central services, and from central services to partner.	**MUST**
FR 3.6.1-5	The MDM Module supports the management of shared master data by enabling multiple domains (for example between the EU and the Member States) to collaborate in a workflow-driven or transaction-oriented process.	**MUST**
FR 3.6.1-6	The MDM Module supports data interoperability by providing functionality to allow multiple systems to communicate, exchange and use data in specified data formats, and communication protocols for collaboration of cross-agency services requiring applications to exchange data in a semantically interoperable manner.	**MUST**
FR 3.6.1-7	The MDM Module provides data replications mechanisms which support full and partial update of the various data sets configurable on a per partner and domain basis. A full update means that the whole data set is synchronised in one logical operation and a partial update means that part of that the whole data set is synchronised in one logical operation.	**MUST**
FR 3.6.1-8	The MDM Module supports data quality tools for identifying and correcting flaws in the data. This includes profiling, cleansing, matching, linking, identifying and semantically reconciling data in different data sources to create and maintain a master record.	**MUST**
FR 3.6.1-9	The MDM Module supports reference data management in terms of a controlled vocabulary that quantifies the valid range of use of master data.	**MUST**

#	REQUIREMENT	CLASSIFICATION
FR 3.6.1-10	The MDM Module supports stateless data replication.	**MUST**
FR 3.6.1-11	The MDM Module supports data versioning and version history.	**MUST**
FR 3.6.1-12	The MDM Module has security, monitoring and auditing functions integrated with the CCN2 Platform.	**MUST**
FR 3.6.1-13	The MDM Module supports taxonomy management.	**MUST**
FR 3.6.1-14	The MDM Module supports data stewardship applications which include the specification of decision rights and an accountability framework to encourage desirable behaviours in the valuation, creation, storage, use, archiving and deletion of master data.	**SHOULD**
FR 3.6.1-15	The MDM Module provides the functionality to resolve multiple labels for classes of data into a single resolved entity, and to analyse relationships among such resolved entities.	**SHOULD**
FR 3.6.1-16	The MDM Module supports MDM across hierarchical organisations and data models (DG TAXUD and Partner).	**SHOULD**
FR 3.6.1-17	The MDM Module supports workflows for the management of data (such as approval of change of data, introduction of new data, and deletion of data), including support of integration with rules engine and external approval systems.	**SHOULD**
FR 3.6.1-18	The MDM Module supports interoperability with other MDM tools (i.e. those potentially operated by the Partners).	**MAY**
FR 3.6.1-19	The MDM Module supports ontology management.	**MAY**

Table 39: Federated Master Data Management requirements

2.4.3.6.2. *FR3.6.2 Managed File Transfer*

#	REQUIREMENT	CLASSIFICATION
FR 3.6.2-1	The MFT Module supports user-initiated file transfers.	**MUST**
FR 3.6.2-2	The MFT Module supports application initiated file transfers via a service interface.	**MUST**
FR 3.6.2-3	The MFT Module supports event initiated file transfers. For example transfers initiated on polling.	**MUST**
FR 3.6.2-4	The MFT Module supports scheduled file transfers.	**MUST**
FR 3.6.2-5	The MFT Module supports sending files from one or more	**MUST**

#	REQUIREMENT	CLASSIFICATION
	sources to one or more destinations with one execution.	
FR 3.6.2-6	The MFT Module supports the ability to cancel file transfers.	**MUST**
FR 3.6.2-7	The MFT Module supports the ability to view, in real time, file transfer progress through all legs in a process and notification of Start, stop and completion.	**MUST**
FR 3.6.2-8	The MFT Module provides the ability to view, in real time, file transfer progress through all legs in a process.	**MUST**
FR 3.6.2-9	The MFT Module supports the ability to view, in real time, file transfer progress through all legs in a process and notification of Inbound data with invalid formatting.	**MUST**
FR 3.6.2-10	The MFT Module provides reports on file access.	**MUST**
FR 3.6.2-11	The MFT Module provides searchable logs which have recorded all significant events logged by the module.	**MUST**
FR 3.6.2-12	The MFT Module provides reliable, one-time-only delivery.	**MUST**
FR 3.6.2-13	The MFT Module provides capabilities to transport files of any size.	**MUST**
FR 3.6.2-14	The MFT Module provides Checkpoint/restart functionality.	**MUST**
FR 3.6.2-15	The MFT Module provides automated file transfer recovery.	**MUST**
FR 3.6.2-16	The MFT Module provides the ability to reinitiate file transfer upon failure of automated file transfer recovery.	**MUST**
FR 3.6.2-17	The MFT Module provides file integrity verification.	**MUST**
FR 3.6.2-18	The MFT Module supports conformation of delivery.	**MUST**
FR 3.6.2-19	The MFT Module can integrate with the orchestration module of CCN2 Platform (i.e. BPEL).	**MUST**
FR 3.6.2-20	The MFT Module is integrated with the IAM module that allows defining groups of users who have access to specific MFT features and files.	**MUST**
FR 3.6.2-21	The MFT Module offers encryption and decryption capabilities for file transmission.	**MUST**
FR 3.6.2-22	The MFT Module provides the functionality to support non repudiation of file transfers.	**MUST**
FR 3.6.2-23	The MFT Module offers functionality that converts from an internal protocol to that required to support connection to endpoints.	**MUST**

#	REQUIREMENT	CLASSIFICATION
FR 3.6.2-24	The MFT Module must integrate with the SOA Backplane so that file transfer events can be published as events to the SOA Backplane (i.e. event delivery network).	**MUST**
FR 3.6.2-25	The MFT Module provides reports on "send and receive" activity.	**SHOULD**
FR 3.6.2-26	The MFT Module provides reports on upload/download traffic and resource usage.	**SHOULD**
FR 3.6.2-27	The MFT Module supports a dashboard that provides status of all file transfers.	**MAY**

Table 40: Managed File Transfer requirements

2.4.3.7.FR3.7 Logging (Monitoring, Metering, Statistics, Auditing)

#	REQUIREMENT	CLASSIFICATION
FR 3.7-1	The Logging Module provides Auditing tools to allow the tracking messages flows and to prove receipt and delivery of messages.	**MUST**
FR 3.7-2	The Logging Module has the ability to log all CCN2 Platform events.	**MUST**
FR 3.7-3	The Logging Module has the ability to track a message from its origin to its destination (within the boundaries of the CCN2 Platform) including all intermediate stages.	**MUST**
FR 3.7-4	The Logging Module provides Metering tools to track service usage and prove use of a service.	**MUST**
FR 3.7-5	The Logging Module provides Management tools to manage all the modules on the CCN2 Platform including MDM, BAM, SOA Backplane and governance.	**MUST**
FR 3.7-6	The Logging Module provides Monitoring tools that deliver functionality to collect and publish statistics on the usage of the resources.	**MUST**
FR 3.7-7	The Logging Module provides service monitoring and control in the form of thresholding, notification, and alerting.	**MUST**
FR 3.7-8	The Logging Module provides service monitoring and control event correlation and fault management.	**MUST**
FR 3.7-9	The Logging Module provides service monitoring and control in the form of consumption and utilisation tracking.	**MUST**
FR 3.7-10	The Logging Module provides Monitoring support for the	**MUST**

#	REQUIREMENT	CLASSIFICATION
	monitoring of services, message traffic, SLOs, service resources and dependencies, and service runtime infrastructure components, and it provides visibility into the environment via dashboards.	
FR 3.7-11	The Logging Module provides Statistics' tools that deliver functionality to collect and publish statistics on services availability.	**MUST**
FR 3.7-12	The Logging Module provides Statistics' tools that deliver functionality to collect and publish statistics on message transit time.	**MUST**
FR 3.7-13	The Logging Module provides Statistics' tools that deliver functionality to collect and publish statistics on QoS (Quality of Service).	**MUST**
FR 3.7-14	The Logging Module provides Statistics' tools that deliver functionality to collect and publish accounting information on message traffic, service usage and data exchange per pattern (synchronous/asynchronous/HTTP/STMP/…) per user/Partner.	**MUST**
FR 3.7-15	The Logging Module provides configurable dashboards.	**MUST**
FR 3.7-16	The Logging Module provides an end-user tool for defining and maintaining dashboards.	**MUST**
FR 3.7-17	The Logging Module has the ability to log all CCN2 Platform events in a centralised manner.	**SHOULD**
FR 3.7-18	The Logging Module provides a centralised management tool for all the modules for the CCN2 Platform.	**SHOULD**
FR 3.7-19	The Logging Module provides Monitoring support for the service level management including compliance tracking and reporting.	**SHOULD**
FR 3.7-20	The Logging Module provides specific dashboards that are accessible from the Partners with a specific configurable set of reports, functions.	**SHOULD**
FR 3.7-21	The Logging Module is capable of synchronisation with other monitoring solutions and systems (such as solutions used by Partners' e.g Tivoli Monitoring or equivalent) using standards protocols (e.g. SNMP).	**SHOULD**

Table 41: Logging requirements

2.5. CCN2 Platform required standards

The following table shows the standards (with the respective considered versions) that the CCN2 Platform supports at it's boundaries (newer versions of the same standards may be proposed):

STANDARD	VERSION	BODY	CLASSIFICATION
.NET	3	Microsoft	**MAY**
AES (FIPS 197)	-	NIST	**MUST**
AMQP	1.0	OASIS	**MAY**
AS1 (RFC 3335)	-	IETF	**MAY**
AS2 (RFC 4130)	-	IETF	**SHOULD**
AS3 (RFC 4823)	-	IETF	**SHOULD**
AS4 (RFC 3335)	Draft	OASIS	**MAY**
BPMN	1.0	OMG	**MUST**
BPMN	2.0	OMG	**SHOULD**
ebXML	-	OASIS	**MAY**
FTP (RFC 959, 3659)	-	IETF	**MUST**
FTP Security Extensions (RFC 2228)	-	IETF	**MUST**
HTTP(S)	1.1	W3C	**MUST**
JBI (JSR 312)	2.0	JCP	**MAY**
JEE	5	Oracle	**MAY**
JMS (JSR 914)	1.1	JCP	**MUST**
LDAP (RFC 4510)	3	IETF	**MUST**
MTOM	2005	W3C	**SHOULD**
OSGi	4.3	OSGi Alliance	**MAY**
SAML	2.0	OASIS	**MUST**
SCA	1.0	OASIS	**MAY**
SDO	2.1	OASIS	**MAY**
SHA-1 (FIPS 180-2)	-	NIST	**MUST**
SMTP (RFC 5321)	-	IETF	**MUST**
SNMP (RFC 3411 – 3418)	3	IETF	**MUST**
SOAP	1.2	W3C	**MUST**
S-RAMP	1.0	OASIS	**MAY**
SSL (RFC 6101)	3.0	IETF	**MUST**

STANDARD	VERSION	BODY	CLASSIFICATION
TLS (RFC 6176)	1.2	IETF	**MUST**
Triple DES (ISO/IEC 18033-3:2005)	-	ISO/IEC	**MUST**
UDDI	3.0.2	OASIS	**MUST**
WS-Addressing	1.0	W3C	**SHOULD**
WS-BPEL	2.0	OASIS	**MUST**
WSDL	1.2	W3C	**MUST**
WSDL	2.0	W3C	**SHOULD**
WSDM	1.1	OASIS	**MAY**
WS-Management specification	1.0	DTMF	**MAY**
WS-Policy Framework	1.5	W3C	**MAY**
WS-Reliable messaging	1.2	OASIS	**SHOULD**
WS-Security	1.1	OASIS	**MUST**
WS-TX	1.2	OASIS	**SHOULD**
X.509	11/2008	ITU-T	**MUST**
XA protocol (ISO 10026-3)	-	Open Group	**MAY**
XACML	3.0	OASIS	**SHOULD**
XMI	2.1.1	OMG	**SHOULD**
XML	1.1	W3C	**MUST**
XML Encryption	1	W3C	**MUST**
XML Signature	2	W3C	**MUST**
XPath	2.0	W3C	**MUST**
XQuery	1.0	W3C	**MUST**
XSD	1.0	W3C	**MUST**
XSLT	2.0	W3C	**MUST**

Table 42: Standards list

2.6.   CCN2 Platform standards definitions[11]

ACRONYM	DESCRIPTION	DETAILS
AES (FIPS 197)	Advanced Encryption Standard	Standard to encrypt electronic data
AMQP	Advanced Message queuing protocol	Proposed protocol standard for general-purpose, high quality of service (QoS), program-to-program messaging.
AS/1	Applicability Statement 1	Electronic Document Interchange standard. Providing secure SMPT exchange
AS/2	Applicability Statement 2	Electronic Document Interchange standard. Providing secure HTTP exchange
AS/3	Applicability Statement 3	Electronic Document Interchange standard. Providing secure FTP exchange.
AS/4	Applicability Statement 4	Complementary specification of ebXML, used for Web Services B2B messaging.
BPMN	Business Process Modelling Notation	BPMN is a standard, graphical, domain-specific modelling language for describing business processes.
ebXML	Electronic Business using eXtensible Markup Language	The ebXML Specification Schema provides for the nominal set of specification elements necessary to specify collaboration between business partners, and to provide configuration parameters for the partners' runtime systems in order to execute that collaboration between a set of e-business software components.
FTP (RFC 959, 3659)	File Transfer Protocol	A IP based protocol for the transfer of files across an IP network.
FTP Security Extensions (RFC 2228)	FTP Security Extensions	RFC 2228 defines extensions to the FTP specification STD 9, RFC 959, "FILE TRANSFER PROTOCOL (FTP)" (October 1985). These extensions provide strong authentication, integrity, and confidentiality on both the control and data channels with the introduction of new optional commands, replies, and file transfer encodings.

---

[11] Some definitions are taken from Wikipedia (www.wikipedia.org)

ACRONYM	DESCRIPTION	DETAILS
HTTP	Hypertext Transfer Protocol	An internet application request-response protocol for use in client server interaction.
HTTPS	Hypertext Transfer Protocol Secure	The HTTP protocol enhanced with a secure transport layer.
JBI	Java Business Integration	A Java standard specification that defines an integration framework that supports plug-in component and connector modules.
JEE	Java Enterprise Edition	An overall programming framework allowing the development of portable applications which are platform independent and will run on any Java Virtual Machine.
JMS (JSR 914)	Java Messaging Services	A Java specification for a message oriented middleware API to exchange messages between applications.
LDAP (RFC 4510)	Lightweight Directory Access Protocol	IP based directory services protocol.
.NET	.NET Framework	The .NET Framework is a software framework that runs primarily on Microsoft Windows.
MTOM	Message Transmission Optimization Mechanism	Describes mechanisms for optimizing the transmission and/or wire format of a SOAP message.
OSGi	Open Services Gateway Initiative	The OSGi Alliance (formerly referenced as Open System Gateway Initiative) was created in 1998 as an industry consortium whose initial goal was to implement a simple way to dynamically deploy and undeploy Java software on constrained, small-footprint, embedded systems. The OSGi Alliance publishes a Java-dynamic component system standard that enables system and application software to be constructed of smaller components that can be dynamically put together in many configurations determined by the conditions found in real-life environments.
SAML	Security Assertion Markup Language	Security Assertion Markup Language (SAML) 2.0 is an open industry standard for federated identity.

ACRONYM	DESCRIPTION	DETAILS
SCA	Service Component Architecture	Service Component Architecture (SCA) is a set of specifications which describe a model for building applications and systems using a Service-Oriented Architecture. SCA extends and complements prior approaches to implementing services, and SCA builds on open standards such as Web services.
SDO	Service Data Objects	Service Data Objects (SDO) are designed to simplify and unify the way in which applications handle data. Using SDO, application programmers can uniformly access and manipulate data from heterogeneous data sources, including relational databases, XML data sources, Web services, and enterprise information systems.
SHA-1 (FIPS 180-2)	Secure Hash Algorithm version 1	Secure algorithm to calculate the checksum of e.g. a message.
SMTP (RFC 5321)	Simple Mail Transfer Protocol	An internet protocol designed for the e-mail message exchange
SNMP (RFC 3411 – 3418)	Simple Network Management Protocol	A protocol for electronic mail transmission across IP networks
SOAP	Simple Object Access Protocol	A WS protocol for the implementation of web services
S-RAMP	SOA Repository Artefact Model & Protocol	The S-RAMP specification defines a standard API and data model for a SOA repository
SSL	Secure Sockets Layer	A cryptographic protocol that provide communication security over the Internet. Version 3.0 is defined by RFC 6101.
TLS	Transport Layer Security	A cryptographic protocol that provide communication security over the Internet. (RFC 5246, RFC 6176).
Triple DES (ISO/IEC 18033-3:2005)	Triple Data Encryption Standard	Encryption standard that applies the DES standard three times.

ACRONYM	DESCRIPTION	DETAILS
UDDI	Universal Description, Discovery and Integration	A platform independent registry standard based on XML to enable heterogeneous information exchange. It provides a mechanism to register and locate web services.
WS-Addressing	Web Services-Addressing	WS-Addressing provides transport-neutral mechanisms to address Web services and messages.
WS-BPEL	Web Services-Business Process Execution Language	WS-BPEL defines a language for specifying business process behaviour based on Web Services.
WSDL	Web Services Description Language	WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate, however, the only bindings described in this document describe how to use WSDL in conjunction with SOAP 1.1, HTTP GET/POST, and MIME.
WS-Management	Web Services-Management	WS-Management defines a SOAP-based protocol for the management of servers, devices, applications and various Web services.
WS-Policy	Web Services-Policy	WS-Policy is a specification that allows web services to use XML to advertise their policies (on security, Quality of Service, etc.) and for web service consumers to specify their policy requirements.
WSDM	Web Services Distributed Management	The WSDM standards specify a common messaging protocol for managed resources and their consumers. It is a vendor, platform, network, and protocol neutral framework for enabling management technologies to access and receive notifications of management-enabled resources. Its is built upon a standardized suite of XML specifications.

ACRONYM	DESCRIPTION	DETAILS
WS-Reliable Messaging	Web Services-Reliable Messaging	WS-ReliableMessaging describes a protocol that allows SOAP messages to be reliably delivered between distributed applications in the presence of software component, system, or network failures.
WS-Security	Web Services-Security	WS-Security is a flexible and feature-rich extension to SOAP to apply security to web services.
WS-TX	Web Services-Transaction	The WS-Transaction specification describes coordination types that are used with the extensible coordination framework described in the WS-Coordination specification.
X.509	ITU-T PKI standard	ITU-T Recommendation X.509 defines a framework for public-key certificates and attribute certificates.
XA	eXtended Architecture	XA stands for "eXtended Architecture" and is an X/Open group standard for executing a "global transaction" that accesses more than one back-end data-store. See ISO 10026-3.
XACML	Extensible Access Control Markup Language	The standard defines a declarative access control policy language implemented in XML and a processing model describing how to evaluate authorization requests according to the rules defined in policies.
XMI	XML Metadata Interchange	A widely used interchange format for sharing objects using XML; applicable to a wide variety of objects: analysis (UML), software (Java, C++), components (Enterprise JavaBeans [EJB], Interface Definition Language [IDL], and Common Object Request Broker Architecture [CORBA] Component Model), and databases (CWM).
XML	Extensible Markup Language	XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is defined in the XML 1.0 Specification produced by the W3C, and several other related specifications, all gratis open standards.
XML Encryption	-	A specification, governed by a W3C recommendation that defines how to encrypt the contents of an XML element.

ACRONYM	**DESCRIPTION**	**DETAILS**
XML Signature	-	XML Signature defines an XML syntax for digital signatures and is defined in the W3C recommendation XML Signature Syntax and Processing.
XPATH	XML PATH Language	A language for referring to specific parts of an XML document and primarily used by XSLT and XLink to access or refer to parts of an XML document.
XQuery	XML Query	A language for retrieving data from XML documents.
XSD	XML Schema	A defined data definition encoded in XML.
XSLT	Extensible Stylesheet Language Transformations	XSL Transformation (XSLT) is used to transform XML documents into other XML documents, spreadsheets, HTML tables, or bulleted lists.

Table 43: Standards definitions

3. Non-Functional Requirements

This chapter describes the non-functional requirements regarding the CCN2 Platform. The non-functional requirements have been subdivided into the following categories:

- Availability (NFR1);

- Performance and Scalability (NFR2).

The non-functional requirements are related to the design principles as described in Design Principles. This section provides the specific requirements the CCN2 Platform must adhere to.

3.1. Availability

All the requirements in this section are classified as **MUST**.

#	REQUIREMENT	EXPLANATION	TARGET VALUE
NFR1.1	Availability (service window)	CCN2 Platform must be designed to operate in continuous fashion.	24H / 7D / 365D
NFR1.2	% Uptime CCN2 Platform communication	Percentage of time that Partners are able to communicate with each other (including planned downtime).	Greater than 99,7% (i.e. a maximum of 26,28 hours downtime per year)
NFR1.3	% Uptime CCN2 Platform	Percentage of time that a Partner can use the complete set of the CCN2 Platform functionality (including planned downtime).	Greater than 99,7% (i.e. a maximum of 26,28 hours downtime per year)
NFR1.4	CCN2 Platform downtime	The maximum downtime of the CCN2 Platform where none of the CCN2 Platform functionality is available, during a single occurrence.	Maximum of 1 hour per occurrence
NFR1.5	Individual CCN2 Platform module downtime	The maximum downtime of a single module during a single occurrence.	Maximum of 2 hours per occurrence
NFR1.6	Main Hub planned downtime	The maximum planned downtime of a Main Hub during a single occurrence.	Maximum of 2 hours per occurrence
NFR1.7	AP planned downtime	The maximum planned downtime of an AP during a single occurrence.	Maximum of 2 hours per occurrence
NFR1.8	Main Hub unplanned downtime	Maximum duration of unplanned downtime of an individual Main Hub during a single occurrence.	Maximum of 2 hours per occurrence

NFR1.9	AP unplanned downtime	Maximum duration of unplanned downtime of an individual AP during a single occurrence (not including hardware replacement).	Maximum of 4 hours per occurrence
NFR1.10	AP switch time	Maximum duration of the reconfiguration of the traffic (to another AP or Main Hub) of a Partner when an AP is failing.	Maximum of 5 minutes

Table 44: Availability non-functional requirements

3.2. Performance and Scalability

3.2.1. *CCN2 Platform*

All the requirements in this section are classified as **MUST**.

#	REQUIREMENT	DESCRIPTION	CCN2 PLATFORM TARGET VALUE
NFR2.1	Average Throughput – Small Messages (5KB)	The CCN2 Platform processing throughput including full cycles of reception and processing, including queue and envelope handling, decryption, verification, rejection handling, translations and filtering, encapsulation, logging, state control and statistics, encryption, forward envelope handling and forward transmission/queue handling.	67K Small messages (5KB) per minute
NFR2.2	Average Throughput – Medium Messages (100KB)		5K Medium messages (100KB) per minute
NFR2.3	Average Throughput – Large Messages (5MB)		30 Long messages (5MB) per minute
NFR2.4	Average Throughput – Extreme Messages (1GB)		0,5 Extreme message (1 GB) per minute
NFR2.5	Peak Throughput	Peak Throughput	10 times the average throughput for a period of 30 minutes.
NFR2.6	Target number of services	The CCN2 Platform must be scalable to extent to a target number of services.	10K services
NFR2.7	CCN Platform Load	Number of messages that the production CCN2 Platform HW & SW should be able to handle (assuming all the existing traffic will be handled by the CCN2 Platform).	15 billion messages per year in 2018
NFR2.8	Scalability	Average growth that CCN2 Platform design should be scalable enough to deal with.	30% year-to-year growth in number of messages and volume (for instance, an estimated 24 billion messages per year in 2020)
NFR2.9	Maximum response time	Response time as seen by a Partner application calling another Partner application and using a synchronous paradigm	300 ms

		for messages of max. 5KB with limited transformations (e.g. character set conversion).	

Table 45: Performance and Scalability non-functional requirements

3.2.2. *Traffic distribution per sites*

The following table is the throughput / volume of the CCN2 Platform (NFR2.7) breakdown per site based on the current CCN/CSI traffic distribution per site (See "Annex II.A - Terms of Reference", section 2.9).

	MSG. COUNT PER MONTH (K)	VOLUME PER MONTH (MB)		MSG. COUNT PER MONTH (K)	VOLUME PER MONTH (MB)
Site 1	13.500	16.500	Site 11	7.000	23.500
Site 2	26.000	25.000	Site 12	26.000	37.000
Site 3	30.500	13.500	Site 13	12.000	26.500
Site 4	30.500	50.000	Site 14	11.000	27.000
Site 5	55.000	81.500	Site 15	43.500	70.500
Site 6	5.500	22.500	Site 16	94.000	123.500
Site 7	29.500	31.500	Site 17	59.500	66.000
Site 8	9.000	7.000	Site 18	1.000	15.500
Site 9	9.000	29.500	Site 19	17.000	41.500
Site 10	18.500	36.500	Site 20	11.000	31.000
Site 21	19.000	37.000	Site 31	1.000	3.500
Site 22	12.000	33.000	Site 32	34.000	45.000
Site 23	21.000	29.500	Site 33	53.500	74.500
Site 24	7.000	24.000	Site 34	109.000	115.000
Site 25	54.500	127.500	Site 35	34.000	23.000
Site 26	39.500	64.500	Site 36	46.000	51.500
Site 27	31.500	44.500	Site 37	20.500	25.000
Site 28	20.000	40.500	Site 38	15.000	111.000
Site 29	20.000	40.000	Site 39	128.500	746.500
Site 30	17.000	40.500			

Table 46: Estimated Site Traffic Requirements in 2018

Note that above table lists only characteristics of 39 sites (contrary to the 46 that are used today). Some sites have been removed because:

- Traffic of the OLAF primary and Secondary Data Centre is merged;

- As the result of the data centre consolidation action (see "Annex II.B - Technical Annex", section 7) the following existing sites will be merged to form the new DG TAXUD Data Centres:

    o the SPEED Bridge and SPEED ECN (2 sites as defined in "Annex II.A - Terms of Reference");

    o the CCN/TC and CBS Data Centre (so, 2 sites as defined in "Annex II.A - Terms of Reference";

    o the ITSM site;

    o the existing DG TAXUD Data centres (2 sites as defined in "Annex II.A - Terms of Reference").

⚠ Taking into account the backup sites of OLAF (Site 38) and DG TAXUD (Site 39), and the disaster recovery of DG TAXUD, the total number of sites for design purposes is 42. Related additional AP must be sized as primary ones.

⚠ Although the total number of the 42 Access Point should be used for the design purpose, it does not means that the CCN2 Platform will have only 42 AP in 2018. Following the CCN2 Platform requirement DP1.17, the number of the AP must not be limited.

The Design and implementation of the Access Points must take into account the need to handle the volumes mentioned in the table above.

The Tenderer is requested to design a maximum of three types of Access Points:

- Access Point - Configuration A

- Access Point - Configuration B

- Access Point - Configuration C

It is a Tenderer design decision to propose three or less AP configurations based on message counts and the volumes presented in the table above. Differentiating the Access Points' configurations is a way to reduce the CCN2 Platform TCO which is one of the key CCN2 Platform evaluation factors.

4. Migration Vision and Approach

The Tenderer must specify the migration from CCN/CSI to CCN2 Platform.

The following are not within the scope of this Tender:

- The support for partners currently using the CSI API to help them redevelop their application in order to phase out of the CSI API currently used

- development of new applications using the full power of the CCN2 Platform .

The goal of CCN2 Platform is not purely to provide a SOA Backplane application for new and existing applications. A key goal of implementing the CCN2 Platform is that it should completely replace the CCN infrastructure (the API for the CCN/CSI stack must be maintained to ensure that applications remain unchanged), after a reasonable migration phase. It is not believed that a "Big Bang" approach to the migration is either feasible or desirable.

The length of this migration phase is a key evaluation criterion of this tender, given that one of the overall goals (and an award criterion), is to minimise the TCO of the combined CCN2 Platform and CCN/CSI. The sooner the CCN infrastructure can be de-commissioned, the quicker the cost of ownership for the EU can be reduced. However this objective cannot come at a higher cost for the combined CCN2 Platform and CCN/CSI. In other words the TCO of the combined CCN2 Platform and CCN/CSI is the overriding goal.

A requirement for the migration from CCN/CSI to CCN2 Platform is that the impact on the Partners' applications (particularly MS) must be minimised. This means that the Partners must not:

- Be required to redevelop any of their existing applications;

- Be required to re-test entirely any of the existing applications (the impact and scope of such tests must be reduced).

This means that the Tenderer will be required to ensure that:

- The Partners' applications which currently use the CSI API to communicate, will be able to use the CCN2 Platform without modification during and after the migration period using CCN2 Platform CSI API interface;

- The CCN2 Platform can interoperate with the CCN/CSI during the migration period.

For CCN/CSI volumetrics please refer to the relevant Annex of this **CCN2-DEV** Call for Tender ("Annex II.A - Terms of Reference", section 2.8).

The Tenderer is requested to outline their proposed migration vision and approach with particular reference to the items outlined in the table below:

#	REQUIREMENT	CLASSIFICATION
MV1	During the migration (from the CCN/CSI to the CCN2 Platform), the CCN2 Platform provides full integration with Partners' applications which are connected via the current CCN/CSI so that they can interoperate with Partners' applications which are connected to the CCN2 Platform and vice versa.	**MUST**
MV2	During the migration (from the CCN/CSI to the CCN2 Platform), the CCN2 Platform IAM module should be integrated with the existing CCN/CSI IAM module so that a user / system authenticated in CCN does not need to re – authenticate when accessing a CCN2 Platform resource and vice versa.	**MUST**
MV3	During the migration (from the CCN/CSI to the CCN2 Platform), any maintenance on users and profiles in the legacy CCN IAM module will be propagated to the CCN2 Platform IAM module and vice versa.	**MUST**
MV4	During the migration (from the CCN/CSI to the CCN2 Platform), the existing HTTP/HTTP(S) exchange functionality currently used in CCN/CSI will be integrated with the CCN2 Platform to ensure seamless HTTP/HTTP(S) interoperability across the Platforms.	**MUST**
MV5	During the migration (from the CCN/CSI to the CCN2 Platform), the CCN2 Platform must provide reporting and statistics as a consolidated view across both the CCN2 Platform and CCN/CSI.	**MUST**
MV6	The risk of degraded performance or outright failure during the migration is minimised using appropriate risk analysis and mitigation strategies.	**MUST**
MV7	Contingency Plans in the event of any case failure for the proposed approach are in place.	**MUST**
MV8	There is an approach to management and monitoring of CCN2 Platform and CCN/CSI during the migration phase.	**MUST**
MV9	There is a Business Continuity Plan during the migration phase.	**MUST**
MV10	There is a defined support organisation during the migration phase.	**MUST**

Table 47: Migration requirements

End of ANNEX II.C