A Report for

TAXUD

CCN Evolution Strategy

May 2010

Engagement: 222758730

Gartner

This report was prepared for TAXUD by:

Authors	Guido van der Harst, Sven Hazejager
Contractor	Gartner Inc.

Framework contract DI/5370-00

Specific contract No. 128

DISCLAIMER

Executive Summary

The Common Communications Network / Common Systems Interface (CCN/CSI) is a value-added network operated by TAXUD. The mission of CCN today and in the future is to provide common services to exchange tax and customs information at reasonable cost, high agility, high security and continuity. CCN was designed between 1993 and 1995 and is operational since 1999. Today, CCN encompasses 40 sites in 29 countries. 119 CCN gateways and mail servers are deployed at the CCN sites. The global availability is around 99.91%.

CCN Participants are enjoying a range of highly effective applications that are enabled by the network. As these applications have been very valuable for the Participants, CCN has become a vital piece of infrastructure. However, from a technological point of view, the CCN solution is proprietary and complex, leading to a long time-to-market for new applications, high development and high maintenance cost. Improvements and innovation are needed to remain at the forefront of effective and efficient operations.

Gartner identified three technology trends that could enable the evolution of CCN. The first is *commoditization*. The added value of an IT organization is no longer in hard-core technology, but in combining commoditized components in a smart way, focusing on added value for the stakeholders. The second, long standing trend is "Moore's Law". *Bandwidth and computing power* continue to grow exponentially enabling new paradigms. The third and final trend is *service orientation* which enables the development of more loosely coupled information systems.

Combining the CCN mission and technology trends leads to the following tentative vision statement for CCN 2.0:

> *Transform CCN from a closed, proprietary platform into a proven, commoditized platform by using agile, open, reusable and standardized components.*

Gartner identified three categories of options to evolve towards CCN 2.0. First, *improvements* focus on improving existing CCN functionalities. Second, *additional services* add new functionalities to CCN. Third, *transformation options* provide transformational change to CCN.

Key additional services are *business activity monitoring* providing real time information about the status and results of various operations, processes, and transactions; and *master data management* enabling the synchronization of non-transactional data between CCN Participants. The transformation options require a commercial, off-the-shelf *Enterprise Service Bus (ESB)* infrastructure to replace today's proprietary solution and a standardized so-called *CCN appliance* to host the ESB and possible other shared components.

Gartner assessed all options along two dimensions: TAXUD effort and overall value. The assessment of the options led Gartner to the conclusion that the road towards CCN 2.0 will be a tough road. The transformation options that deliver high value require a high effort. Furthermore, they require an initial investment in other options that provide less value at first. Gartner identified a list of work packages that could take six years of execution before TAXUD can start implementing the transformation options that actually add significant value to the CCN Participants.

Table of Contents

Executive Summary ..... **ii**
1.0 Introduction **6**
1.1 Background 6
1.2 Objective of this study 6
1.3 Audience 6
1.4 Structure of this Report 7
2.0 Current State, CCN 1.0 ..... **8**
2.1 CCN Today 8
2.2 Business and Organizational Trends 9
2.3 High Level Requirements 10
3.0 Future State, introducing CCN 2.0 ..... **11**
3.1 Technology Trends 11
3.2 CCN 2.0 Vision Statement 13
3.3 Overview of Evolution Options 14
3.4 Assessment Methodology 15
3.5 Outline of the next chapters 16
4.0 Improvements **17**
4.1 Improve Data Center Management (I1) 17
4.2 Leverage Internet for Connectivity and Fail-Over (I2) 20
4.3 Improve Common Testing Environment (I3) 23
4.4 Open Specifications (I4) 27
4.5 Conclusions 29
5.0 Additional Services **30**
5.1 Common Infrastructure services (S1) 30
5.2 Business Activity Monitoring (S2) 32
5.3 Master Data Management (S3) 35
5.4 Federated Identity (S4) 38
5.5 Central Internet Gateway (S5) 41
5.6 Conclusions 44
6.0 Transformation Options **45**
6.1 Overview of Options 45
6.2 Commercial, off-the-shelf ESB (T1) 46
6.3 Common Components (T2) 50
6.4 Data Container Paradigm (T3) 53
6.5 Unified Storage (T4) 57
6.6 Conclusions 60
7.0 Roadmap and Sourcing **61**
7.1 Roadmap and Work Packages 61

7.2 Good IT Stewardship 62
7.3 Vendor Management 63
7.4 New CCN 2.0 Framework Contract 65
8.0 Conclusions and Recommendations 66
A.0 References 70
A.1 Workshops 70
A.2 Interviews 70
B.0 MS Questionnaire 71
C.0 Plan for Iteration 2 73
C.1 Objective 73
C.2 Tasks 73
C.3 Planning 74

Report

1.0 Introduction

1.1 Background

The Common Communications Network / Common Systems Interface (CCN/CSI) is a value-added network operated by TAXUD to support the fulfillment of its mission. The CCN was designed between 1993 and 1995 and is operational since 1999. It transported 820+ million messages in 2009 between the member states of the European Union. Today, CCN improvements and innovation are needed to remain at the forefront of effective and efficient operations.

1.2 Objective of this study

Gartner has been requested to support TAXUD to facilitate the definition of an evolution with regards to the CCN network, which will be shaped through several iterations. The goal of the first iteration is to deliver a consolidated architecture outline for improvement and innovation including the outline of the migration program. During the second iteration the results of Iteration One are tested and qualified in a broader audience outside of TAXUD, i.e. Member States and other DGs involved in CCN.

The scope of this study concerns Iteration One. The full objectives of this study are to:

- *Assess the current architecture* – of the CCN/CSI infrastructure by confronting the current situation with the business users within TAXUD and INFSO and DIGIT;
- *Draft ideas on the evolution* – of the architecture using scenario's on how the future should look like in terms of Policy, legislation, taxes/customs, IT, technology trend;
- *Provide tactical recommendations* – for short term improvement of the CCN infrastructure (CCN1);
- *Draft strategic recommendations* – for long term improvement and development of the CCN infrastructure (CCN 2.0);
- *Outline the migration strategy* – and architecture for improvement and innovation towards CCN 2.0;
- *Outline the migration program* – to define the projects that lead to CCN1 and onwards to CCN 2.0;
- *Outline the second iteration activities* – to further refine the architecture and program in the next phase.

In the description above, 'outline' is meant as a summary showing the chief facts (inclusions and limitations). Not a detailed description – but still a statement to take decisions on.

1.3 Audience

This report is written for the audience participating in the second iteration. Furthermore, this report is written for the sponsor Mr. Theodoros Vassiliadis, Head of Unit Automated Customs and Taxation Services of TAXUD, and the management team of TAXUD.

1.4 Structure of this Report

Chapter 2 assesses the current architecture. The future outlook regarding policies, legislation, taxes/customs are also taken into account. The chapter concludes with a list of high-level requirements for CCN 2.0. Chapter 3 looks into IT trends and technology and, based on the high-level requirements, provides a tentative vision statement for CCN 2.0, sketches the contours of CCN 2.0 and introduces the assessment approach.

Chapter 4 focuses on the short term improvements for CCN. Additional services are discussed in chapter 5. Chapter 6 elaborates on the transformation options towards CCN 2.0.

Chapter 7 discusses the tentative roadmap how to evolve towards CCN 2.0 and what sourcing strategy is needed to get there. Finally, chapter 8 provides a summary of the main conclusions and recommendations of this report.

This report holds the following appendices. Appendix A lists the references, appendix B provides the questionnaire for the Member States, appendix C provides the plan for the second iteration.

2.0 Current State, CCN 1.0

This chapter assesses the current architecture. The future outlook regarding policies, legislation, taxes/customs and IT are also taken into account. This chapter concludes with a list of high-level requirements for CCN 2.0.

2.1 CCN Today

The CCN network has proven to be reliable and has come a long way since it was first implemented. Today, CCN encompasses 41 sites in 29 countries. 119 CCN gateways and mail servers are deployed at the CCN sites. The global availability is around 99.91%.

CCN Participants are enjoying a range of highly effective applications that are enabled by the network. CCN is used for the implementation of all trans-European IT systems and applications enabling the customs union or fiscal policies. Today, over 50 such systems or applications exist. Examples include:

- The Excise Movement Control System (EMCS);
- The New Computerized Transit System (NCTS);
- Information about the Integrated Community Tariffs (TARIC);
- European Binding Tariff Information (BTI / RTCE);
- The VAT Information Exchange System (VIES).

As these applications have been very valuable for the Participants, CCN has become a vital piece of infrastructure. However, from a technological point of view, the CCN solution is complex, and improvements and innovation are needed to remain at the forefront of effective and efficient operations.

Due to its complexity, CCN Participants experience low flexibility, long lead times for implementations (low agility) and high annual maintenance costs. Gartner has identified four root causes for today's issues:

- *Complex proprietary specifications* – The specifications that are created for the message exchanges are complex, as a result of a low-level message-oriented paradigm;
- *30+ different implementations* – Each CCN Participant implements the specifications independently, in their own way, using their own technology. Ambiguities in the specifications lead to problems;
- *Complex proprietary interface* – The CSI application programming interface, that TAXUD maintains so that the CCN Participant applications can interface with the CCN network, is fully custom built and complex. In addition, many different platforms are supported, leading to a duplication of effort;
- *Outdated custom made middleware solution* – The CCN message-oriented middleware was developed almost two decades ago. Most code is custom, complex and hard to maintain. Middleware on the market today is much more advanced.

These issues are not surprising. In the early 1990s, when CCN was designed, Wide Area Network (WAN) bandwidth was extremely limited, and the Internet was still in its infancy. Companies started to exchange standardized messages (Electronic Data Interchange – EDI) over proprietary networks (such as X.25). The design of CCN clearly reflects the state of affairs of that era.

Since then, information technology has made enormous strides forward. Bandwidth, and with it the Internet, have become omnipresent, highly reliable, flexible, and cheap. The lower

layers of the IT stack have commoditized rapidly as vendors have come up with Commercial Off The Shelf (COTS) solutions that provide much more functionality to integrate applications than what used to be possible. This in turn has enabled IT organizations to move up the value chain: core technology is now taken care of by products and solutions, so the focus could shift to innovative, value-added business functionality and services.

Consequently, CCN has been overtaken by technology and the market. Its head start in the 1990s has become a handicap, slowing down innovation and increasing complexity.

The question now at hand is: How can CCN evolve, offering innovative, value added services to the CCN Participants, while continuing to provide today's functions, and improving in the areas of cost effectiveness and agility? This report proposes a number of improvements and architectural changes that address this question by leveraging proven technology that is available today.

2.2 Business and Organizational Trends

Several trends in the context of TAXUD play a key role in the definition of requirements for CCN 2.0.

At the process level, further **harmonization** is a major goal. More collaboration between CCN Participants regarding the harmonization of operations is required and expected in the future. The systems that track the movement of goods across the European Union are seen as relatively complex systems and therefore need a complex coverage of application protocols. A reference database for transit movement in Europe is considered, which would require large bandwidth and high availability of systems. Furthermore, the majority of systems running on CCN/CSI are mission critical systems, meaning that the systems are a vital component to adhere to the legislation with a maximum permissible downtime of two hours.

The **volumes** in the current network **increase** around 30-40 percent per year. Forecasts regarding the volume increase for the next 10 years and beyond are difficult to compile. Volume increases depend on future legislative requirements and their effects on application- and network traffic. Additionally, volumes should be predicted depending on economic forecasts, which are difficult to obtain currently.

In terms of increase in volumes, Taxation expects stable demands in the medium-term future. Although there are large proposals for legislation in preparation, e.g. for European central information exchanges for direct taxes such as immovable properties or salaries of employees, their implementation cannot be foreseen. These initiatives would require that in the long-term other authorities, e.g. cadastre office, need to be included with access to CCN, which would increase volumes even more.

In the future, expansion of the scope of CCN **beyond the European Union** is also a possibility. There exist contacts and collaboration to other countries of free trade zones such as NAFTA, as well as the world customs organization WCO, and other non-EU CCN Participants like e.g. Russia. The taxation and customs authorities also have cooperation with private organizations, e.g. Taxation has cooperation with the organization SWIFT for the banking industry. CCN 2.0 should contain access possibilities for those private organizations.

And finally, the future vision of a **single window** as a single access point for traders should be supported by CCN 2.0. The preparations for the implementation of Single Window are seen as a program further into the future. However, at present, no concrete requirements can be discerned from this vision.

2.3 High Level Requirements

From the current situation and future developments the following high-level requirements for CCN 2.0 are derived.

- **Do more with less**
  - Shorten time-to-market
  - Reduce costs (95% maintenance – 5% development)
- **Continuity** – ensure that current operations continue to be up-and-running
  - Continued support for CCN/CSI interface
  - Today's and tomorrow's applications are mission critical
  - Proven technology
- **Scalability** – ensure that the volumes can grow
  - Volume will increase (40% YOY volume growth so far)
  - Salaries, properties, employment, royalties, dividend, invoices
- **Agility** – ensure that choices facilitate innovation and avoid lock-in
  - Lesson from the past: future is difficult to predict
  - Open standards at the perimeter of CCN 2.0
- **Security** – ensure availability, data integrity and confidentiality
  - Refined access layers, also access for smaller local community offices

3.0 Future State, introducing CCN 2.0

3.1 Technology Trends

As mentioned earlier, since CCN was designed in the early 1990s, information and communication technology has shown enormous improvements in terms of performance and reliability, at tremendously lower costs. Gartner identified three key technology trends that will enable the evolution towards CCN 2.0:

- Commoditization;
- Increases in bandwidth and computing power;
- The Service-Oriented Architecture (SOA) paradigm and Enterprise Service Bus (ESB) products.

Commoditization

The interest in commoditized, utilitarian technology is a direct consequence of the phase of extreme customization that occurred between 1993 and 2000. Ideas such as Software-as-a-Service (SaaS) have become popular because more and more customers were disillusioned with the results of ambitious, expensive, highly customized IT projects and, thus, were open to solutions with more-modest goals and costs but more-achievable results. The recent period of standardization has seen greater attention to the idea of taking the prebuilt "Lego" blocks that are available over the Internet, rather than building them "from scratch." The next wave of customization and innovation will be characterized by the use of building blocks that are available off-the-shelf. These customizations will oftentimes be, in effect, "configurations" – the need to start from scratch and to reinvent the wheel will be less necessary.

With the availability of so many "Lego" blocks from the "cloud," developers won't need to be "hard-core techies," but simply, people who can use technology in the way that we now commonly use PowerPoint; that is, we don't need to know how the program is written. This way, the added value of IT organizations is higher up in the IT stack – no longer focusing on the hard-core technology, but instead on combining commodity components in a smart way, focusing on added value to the business and other stakeholders.

Of course, specific functionality often does not come in the form of "Lego" blocks and partial customization will always be necessary. The commodization allows IT organizations to focus their efforts on the truly differentiating parts.

Increases in bandwidth and computing power

Moore's Law states that the number of transistors that can be placed inexpensively on an integrated circuit has doubled approximately every two years, and these growth figures roughly apply to bandwidth as well. When CCN was designed, the Internet was still in its infancy, and WAN bandwidth was scarce and expensive. Proprietary networks came into existence, driven by message exchange demands from businesses (EDI). Back then, network speeds of 2400 bits/sec were common. The standard for personal computing power was set by the introduction of the Intel Pentium in 1993, with its 3.1M transistors running at 66MHz. And according to the Minnesota Internet Traffic Studies (see footnote 1), the Internet traffic in the US in 1993 was approximately 0.008 PB/month.

[1] http://www.dtc.umn.edu/mints/igrowth.html

Today, multi-Mbit WAN links are common, with Internet backbone links operating at multi-Gbit/sec speeds. The Intel Core i7 CPU boasts 731M transistors running at 3.33GHz, at a lower price than the original Pentium. And the Internet traffic in the US in 2008 was estimated to be 1,200 to 1,800 PB/month.

These developments have a tremendous impact on network infrastructures such as CCN. With bandwidth and computing power no longer being constraints, new features and services can be offered at the highest levels of performance and reliability, at a fraction of the original cost.

The Service-Oriented Architecture (SOA) paradigm and Enterprise Service Bus (ESB) products

Related to the aforementioned commoditization and the ideas of combining building blocks are the development of the SOA paradigm and the maturing market for ESB products. A SOA is a flexible set of design principles used during the phases of systems development and integration. A deployed SOA-based architecture will provide a loosely-integrated suite of services that can be used within multiple business domains. SOA defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms. Rather than defining an API, SOA defines the interface in terms of protocols and functionality. An endpoint is the entry point for such an SOA implementation. SOA promotes reuse at the macro (service) level rather than micro (messages) level by defining meaningful (in terms of business) services. SOA aims to achieve the goals of increased interoperability (information exchange, reusability, and composability), increased federation (uniting resources and applications while maintaining their individual autonomy and self-governance), and increased business and technology domain alignment, all of which are relevant in the context of TAXUD. Modern application platforms such as Java J2EE and Microsoft .NET support SOA standards such as web services and XML messaging off-the-shelf, enabling cross-platform interoperability and letting the developers focus on the functionality of the services instead of their technical implementation.

An ESB is an important enabler for an SOA. An ESB brings flow-related concepts such as transformation and routing to an SOA. An ESB can also provide an abstraction for endpoints. This promotes flexibility in the transport layer and enables loose coupling and easy connection between services.

Many of CCNs custom-designed and custom-developed features (routing, reliable messaging, encryption) are provided by today's ESB products off-the-shelf, requiring only configuration. And because these products support the SOA-based standards that modern application platforms support as well, technical interoperability is no longer a concern.

By leveraging these technology trends, that are available today, TAXUD will be able to provide a CCN 2.0 to the CCN Participants that is:

- Standardized;
- Componentized;
- Reusable;
- Open;
- Agile.

From a CCN Participant perspective, these characteristics translate into a number of direct, tangible benefits:

- Less application development effort;
- Lower lead times for development;

- Lower maintenance costs due to less complex applications;
- Higher quality of applications and operations.

3.2 CCN 2.0 Vision Statement

Before we formulate a vision statement for CCN 2.0 we first state a *mission statement* for CCN 2.0 derived from the high-level requirements (section 2.3):

Provide ***common services***

to ***exchange*** *tax and customs information*

at ***reasonable cost***, ***high agility***, ***high security*** *and* ***continuity***

To formulate a *vision statement* for CCN 2.0 we would like to make an analogy with cars. One could compare today's CCN with a 1981 DeLorean DMC-12. In those days the DeLorean with stainless steel frames, fiberglass underbody and gull-wing doors was an innovative concept. However, production of the car, with its many exotic and custom-made parts, proved to be extremely challenging and expensive, and to keep a DeLorean running smoothly today at high performance requires specific expertise and becomes quite costly.

Figure 1 1981 DeLorean DMC-12 with stainless steel frames, fiberglass underbody and gull-wing doors

Today, many brands of cars from a manufacturer are extremely similar "under the skin." Yet the diversity of autos in developed Western countries has never been greater. Manufacturers produce autos for smaller segments of the population based on a more granular understanding of each segment's preferences and requirements. To "build from scratch" for each of these segments would be prohibitively expensive and unprofitable. By taking

previously developed manufacturing "platforms" and parts, new configurations can be created that are economically viable.

Figure 2 The 2006 Cadillac BLS, 2002 Opel Vectra and 2003 Saab 9-3 are all based on the General Motors Epsilon I platform and share most parts

The General Motors Epsilon I platform forms the basis for the 2006 Cadillac BLS, 2002 Opel Vectra and 2003 Saab 9-3, each of which is a unique car, but only partially customized. This common car platform has enabled GM to reach high levels of commoditized part sharing and to use efficient, very similar production lines, while still being flexible enough to market a number of different cars and brands.

These three cars provide better performance, higher reliability, less fuel consumption and lower operating costs, at a lower purchase price, than the 1981 DeLorean DMC-12.

In our vision, CCN should transform to such a proven, reliable yet heavily commoditized car, applying efficient manufacturing techniques and reusing common parts as much as possible.

To sum it all up, the vision statement for CCN 2.0 is:

> *Transform CCN from a closed, proprietary platform into a proven, commoditized platform by using agile, open, reusable and standardized components.*

3.3 Overview of Evolution Options

To move from a "DeLorean" towards a "General Motors Epsilon" the study revealed the following categories of options:

- *Improvements* – These improve the current functionality of CCN (enhance the DeLorean);

- *Additional Services* – These add new functionalities to CCN (introduce elements of the Epsilon);
- *Transformation* – These options provide transformational change to CCN (transform towards the Epsilon).

Chapter 4 discusses the identified improvements, chapter 5 elaborates on the additional services, finally chapter 6 explains the transformation options.

3.4 Assessment Methodology

Each option is assessed along two dimensions:

- *TAXUD Effort* – the amount of effort that is required from TAXUD to implement the option;
- *Overall value* – the amount of value for all participants that the implementation of the option generates.

For the TAXUD Effort we look into the duration and the cost of the implementation as indicated in Table 1.

Effort	Duration	Cost
Low	< 9 months	< 1 M€
Medium	9 - 18 months	1 - 5 M€
High	> 18 months	> 5 M€

Table 1 Definition of TAXUD effort

For the overall value we look at three aspects. These aspects are related to the high-level requirements that make a difference: do more with less and higher agility.

- The reduction of the yearly maintenance and operations cost for all CCN Participants and TAXUD. Today's yearly maintenance and operations cost of infrastructure and systems in the EU is estimated at 450 M€ (see footnote 2);
- The reduction of the yearly development cost for all CCN Participants and TAXUD. Today's yearly development cost is estimated at 50 M€ (see footnote 2);
- The increase of the speed-to-market, in other words: the lead time of new functionality from inception to production. Today's speed-to-market is four years.

Value	Total maintenance cost		Total development cost		Speed-to-market	
Low	< 5%	< 22.5 M€	< 10%	< 5 M€	< 25%	< 1 year
Medium	5 - 15%	22.5 - 67.5	10 - 30%	5 - 15 M€	25- 50 %	1 - 2
High	> 15%	> 67.5 M€	> 30%	> 15 M€	> 50%	> 2 years
Weight	1		2		2	
Today	450M€		50M€		4 years	

Table 2 Definition of overall value

To determine the overall value we have given the three aspects a weight. First, each aspect is given a numerical score (0, 1 or 2) based on the relative improvement in that category. For instance, a 20% estimated improvement for maintenance cost counts as 2, and a

2) These estimates require validation. They are based on the information that security amendment implementation in the EU in the year 2009 had a cost over 80 M€

speed-to-market improvement of less than 25% counts as 0. The three scores thus derived are used to calculate the weighted score for overall value as follows:

ValueScore = (1 x *Maint.Score* + 2 x *Dev.Score* + 2 x *Speed.Score*) / 5

As the score for the overall value is between 0 and 1, the low, medium and high categories are assigned as follows:

ValueScore	Category
$n \leq 0.33$	Low
$0.33 < n < 0.67$	Medium
$n \geq 0.67$	High

Table 3 Assignment of overall value categories based on calculated score

3.5 Outline of the next chapters

Chapters 4, 5 and 6 explain the improvements, additional services and transformational options in detail. Each option is discussed along the following outline:

- *Description* – Brief explanation of the option;
- *Technology* – Technologies involved to implement the option. Sometimes a logical architecture is presented to clarify the option;
- *Adherence to Requirements* – This section explains how the option contributes to the key high-level criteria of continuity, scalability and security. The other criteria are discussed in the value section;
- *Development/Sourcing* – What is the most appropriate approach for TAXUD to realize the option? How can TAXUD acquire the option?
- *Deployment/Maintenance* – How should the option be deployed in practice? How should TAXUD organize maintenance and operations?
- *Dependencies* – Are there any dependencies from other options?
- *Risks* – What are the risks of implementing the option?
- *Effort* – What is the effort from a TAXUD perspective (as explained in section 3.4)?
- *Value* – What is the overall value from a CCN Participant perspective? How does the option adhere to the key requirements do more with less and agility?

4.0 Improvements

4.1 Improve Data Center Management (I1)

Description

At present, the CCN/CSI components are distributed over 41 data centers. Their configuration is diverse, with many interdependencies that require significant human attention and effort during the implementation of changes. As a result, these implementations are costly and have a long lead time. Additionally, ongoing operations and maintenance costs are perceived as relatively high.

Although the root cause is the accumulation of complexity within the CCN and CSI components over the years, tactical measures that address specific operational procedures can have a positive effect on the short term.

These measures comprise formalizing operations and deployment processes and procedures, for instance through implementing specific parts of the IT Infrastructure Library (ITIL), supported by the implementation of technology components such as server provisioning and configuration management tools, smart infrastructure monitoring, and virtualization technology.

At time of writing this report, efforts to implement parts of IBM Tivoli infrastructure management software were underway.

Technology

A possible first measure for improvement is the formalizing of operations and deployment processes by implementing parts of the **IT Infrastructure Library (ITIL).** ITIL is a standard process framework for integrated IT service support and delivery processes that are used to manage an IT operations environment.

ITIL v.2 is a well-established framework that has been around for 20 years. Its adoption continues steadily worldwide and across most industries. For most enterprises, during the past three to four years, ITIL has moved rapidly from awareness of the framework, to discussion, then to adoption of some key service support and delivery processes. Thus, most organizations have realized that ITIL implementation is a cultural-change exercise, so they are trying to overcome this big hurdle.

Although it is mature as a framework, ITIL v.2's popularity as a panacea is waning because the profound change it requires has become abundantly clear to many enterprises. However, the benefits of improved IT services at lower costs require most enterprises to adopt this best-practice framework. ITIL v.2, with its narrower scope on service management, remains one of the most commonly used aspects of ITIL, despite v.3 having existed for two years.

More mature operational processes also benefit more from supporting technology, such as server provisioning and configuration management tools, smart infrastructure monitoring, and virtualization technology.

Server provisioning and configuration management is a quickly maturing set of tools focused on managing the configuration life cycle of physical server environments, with less-mature functionality around managing the virtual servers.

Application provisioning and configuration management (including patch management) is a broad suite of multiplatform functionality to discover and provision (that is, package, deploy and install) OSs and application software; these tools also can make ongoing updates to

OSs or applications (for example, patches, new versions and new functionality), or they can update configuration settings.

Inventory/discovery, configuration modeling, audit and compliance enable the discovery of software, hardware and virtual servers; some can discover dependency relationships across servers and applications. Using modeling of application and OS configuration settings (that is, the desired state, or "gold" standard), these tools can report and may be able to remediate variations by modifying the actual state back to whatever the model requires, or the desired state for applications, as well as security configuration settings.

Smart infrastructure monitoring by using **Event Correlation and Analysis (ECA)** tools helps IT operations personnel contend with the deluge of events that comes in from the IT infrastructure by eliminating duplicate event signals, filtering events according to operational or business priorities and analyzing events to determine root cause. The goals are to improve the mean time to isolate and repair problems, and to prioritize IT support efforts according to business process value. The core value proposition of these products is to achieve management by exception. This requires an understanding of "normal" behavior in the IT infrastructure and alerting the IT operations staff only when an exception occurs, such as an outage, a failure or a threshold breach, indicating that the IT infrastructure is no longer behaving "normally."

IT organizations invest in ECA tools to improve the productivity of the IT operations staff and to reduce the time it takes to troubleshoot problems by consolidating events from various devices, applications and other management tools. Without proper event management, the IT operations group can be deluged with event storms, numerous false positives and a "sea of red" on their consoles.

System virtualization technology introduces an abstraction layer between the physical hardware and the operating system. Key advantage is that multiple OS environments can co-exist on the same server, in strong isolation from each other. Additionally, the virtualization software provides functionality for system provisioning.

Enterprises can achieve a 20% to 50% cost savings, while enjoying increased flexibility and speed, and improved quality of service. For example, server virtualization yields a rewarding return on investment (ROI) in servers, power and cooling, data center space, and administration, while enabling administrators to develop business-driven policies for optimizing resources.

Adherence to Requirements

Table 4 shows how improving data center management adheres to the key high-level requirements.

Development/Sourcing

Acquisition of these improvements falls within existing contracts. Process improvement measures are fully in scope of the present outsourced CCN/CSI environment and are as such a responsibility of the existing supplier.

New process-oriented agreements with the supplier will have to be made, such as input/output criteria, lead times, allowable failure rates and reporting procedures. Existing SLAs are probably not sufficient. The usage of virtualization, provisioning and configuration management tooling, and smart infrastructure monitoring tools and should also be specifically agreed.

In case of a (re-)tender in the future, these improvements should be an integral part of the specifications and agreements with the new supplier.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	No impact
	Today's and tomorrow's applications are mission critical	Better data center management leads to fewer process interruptions
	Proven technology	ITIL and the recommended technologies are proven
Scalability	Volume will increase (40% YOY volume growth so far)	Virtualization increases infrastructure efficiency and allows for more flexible capacity management
Security	Refined access layers, also access for smaller local community offices	No impact

Table 4 Data center improvement adherence to high-level requirements

Deployment/Maintenance

The implementation of process improvements impacts the way the TAXUD service management organization interacts with the supplier. Any processes that cover both parties should be fully in scope of the improvement program, and hand-over points must all be clearly defined.

The implementation of supporting tools and technology, as well as their maintenance, is a responsibility of the provider, and should be transparent to the outside world.

Dependencies

There are no dependencies with other improvements.

Risks

The risks associated with implementing these improvements are low. The implementation of process improvement and smart infrastructure monitoring should be fully transparent to the CCN Participants.

The introduction of event correlation and analysis tools, as well as migrating all existing systems into a virtualized environment, impacts the existing infrastructure and running services. Careful planning, test runs and rollback procedures need to be in place to ensure minimal disruptions in the service.

Effort

We assess the implementation effort of I1 as **medium**: approximately 9 – 18 months duration, and a 1 – 5 M € investment is required. Implementation involves process improvement, and procurement and implementation of specific technology that introduces a learning curve before the benefits can be fully realized.

Value

For the CCN Participants I1 will encompass an even higher availability of the CCN gateway and backbone. We assess the value of I1 to the CCN Participants as follows:

- As a result of expected improvements in service quality, agility and costs, the estimated impact on annual maintenance cost is <5%;
- There is no measurable impact on development costs for CCN Participants;
- There is some impact on speed-to-market of new implementations: <25%.

The inherent complexity of the CCN/CSI is not addressed which limits the benefits. The overall value of these improvements is therefore **low**.

4.2 Leverage Internet for Connectivity and Fail-Over (I2)

Description

At present, all CCN traffic is routed over the private network, managed by Orange Business Services. This network is operated against very high service levels to cater for mission-critical communications, that requires the highest standards in security, reliability, and performance. This quality comes at a high price.

Not all traffic over the network requires this high quality. Asynchronous messaging is not time-sensitive and delivery in several seconds, as opposed to milliseconds, would be sufficient. This also applies to bulk data transfers over the network, such as backups or deployment packages of new software, that often run at night or in the background, and human-oriented communications such as e-mail, VOIP and Intranet web applications.

By allowing this non-essential traffic to flow over the Internet, the core network could be downsized to accommodate only mission-critical traffic. In addition, some smaller, non-critical sites could be migrated fully onto the Internet-based WAN.

Although not guaranteed, the robustness of such a virtual, secondary network would in practice be very high due to the resilient nature of the Internet itself. Security would need to be addressed and tightly managed. If properly setup, the secondary network would be equally as secure as the core network. The secondary network could even be used as a fail-over option for the core network, allowing service levels on the core network to be reduced.

Routing of traffic over the primary and secondary parts of the network would be handled by the CCN equipment itself and be transparent to the applications.

Cost savings can mainly be realized through significantly lower bandwidth requirements on the core network and potentially lower service levels on the core network if fail-over is in place. In some real-world cases (see footnote 3), Gartner has seen this design reduce WAN costs by as much as 50%. For example, in the United States, MPLS pricing is still 20% higher than comparable Internet-based solutions.

Using the Internet for connectivity and fail-over does not include or imply an open connection between CCN and the Internet: the virtual, transparent, secure secondary network runs **on top** of the Internet. A central gateway to **connect to** the Internet is proposed elsewhere in this report (see section 5.5) as an additional service.

Technology

Multiprotocol Label Switching (MPLS) is well-established as the primary choice of service for the enterprise WAN and should be used for the primary, core CCN/CSI network.

---

3) See "How to Significantly Reduce Networking Costs," 2 March 2010, Gartner Research G00174653

For the secondary, virtual network routed over the Internet, Internet Protocol Security (IPsec) is the most viable technology. IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host. The gateway-to-gateway tunneling mode is appropriate for CCN/CSI.

Since IPsec is a dual mode, end-to-end, security scheme operating at the Internet Layer of the Internet Protocol Suite or OSI model Layer 3, applications need not be specifically designed to use IPsec.

Routing decisions based on the type of application will, as described above, be based on the time sensitivity of the application and the business criticality of the application, as shown in Table 5.

MPLS	IPsec over Internet
Time-sensitive applications	Time-insensitive applications
Transactional applications	Batch-based applications
IP telephony	E-mail
IP videoconferencing	File transfer
SAP, Siebel	Content distribution
File sharing	Instant messaging

Table 5 Comparing MPLS and IPsec over Internet application suitability

The CCN equipment in all CCN/CSI locations will need to be extended to provide hybrid connectivity, in order to achieve a full mesh for both the primary and secondary networks, as depicted in Figure 3 below. At present, the CCN gateways already support two WAN networks, so possibly only the configuration would need to be updated.

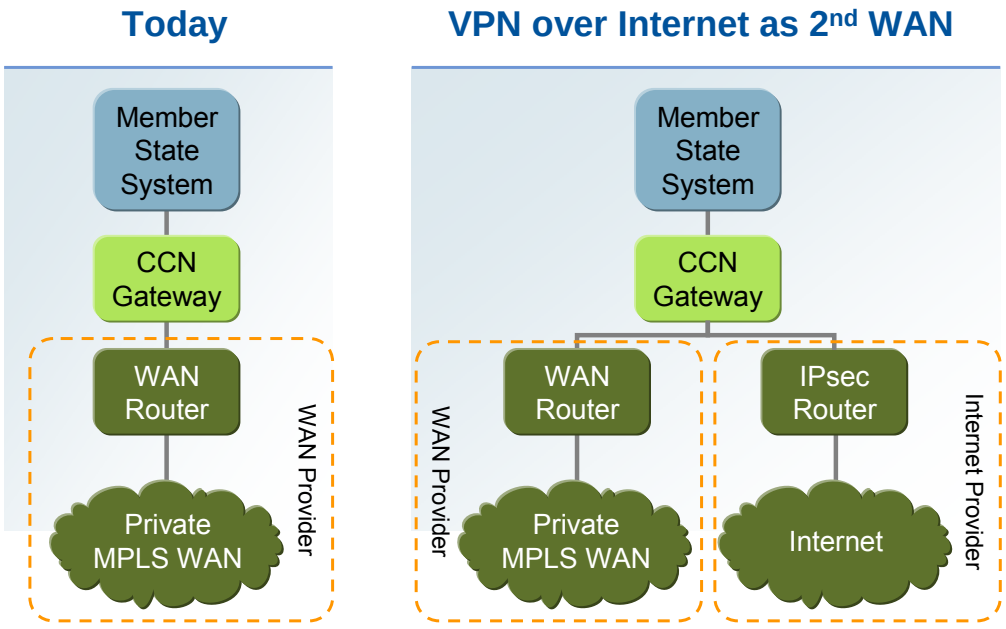

Figure 3 Using Internet for connectivity is handled by the WAN provider

Adherence to Requirements

Table 6 shows how leveraging the Internet for connectivity and fail-over adheres to the key high-level requirements.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	No impact
	Today's and tomorrow's applications are mission critical	A secondary WAN over the Internet is also a very resilient fail-over option, increasing reliability
	Proven technology	IPsec is a proven technology
Scalability	Volume will increase (40% YOY volume growth so far)	By moving bulk traffic onto the Internet, scalability is increased
Security	Refined access layers, also access for smaller local community offices	No impact

Table 6 Internet connectivity adherence to high-level requirements

As with the improvement of data center management, these WAN improvements primarily address the "do more with less" criterion by reducing operational costs. As there is no additional functionality, none of the other requirements are positively or negatively impacted.

There is a potential issue with existing security policies in CCN Participants by allowing some CCN traffic to flow over the Internet. This requires additional investigation. If properly setup, the security of the IPsec-based Internet traffic need not be less than that of the core WAN.

Development/Sourcing

The implementation of the hybrid network can be fully done by the network supplier. It is expected that this can be realized under the existing contracts.

Deployment/Maintenance

The deployment of the virtual, secondary network is fully transparent to both the CCN Participant applications and the CCN gateways. Network traffic routing according to quality levels and policies is handled completely by the WAN routers.

The operation of the WAN routers can either be handled by TAXUD or by the WAN provider. In the first scenario, TAXUD has full flexibility to choose the best Internet connections for each location, managing the IPsec VPN itself, centrally. The downside of this approach is a significant increase in required effort in terms of network management and supplier management.

In the second scenario, a single provider is chosen for managing both networks and operating the routers. Traffic routing policies will still be set by TAXUD. This scenario is depicted in Figure 3.

Dependencies

No dependencies with other improvements exist.

Risks

There is a risk that some CCN Participants do not accept any Internet-based solution. Although securing the secondary Internet-based WAN is technically feasible and viable by using IPsec (which is a proven technology), properly configuring security is complex and critical to the success of this improvement. This needs to be addressed before any implementation steps are made.

Effort

We assess the overall effort of this improvement as **low**:

- Realization could be fully outsourced to the existing WAN supplier;
- There is no impact on existing or new applications because the solution is transparent to the application layer.

Value

I2 brings more flexibility in CCN connectivity to CCN Participants. Non-mission critical traffic can be routed over the Internet in a secure fashion. We assess the value of I2 to the CCN Participants as follows:

- Although there a significant cost reductions to be made in terms of WAN costs, it will still be a relatively small reduction relative to the total yearly costs: <5%;
- There is no impact on development costs for CCN Participants;
- There is no impact on speed-to-market of new implementations.

Therefore, the overall value of this improvement is **low**.

4.3 Improve Common Testing Environment (I3)

Description

With 30+ CCN Participants, each implementing the specifications for the transactions that flow over the CCN/CSI network, testing is a key issue to ensure compliance and reliability. The distributed nature of application development and the way communications protocols are currently specified largely dictate the methods and structure for testing. At the high level, testing of distributed CCN applications can be divided into:

- **Application testing** by the CCN Participants themselves, for instance unit testing, integration testing, and user acceptance testing;
- **Conformance testing** supported by TAXUD, to test conformance to the specified message flows over the CCN network.

Application testing is fully in scope of the CCN Participants. Because each Member State implements the same common CCN specifications, duplication of testing effort exists and would be a good candidate for efficiency gains. However, because each application could have different functionality built "on top of" the common specifications, the testing effort is inherently complex and not easily centralized, and no quick improvement exists to make this more efficient without changing the way CCN applications are designed and developed. This is where the transformational options come into play, for instance T2 – Common components and T3 – Data container paradigm, which change the application development lifecycle, and thereby also dramatically improve the efficiency of the associated testing activities. For more information, see sections 6.3 and 6.4.

Conformance testing is done after the initial application tests. In this process, supported by TAXUD, the application under test is connected to a controlled test application (TTA) that simulates its CCN counterparty. At present, TAXUD spends a significant amount of time setting up these tests, running them, and reporting on the outcomes. The issues currently faced with the conformance tests are:

- No full coverage of all business scenarios;
- Maintenance of the tests: in case of change/creation/deletion of a scenarios/dataset, the other scenarios/dataset may be impacted and create issues during the CT campaign;
- No reliable validation of the scenarios and dataset before starting the CT campaign.

TAXUD can use modern technology to at least partly alleviate the challenges associated with conformance testing:

- Automation of test environment provisioning (setting up the virtual machines, configuring the queues, loading the test data);
- Virtualization of infrastructure, possibly using an elastic infrastructure (cloud) supplier;
- Applying test harness, test automation and test reporting tools where possible.

In addition, overall software quality could increase if an improved testing environment leads to more frequent testing (that happens earlier in the development cycles of the applications), ultimately leading to lower application maintenance costs and fewer production incidents.

Technology

By using **system provisioning** tools, as described in section 4.1, efforts to create (on demand) a homogeneous, isolated test environment for a CCN Participant can be significantly reduced. In addition, using these tools ensures a clean, stable baseline environment for the CCN Participants to run their tests on using configuration management tooling.

Virtualization technology (also described in section 4.1) is particularly useful when multiple CCN Participants would like to run tests in parallel. Virtualization allows TAXUD to rapidly set up a large number of isolated test environments that can be used independently from each other and in parallel. Virtualization software allows easy and automated creation, replication and deletion of virtual machines.

Virtualization also allows TAXUD to, whenever the capacity demands exceed the regular, in-house infrastructure, go onto the market and acquire (or rent) virtual infrastructure capacity for a period of time. The market for elastic, on-demand virtual cloud infrastructure capacity is rapidly maturing, and traditional hardware vendors such as IBM are now also offering capacity. Obviously, security, privacy, availability and performance are important factors that would need to be taken into account, but Gartner believes that using cloud infrastructure capacity for the testing environment (on an as-needed or permanent basis) is a valid option that should be considered.

By only paying for used capacity, cloud infrastructure can be a valuable addition to TAXUD's existing test infrastructure. It increases flexibility by providing an almost instantaneous and unlimited extension of capacity, when required.

The third technology area, **automated software test** products, also known as automated software quality assurance (ASQ) products, consists of two key categories:

- Test management – Tools to manage and plan testing activities and their results;

- Automated functional and regression testing – Tests that mimic a single user to find defects in the application.

In general, software quality encompasses a much broader number of activities, and thought leaders are driving broader toolsets and creating better integration across the life cycle. Other areas include test data selection and management, unit testing, security and compliance, and usability. The market is also evolving to better support package applications, deal with SOA and Web 2.0 technologies, and take advantage of virtualization and SaaS delivery mechanisms.

Recent years have seen an improvement in the integration of ASQ tools with the rest of the application lifecycle management platform (which also includes requirements management, and software change and configuration management) to help automate the overall execution of software projects. This includes integration between requirements and test cases, integration into the build process for automated execution of test suites, and integrated reporting to better understand the current status of a project from a quality and completeness perspective.

For TAXUD, a subset of these test tools would be applicable, and be valuable for the CCN Participants. Firstly, automated functional and regression testing tools can be used to test complete message exchanges, based on the common specifications, at the CCN/CSI interface level. Using these test tools, functional users creating the specifications should also be able to create test cases for regular and exceptional message flows, which can subsequently be tested in the virtual test environment. These tools could thus (partially) cover the current need for custom developments (TTA).

Secondly, test management tools allow for the aggregation of test results from these scripts, giving the CCN Participants insight into what tests failed using a dashboard approach. This would reduce the burden on TAXUD's support personnel, and allow for better, integrated management of the test environments and the tests to run.

Today, TAXUD already automates some areas of the conformance tests. The added value is therefore mostly in the better integration between planning and execution, and the ability to involve the functional users (that create the CCN specifications) in writing the test scripts, as opposed to having a CCN developer program them into the TTA application.

Adherence to Requirements

Table 7 shows how improving the common testing enviroment adheres to the key high-level requirements.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	No impact
	Today's and tomorrow's applications are mission critical	Better testing leads to higher software quality, resulting in fewer production incidents
	Proven technology	Test tools and management solutions are proven
Scalability	Volume will increase (40% YOY volume growth so far)	Automated testing is extremely scalable
Security	Refined access layers, also access for smaller local community offices	No impact

Table 7 Common testing environment adherence to high-level requirements

Development/Sourcing

Acquisition of the software licenses for the test tools and the hiring of expert resources for implementing them is expected to fall within existing framework contracts.

The infrastructure capacity required for the test environment depends on I1, as virtualization and server provisioning are prerequisites for providing a scalable and flexible testing platform to the CCN Participants.

Deployment/Maintenance

The deployment of the test environment would use the improved data center management processes. The virtualized environments are expected to be run centrally. Alternatively, the CCN gateway appliance could also host a test service to cover some of the testing requirements of CCN Participants.

Operations and maintenance of the testing environment would be part of regular data center operations. By using server provisioning and virtualization tools, the test environment can be scaled up and down with relatively little effort.

Dependencies

These improvements depend on the implementation of I1, improved data center management, specifically the server configuration and provisioning tools.

Risks

The risk associated with implementing these improvements is low. The implementation of a common testing environment is independent from the production environment, so it should be fully transparent to the business service consumers.

Effort

The required effort for the implementation of the common testing environment falls into two parts: the initial investment for getting the environment and tools up and running, and the ongoing effort to translate specifications into automated test scripts.

The initial investment is considered to be of **medium** effort. Cost is expected to be 1 to 5 M€, with a duration of 9 to 18 months.

The ongoing efforts will be significant as well. The TAXUD specifications are complex, requiring large amounts of effort to translate these into tests, and it is expected that no more than 50% of the tests could be automated, limiting the benefits. However, translating the specifications into test scripts is already done today by each of the CCN Participants. The economies of scale of centralizing at least part of this effort will result in net savings from a holistic standpoint.

Value

Once the test environment is in place, and the specifications can be tested automatically (at least partially), the CCN Participants will be able to realize significant cost savings, both directly (from reduced testing effort) and indirectly (from increased software quality leading to reduced corrective maintenance costs).

No direct benefits exist for deployment and maintenance, however indirectly, as mentioned above, corrective application maintenance costs will be reduced as a result of higher quality software.

We assess the value of the common testing environment as follows:

- Development costs for CCN Participants are expected to be reduced significantly: more than 30%;
- Speed-to-market will be improved as well, but still less than 25%;
- Overall total maintenance costs will be reduced as well, but as corrective maintenance is not a large part of the overall annual budget, these savings will be less than 5%.

Therefore, the overall value is considered to be **medium**.

4.4 Open Specifications (I4)

Description

The TAXUD provided specifications for CCN applications rely on proprietary standards. The FTSS and DNxA documents specify in detail the message flows between the applications. The FTSS documents represent the global/functional design. The DNxA documents the detailed/technical design. In a recent study for TAXUD Gartner demonstrated how the specifications can become less proprietary by following the BPMN standard to model the processes and XML Schema to model the messages. A brief summary of the recommendations follows below.

For process design the emerging de facto standard is BPMN (Business Process Modeling Notation). This standard is maintained by OMG. The current version is 1.2 established January 2009. Version 2.0 is expected to be standardized in June 2010.

Version 1.2 already covers the process elements found in the FTSS and DNxA documents. However, Gartner expects version 2.0 to realize a major breakthrough in the adoption of BPMN both by organizations and vendors.

Semantics and data design relates to the contents of the messages being exchanged between the participants. Semantics reflect the meaning of data elements (e.g. a country code reflecting a country), syntax determine the format (e.g. country code is two alphanumeric positions).

There are many semantic standards. Gartner recommends TAXUD to define a hierarchy of semantic standards. This hierarchy or cascading list may look like:

- *CCN Application specific standards* — specific semantics that have been developed as part of the specification. e.g. message codes.
- *CCN Domain specific standards* — e.g. WCO Harmonized System (HS), the Goods Classification Code, UN/CEFACT standards.
- *European Commission promoted standards* — e.g. the standards promoted on www.semic.eu as part of DIGIT's IDABC program.
- *Other commonly used standards*. — e.g. ISO standards, EUROSTAT standard code list (SCL) for currencies

The de facto standards for modeling message or document formats is XML Schema (XSD). The current version is 1.0 since 2004. XML Schema is a W3C standard. W3C has released version 1.1 as "candidate recommendation" last August, standardization is expected in Q2 2010. Version 1.1 is more elaborate than version 1.0. Gartner recommends to use XML Schema 1.0 to specify message formats. There exists wide tool vendor support for XML Schema.

Technology

Using open standards will foster horizontal and vertical interoperability. Horizontal interoperability covers the dissemination of specifications to the Member States in such a way that the specification can be reused by the Member State in their modeling environment. Horizontal interoperability goes beyond exchanging specifications in PDF format. Vertical interoperability is the possibility to directly use a specification to generate the implementation of the specification. Vertical interoperability is also known as Model-Driven Architecture (MDA).

Vendor support that enables the reuse of BPMN and XML Schema specifications across different platforms is becoming more mature.

Development/Sourcing

The usage of these standards should be agreed upon with the CCN Participants and become part of the CCN standards list.

Deployment/Maintenance

A governance process must be in place to ensure that version management of the standards is in place. When a newer version gains sufficient momentum this newer version should become the CCN standard.

Dependencies

This option can be executed independently from other options.

Risks

Care must be taken when selecting the versions of the standards.

Effort

The TAXUD effort to implement the usage of the open standards is limited. Gartner assesses the effort as **Low**.

Value

For the CCN Participants I4 will imply easier understanding of new CCN application specifications, easier reuse of the specification and possible generation of parts of de code of new CCN applications. Easier understanding because BPMN and XML Schema are common standards. Easier reuse because BPMN and XML Schema definitions can be loaded into tooling (for BPMN starting at version 2.0). Possible generation because tooling exist that can transform BPMN and XML Schema definitions into e.g. BPEL which can be executed by a BPEL engine (BPMN version 2.0 can also directly be executed, Gartner expects BPMN to replace the BPEL standard).

Gartner assesses the value of the I4 scenario as follows:

- The total maintenance cost will not change significantly;
- The total development cost may show savings of up-to 30% due to better understanding of the specifications and possible generation of code;
- The speed-to-market may be reduced with 1 to 2 years for the same reasons.

Therefore, Gartner assesses the value of I4 as **medium**.

4.5 Conclusions

Improvement	Effort	Value	Maintenance	Development	Speed2M
I1 - Data center	Medium	Low	Low	Low	Low
I2 – Internet	Low	Low	Low	Low	Low
I3 – Testing	Medium	Medium	Low	High	Low
I4 – Open Specs	Low	Medium	Low	Medium	Medium

Table 8 Assessment of the identified improvements

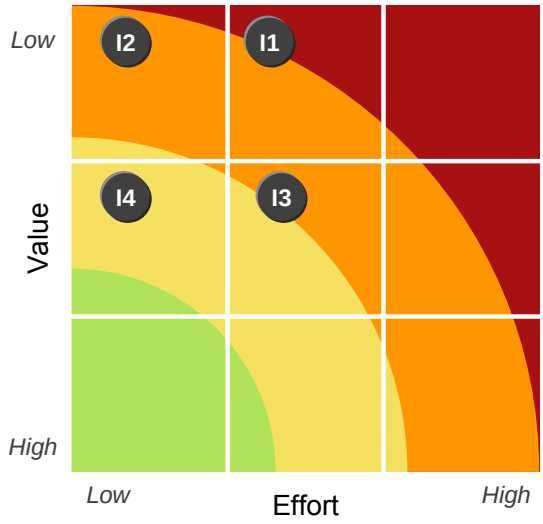

Figure 4 Assessment of value vs. effort for the identified improvements

5.0 Additional Services

5.1 Common Infrastructure services (S1)

Description

At present, each CCN Participant runs its own data center to support its CCN/CSI applications. In there, both the CCN gateway and the CCN/CSI applications are run. Non-functional requirements such as high performance and high availability require significant investments in redundant infrastructure and operational processes.

These investments could be too costly for some CCN Participants, especially the smaller Participants that run only a small amount of applications and therefore cannot benefit from economies of scale.

TAXUD could play a role in bringing together some of these CCN Participants, colocating their applications in a single, combined data center, thus introducing economies of scale. TAXUD's role could vary from only facilitating discussions between CCN Participants to managing the entire acquisition and provision process of the combined data center, including managing the CCN/CSI components.

The CCN Participants that share their data centers would enjoy reduced costs, enhanced continuity and future scalability.

Technology

When sharing a data center, operational processes (such as configuration management and capacity management) need to be formalized. The data center processes and tools described in section 4.1 are all relevant to this end: implementing specific parts of the IT Infrastructure Library (ITIL), supported by the implementation of technology components such as server provisioning and configuration management tools, smart infrastructure monitoring, and virtualization technology to create separate environments for each CCN Participant.

Adherence to Requirements

Table 9 shows how common infrastructure services adhere to the key high-level requirements.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	No impact
	Today's and tomorrow's applications are mission critical	High availability infrastructure ensures continuity even to the smallest of CCN Participants
	Proven technology	Infrastructure management and virtualization technology is proven
Scalability	Volume will increase (40% YOY volume growth so far)	Centrally managed infrastructure allows for better capacity planning to accommodate future growth
Security	Refined access layers, also access for smaller local community offices	No impact

Table 9 Common infrastructure services adherence to high-level requirements

Development/Sourcing

The shared data center could be provided by a market supplier or by a single CCN Participant. In case of a market supplier, virtualized infrastructure with a flexible capacity/payment scheme will be most cost effective. An alternative solution would be investing in a shared data center that is dedicated to the CCN Participants joining in.

In addition to procuring infrastructure from the market, a large CCN Participant could sell spare capacity in one of its data centers (that already is CCN/CSI-enabled) to the group of smaller CCN Participants. An example could be the UK's Government Cloud (G-Cloud).

In all cases, TAXUD would either not be involved in the procurement process at all, or only in an advisory role.

Deployment/Maintenance

Deployment of the common infrastructure platform would be dependent on the chosen acquisition model and the role TAXUD would play therein.

Dependencies

No dependencies with the other improvements or services exist. Configuration management tools from I1 could be leveraged.

Risks

Two risks associated with this service can be identified:

- Sharing infrastructure introduces the risk of incidents impacting multiple CCN Participants at the same time. Virtualization technology would need to be used to ensure isolation of applications to mitigate this risk;
- Procuring the infrastructure from the market, especially in a virtualized cloud manner, could lead to concerns about data protection and security. The agreements with the supplier would need to address these concerns.

Effort

It is expected that the initial investment would be 1 - 5 M€, with a duration of 9 - 18 months. After procuring the infrastructure, it needs to be configured for CCN/CSI. After that, the applications from the CCN Participants need to be migrated in order to realize the benefits. Therefore, we assess the effort for setting up a shared infrastructure as **medium**.

Value

For the CCN Participants with limited capacity to operate data centers S1 will bring significant value. The key benefit of shared infrastructure services is cost reduction for the CCN Participants, both directly (by saving on infrastructure costs) and indirectly (by benefiting from better processes and increased reliability).

We assess the value of the common infrastructure services for the CCN Participants as follows:

- Maintenance costs could be reduced by 5 to 15%;
- Application development costs would not be impacted;
- Increased flexibility would lead to some speed-to-market improvements (less than 25%).

Therefore, the overall value of this additional service is **low**.

5.2 Business Activity Monitoring (S2)

Description

Every day, large amounts of network messages flow over the CCN network, all being part of business transactions. Valuable business insight can be derived by aggregating and analyzing this data.

At present, TAXUD already employs network monitoring and, for some types of transactions, business process monitoring. These monitoring tools are custom made for each type of transaction, and are therefore costly to create, change and maintain. In addition, gathering statistics and generating reports requires intervention from TAXUD's technical support personnel and has at least a 24 hour lead time.

True business activity monitoring (BAM) aims to provide real time information about the status and results of various operations, processes, and transactions. The main benefits of BAM are to enable an enterprise to make better informed business decisions, quickly address problem areas, and re-position organizations to take full advantage of emerging opportunities.

One of the most visible features of BAM solutions is the presentation of information on dashboards that contain key performance indicators (KPIs) used to provide assurance and visibility of activity and performance. This information is used by technical and business operations to provide visibility, measurement, and assurance of key business activities. It is also exploited by event correlation to detect and warn of impending problems.

Although BAM systems usually use a computer dashboard display to present data, BAM is distinct from the dashboards used by business intelligence (BI) in so far as events are processed in real-time or near real-time and pushed to the dashboard in BAM systems, whereas BI dashboards refresh at predetermined intervals by polling or querying databases. Depending on the refresh interval selected, BAM and BI dashboards can be similar or vary widely.

TAXUD could provide a BAM platform to CCN Participants, which would enable end users to monitor their processes on-demand from end to end in a meaningful manner. For example to alert customs if a truck passes the German border just 20 minutes after loading goods in Antwerp.

The key benefit of a full BAM platform is the fact that end users are able to setup (and remove) triggers and monitors, and see relevant information in real time, without any intervention from TAXUD's valuable technical support personnel.

Technology

According to Gartner, BAM technology can either be a completely stand-alone solution, monitoring message flows and providing a separate event analysis and correlation environment, or it is integrated in modern business process management (BPM) and enterprise service bus (ESB) suites.

Using a publish/subscribe model, **stand-alone BAM** applications subscribe to relevant messages, extracting activity information as messages are received. As this generation matured, other techniques for gathering event objects were adopted, such as application adapters, change data capture agents, log file transfers and screen scraping.

The defining characteristic of a stand-alone BAM application is that it connects to multiple event sources and has its own extensible data model which is populated by a transformation layer that normalizes attributes across multiple event formats. The continuous update of the data model, dashboards and threshold evaluation provides the real-time nature that traditional BI tools do not offer as depicted in Figure 5.

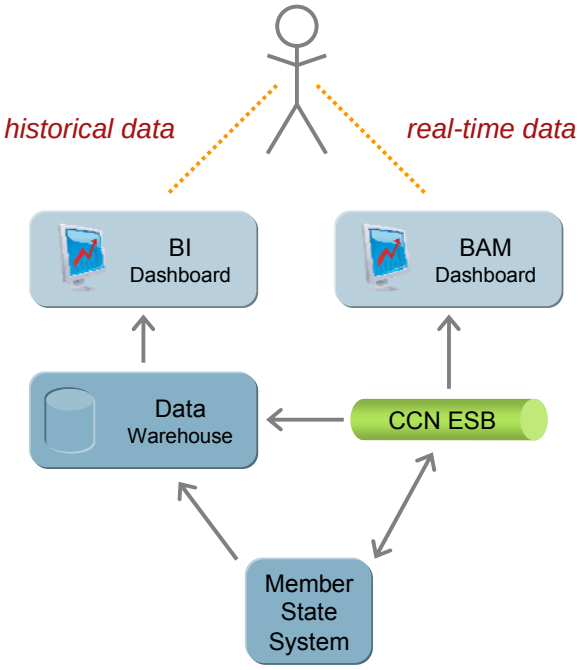

Figure 5 Conceptual differences between BAM and BI

A similar approach to monitoring, targeted to IT infrastructure operations rather than business operations, is available from vendors such as BMC Software, IBM Tivoli and HP/Mercury, sold as business service management tools. Vendors that deliver a platform for building stand-alone BAM applications include Altosoft, IBM Cognos Now!, Systar, SeeWhy Software and Syndera.

The prime examples of vendor products supporting an **integrated BAM** model are IBM WebSphere Business Monitor, Oracle BAM, Progress Software Apama, Software AG Optimize and Tibco BusinessFactor. In each case, the BAM software is able to stand on its own, but includes inherent features to integrate into vendor's process development and execution tools. In the case of Oracle, and eventually SAP, BAM software is part of their software stack, available as a shared service for applications developed by the vendor's or their customer's developers. This model will mature and persist through 2020.

A defining characteristic of integrated BAM is that it is integrated into a larger software development environment and integrated with specific applications, like first generation BAM, but can absorb and emit events outside its environment. Organizations should evaluate a vendor's BAM offering in the context of purchasing business applications, software development stacks and business process management suites.

The value of an integrated solution may outweigh the competitive differences of best-of-breed BAM platforms. For example, the integration between a process modeler and the BAM dashboard simplifies change management by keeping BAM models synchronized with orchestrated workflows, while a best-of-breed BAM platform may offer better deadline and service-level monitoring applications.

In summary, a stand-alone BAM solution could already provide added value for TAXUD and the CCN Participants in the CCN 1.x scenario. In the CCN 2.0 scenario however, the BAM option should be evaluated together with the selection of the ESB, as several ESBs come

with an integrated BAM solution, and specific CCN-BAM adapters would not need to be developed.

Adherence to Requirements

Table 10 shows how business activity monitoring adheres to the key high-level requirements.

Development/Sourcing

Procurement of licenses for BAM technology is expected to be supported by existing framework contracts of the Commission. The implementation effort will be managed by TAXUD internally, using either internal or external resources.

Deployment/Maintenance

The BAM platform would need to be deployed in a central data center and operated by TAXUD. We envision that each CCN Participant has access to a dedicated environment where end users can set up alerts and monitor activity. Some form of isolation from the other CCN Participants would need to be assured.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	No impact
	Today's and tomorrow's applications are mission critical	No impact
	Proven technology	BAM has matured and is proven in specific situations
Scalability	Volume will increase (40% YOY volume growth so far)	BAM is scalable to very large amounts of data
Security	Refined access layers, also access for smaller local community offices	No impact

Table 10 Business activity monitoring adherence to high-level requirements

Dependencies

In principle, no dependencies to the other improvements or services exist. The BAM service could be realized on top of the present CCN architecture (by using custom developed CCN-BAM adapters).

However, the BAM platform is related to the ESB scenario as part of CCN 2.0. Implementation of an ESB in CCN 2.0 (T1) enables the realization of a BAM without the custom developments, in other words: at lower cost than providing BAM on top of CCN 1.0.

No other dependencies exist.

Risks

A key concern with the BAM is data security and protection. CCN Participants could be reluctant to allow the type of traffic inspection that is necessary for the BAM to monitor transactions at a business level and correlate events. End user access control needs to be

configured properly, and data gathered needs to be secured according to CCN Participant requirements and policies. This is a policy issue, and not a technical matter.

Effort

The investment is expected to be 1 - 5 M€, with a duration of 9 - 18 months. The product needs to be installed, configured and custom probes need to be developed to monitor the CCN traffic. In addition, the BAM needs to be configured (access restrictions are of particular concern), and end users need to be trained before the benefits can be realized.

Therefore, we assess the implementation effort of a BAM solution as **medium**.

Value

BAM will enable the CCN Participants to monitor the behavior of the CCN applications in real-time in a universal fashion without investing in technology for each application separately.

Once the BAM platform is in place, the current custom monitoring solutions can all be deprecated. This results in a significant reduction in code base, lowering maintenance costs.

Although a common BAM platform can have significant value for the CCN Participants, if regarded using the assessment methodology described in section 3.4, the overall value is still **low**:

- Total maintenance cost is considered to be reduced by 5 to 15%;
- Development cost will be reduced by less than 10%;
- And although speed-to-market will be improved considerably for new monitoring requirements, the overall effect will be less than 25%.

5.3 Master Data Management (S3)

Description

The Customs Union that is supported by TAXUD requires CCN Participants to share large amounts of information and data. At present, TAXUD maintains a number of custom solutions to maintain the common data set amongst the CCN Participants.

Historically, bandwidth constraints on the CCN network required the replication of common data amongst the CCN Participants. At present, all data is replicated across applications using custom interfaces, and proper reconciliation does not always happen. Point-to-point data synchronization scripts have proliferated, and managing the data has become more and more complex. In effect, there is no notion of a single truth. In short: there is sharing of common data, but it is not properly managed.

Master data management (MDM) comprises a set of processes and tools that consistently defines and manages these types of non-transactional data entities. MDM has the objective of providing processes and tools for collecting, aggregating, matching, consolidating, quality-assuring, persisting and distributing such data throughout an organization to ensure consistency and control in the ongoing maintenance and application use of this information.

Today, the original constraints no longer exist, and TAXUD could use MDM processes and tools to:

- Rationalize the current common data set, reducing complexity and increasing data quality;

- Centralize and manage other common data, that is now dispersed across the CCN Participants.

The long term benefit to CCN Participants would be to be able to rely on the single truth, provided by TAXUD: information as a service. On the short to medium term, the MDM tooling could be used to replace many of the custom scripts by a single solution, simplifying the environment, thereby reducing cost and chances of error.

Technology

MDM technology enables organizations to ensure the uniformity, accuracy, stewardship, semantic consistency and accountability of the enterprise's official, shared master data assets, enabling organizations to eliminate endless debates about "whose data is right," and ensure that different IT systems and functional or product line groups within the organization are sharing the same master data.

Data integration tool markets have traditionally been of a "siloed" nature. Separate markets and vendors existed for the various classes of data integration technology, such as extraction, transformation and loading (ETL), data federation and replication. Convergence continues among the data integration technology submarkets, as vendors extend their capabilities to add other data integration styles, and larger vendors amass technology that spans many of these submarkets. In addition, buyers of these tools increasingly seek a full range of capabilities to address multiple use cases.

These converged tools will include the core elements of data integration, but with the ability to deploy these elements in a range of different styles (including as data services), driven by common metadata and modeling, design and administration environments. The goal is to model integrated views and data flows once, and to be able to deploy them in various runtime modes - from batch to real-time, from physical to virtualized, and so on.

Example vendors that provide data integration tools to support master data management are: iWay Software, IBM, Informatica, Oracle, SAP BusinessObjects, SAS Institute, and Sybase.

Adherence to Requirements

Table 11 shows how master data management adheres to the key high-level requirements.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	No impact
	Today's and tomorrow's applications are mission critical	Increased reliability by using a single truth and common definitions
	Proven technology	MDM tools are proven
Scalability	Volume will increase (40% YOY volume growth so far)	MDM tools give the required flexibility to rapidly accommodate new, future common data
Security	Refined access layers, also access for smaller local community offices	No impact

Table 11 Master data management adherence to high-level requirements

Development/Sourcing

Procurement of licenses for MDM technology is expected to be supported by existing framework contracts of the Commission. The implementation effort will be managed by TAXUD internally, using either internal or external resources.

Deployment/Maintenance

The deployment of MDM would primarily be done centrally and operated and maintained by TAXUD. Process agreements with CCN Participants would be needed for each (set of) data synchronization script(s). Some form of data transfer mechanism (push/pull, publish/subscribe) would need to be agreed as well.

Dependencies

In principle, no dependencies with other improvements or services exist. Leveraging the Internet for connectivity and fail-over (I2) would enable the synchronization and replication of large amounts of data to occur over the Internet, leading to lower WAN costs.

Risks

By centralizing more information, data security becomes a larger issue than it is today. Access control and protective measures will have to be installed, in line with CCN Participant requirements and policies.

Effort

The implementation effort of full MDM is considered to be of **medium** size. The platform and tools need to be installed and configured, the processes need to be put into place, and a migration effort will need to be done. Such an effort will probably include discussions with CCN Participants on data quality as well, to ensure a clean starting point for the MDM.

Value

By being able to rely on more central data, that is uniformly defined and of high quality, CCN Participant applications could become less dependent on local data stores, reducing complexity and overall development efforts for the CCN Participants.

Application deployment and overall maintenance costs will be reduced once the MDM platform is in place. Custom data synchronization scripts, that are hard to develop, maintain and error-prone, are no longer required.

Uniform definitions and information ultimately lead to higher quality of business process execution and a lower incident rate.

More directly, and evaluated against the assessment methodology (see 3.4):

- Application development costs would be lowered (10 – 30%);
- Total maintenance costs would be lowered (5 – 15%);
- Speed-to-market will be somewhat improved: less than 25%.

Therefore, we assess the overall value of the MDM service as **medium**.

5.4 Federated Identity (S4)

Description

All CCN Participant applications connected to CCN employ the CCN user authentication and authorization. Currently, CCN offers a model of federated identity management and a single sign-on mechanism, based on a proprietary implementation, which is not integrated at all with any stronger mechanism already in place in national administration.

Users are managed by national administration security officers and are allocated the required access profiles according to their role as defined in the application specification. The central applications operated by TAXUD get the user identification and access profiles from the CCN network, but there is a very complex process for synchronizing this information with the internal authorization mechanism of the application server.

In the case of Commission internal users, user management is specific and managed by TAXUD. It relies on the internal authorization mechanism of the application server.

The present fully custom built solution results in higher-than-desired vendor captivity and integration issues.

Federated identity based on open standards would alleviate these problems, as it allows the sharing of identities across the CCN network, leveraging existing authentication schemes already in use by the CCN Participants. It would reduce maintenance costs, while improving overall security.

Additional functionality would also become available, for instance CCN Participant A could give officials of a certain rank in CCN Participant B read-only access to certain applications that reside in CCN Participant A. The officials in CCN Participant B would then use their own authentication mechanisms.

TAXUD could implement a mechanism to facilitate federated identity, leveraging available open source components and open standards for identity sharing. In that way, TAXUD would provide the standards and tools to support a "community of trust" that can easily be re-used across all CCN Participant applications.

Note that there is no central user directory or account management; the re-use of existing directories and processes is a key benefit of federated identity.

The scope of this proposed new service is federated identity for CCN Participant officials that are users and/or administrators of the CCN applications, and as such already are part of the existing authentication frameworks residing in the CCN Participants.

In the future, this service could be extended to include citizens as well, by connecting to the various national eID initiatives that are currently underway (for instance, DigiD in The Netherlands). Although this would be a complex undertaking, federated identity technology does allow it.

Technology

The recommended standard to use for sharing identity information is the Security Assertion Markup Language (SAML). It is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.

SAML assumes the principal (often a user) has enrolled with at least one identity provider. This identity provider is expected to provide local authentication services to the principal.

However, SAML does not specify the implementation of these local services; indeed, SAML does not care how local authentication services are implemented.

Thus a service provider relies on the identity provider to identify the principal. At the principal's request, the identity provider passes a SAML assertion to the service provider. On the basis of this assertion, the service provider makes an access control decision.

Figure 6 describes this process conceptually. The User Agent requests a service from the Service Provider (1), which responds with an authentication challenge (2). The User Agent authenticates itself with the Identity Provider (3, 4) and forwards the SAML assertion to the Service Provider (5). The Service trusts the assertion and redirects the User Agent to the protected resource (6, 7, 8).

By relaying SAML messages over the CCN network, and using SAML in the common applications that are under its control, TAXUD will provide the technical means necessary for federated identity.

Most of the effort is of a organizational alignment matter. CCN Participants will need to agree on security policies, role descriptions and the actual usage of the SAML messages. These are non-technical discussions that TAXUD could facilitate but not resolve by itself.

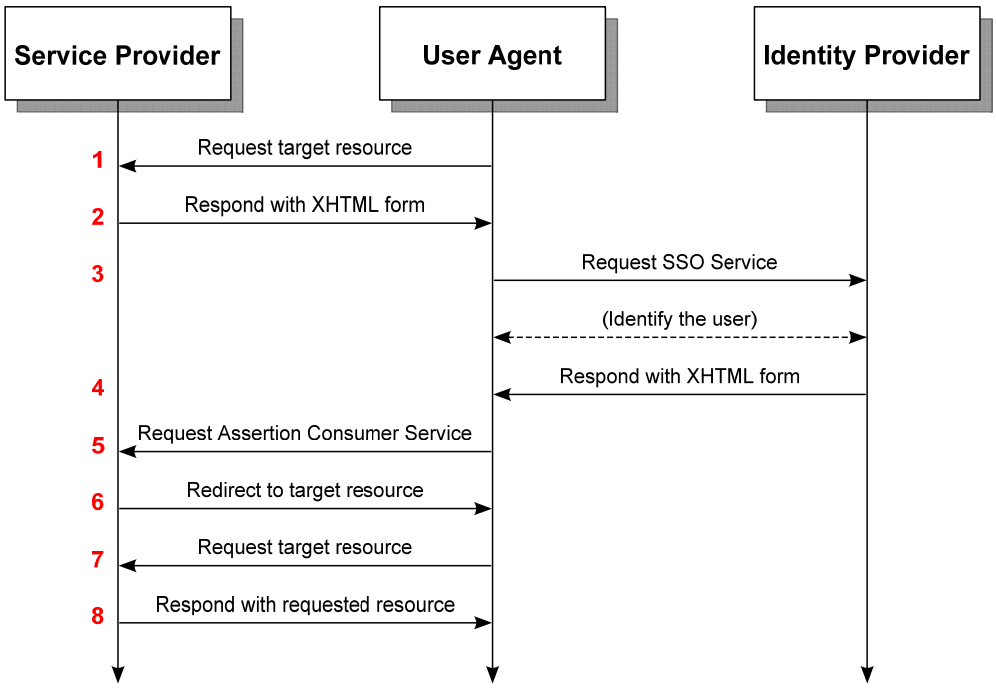

Figure 6 SAML example

Adherence to Requirements

Table 12 shows how federated identity adheres to the key high-level requirements.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	No impact
	Today's and tomorrow's applications are mission critical	No impact
	Proven technology	SAML is a widely adopted open standard that is implementation independent and gives maximum flexibility
Scalability	Volume will increase (40% YOY volume growth so far)	No impact
Security	Refined access layers, also access for smaller local community offices	Commonly agreed access profiles allow for better access control. Also, central authentication mechanisms are more secure than existing application-level solutions

Table 12 Federated identity adherence to high-level requirements

Development/Sourcing

No specific tools are required to implement federated identity. Significant effort is required to connect all existing CCN Participant central user authentication mechanisms to the CCN SAML messages in a standardized way. In addition, agreements will have to be made in order to establish the community of trust at the organizational level.

It is expected that the required human resources are procured using existing contracts.

Deployment/Maintenance

No central tools need to be deployed. TAXUD's role in deploying and maintaining the Federated Identity service would be process-oriented, to standardize the SAML message exchanges and by facilitating agreements between CCN Participants to establish a community of trust.

Dependencies

Federated identity can be realized in the current CCN landscape without dependencies on other improvements or services.

The ESB solution from CCN 2.0 (T1) could help implementation, as in some cases the ESB can mediate an interaction that crosses security domains by mapping credentials from one domain to credentials that are acceptable by the second domain.

Risks

The implementation of federated identity by itself does not introduce risks. However, as CCN Participants will start to trust authentication mechanisms in other CCN Participants, security policies are necessary to avoid an overall lower security if a single CCN Participant proves to be the weakest link.

Effort

The estimated effort for a full implementation of federated identity is **high**, as this would require agreement and alignment of user authentication mechanisms and would need to include migrating existing applications to achieve full benefits. Duration would be > 18 months, with an estimated cost of > 5 M€.

Value

For the CCN Participants, significant value can be gained in the application development and maintenance processes, as a direct result of being able to reuse centralized authentication mechanisms and the removal of duplicated effort for user account management.

By removing duplicated efforts for user authentication and account administration, overall maintenance costs are reduced considerably. However, full benefits can only be realized once existing applications are migrated onto the new federated identity platform as well.

Federated Identity is assessed as follows:

- Development costs are expected to be reduced by 10 to 30%;
- Maintenance costs are expected to be reduced by 5 to 15%;
- Some gains in terms of speed-to-market are expected as well: less than 25%.

Therefore, we assess the overall value of Federated Identity as **medium**.

5.5 Central Internet Gateway (S5)

Description

CCN Participants are having increasing demands for secure and reliable electronic messaging with non-Participants, such as countries outside the EU with which large amounts of trading take place. At present, the CCN network is closed, and Participants would need to implement their own bilateral communications agreements and technology. This constitutes a potential duplication of implementation effort and many peer-to-peer connections that are, on the whole, difficult to manage and control.

With the Internet being ubiquitous, the infrastructure to communicate with these non-Participant countries is already there. TAXUD could play a role and offer a tightly controlled yet flexible CCN-to-Internet Gateway. The objective is to have all CCN-to-Internet traffic pass over this central gateway to simplify operations and to ensure compliancy to security and other related policies.

The benefit for CCN Participants would be a reduction in effort whenever communications need to be set up with a country or trading partner outside the CCN realm.

Technology

In its most basic form, the Central Internet Gateway would be a combined firewall and router, operating at the TCP/IP layer. This would allow routing and access policies based on TCP/IP parameters such as addresses and ports, as well as enabling security at the network level through IPsec. The Gateway would not be concerned with message content.

Additional functionality, such as bi-directional transformations and mappings between CCN messages and other message types, and more fine-grained access control, would require specific software. An ESB would be required with specific adapters for each external

message type. Today's ESBs provide straightforward message transformation tools and adapters that only need configuring.

Adherence to Requirements

Table 13 shows how the Central Internet Gateway adheres to the key high-level requirements.

Development/Sourcing

Procurement of the router/firewall hardware and the Internet links is expected to be supported by existing framework contracts of the Commission. Implementation of the basic firewall/routing solution could be outsourced to the WAN provider.

If additional functionality is desired, the required ESB licenses need to be procured. These are expected to fall under existing contracts as well. The implementation effort will be managed by TAXUD internally, using either internal or external resources.

Deployment/Maintenance

To avoid a single point of failure, the Central Internet Gateway would need to be deployed in a fully redundant fashion with fail-over functionality. Multiple Internet links, based on different network technologies and using different access providers, are essential.

In case of the more basic router/firewall solution, maintenance of the Gateway could be outsourced with the existing WAN provider. Creation and maintenance of the routing and access policies would still be a responsibility for TAXUD.

Should the ESB-based solution be chosen, an appropriate hardware platform would need to be deployed in the central data center and operated and maintained by TAXUD.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	No impact
	Today's and tomorrow's applications are mission critical	No impact
	Proven technology	Firewall, routers and ESBs are all proven technology
Scalability	Volume will increase (40% YOY volume growth so far)	No impact
Security	Refined access layers, also access for smaller local community offices	The Internet Gateway allows for secure connections and routing based on policies. With the addition of message transformation functionality, more finely grained access control can be achieved

Table 13 Central Internet Gateway adherence to high-level requirements

Dependencies

The basic router/firewall solution does not depend on other improvements or services, although implementation would be more efficient if combined with I2 – using the Internet for connectivity and fail-over.

The ESB solution is dependent on improvements in data center management and provisioning: I1.

Risks

Two risks are associated with this additional service:

- Single point of failure. As mentioned above, the Central Internet Gateway needs to be made fully redundant to ensure no single point of failure;
- Reluctance of CCN Participants. Perhaps Participants would like to keep control of communications with external parties to themselves. Proper agreements and open, transparent policies are required to ensure buy-in.

Effort

We assess the overall effort of this additional service as **low**:

- Realization of the basic router/firewall solution could be fully outsourced to the existing WAN supplier;
- Realization of the more advanced ESB-based solution is still relatively simple because it is isolated from other CCN components and functionality;
- There is no impact on existing or new applications because the solution is transparent to the application layer.

Value

S5 would provide CCN Participants easier means to connect to non-CCN Participants.

We assess the value of S5 to the CCN Participants as follows:

- Although there a significant cost reductions to be made in terms of WAN costs, it will still be a relatively small reduction relative to the total yearly costs: <5%;
- There is a small amount of positive impact on development costs for CCN Participants: <10%;
- The speed-to-market of new implementations is slightly improved.

Therefore, the overall value of this improvement is **low**.

5.6 Conclusions

Additional service	Effort	Value	Maintenance	Development	Speed2M
S1 - Infra services	Medium	Low	Medium	Low	Low
S2 - Activity mon.	Medium	Low	Low	Low	Low
S3 - Master data	Medium	Medium	Medium	Medium	Low
S4 - Federated id.	High	Medium	Medium	Medium	Low
S5 - Internet gatew.	Low	Low	Low	Low	Low

Table 14 Assessment of the identified additional services

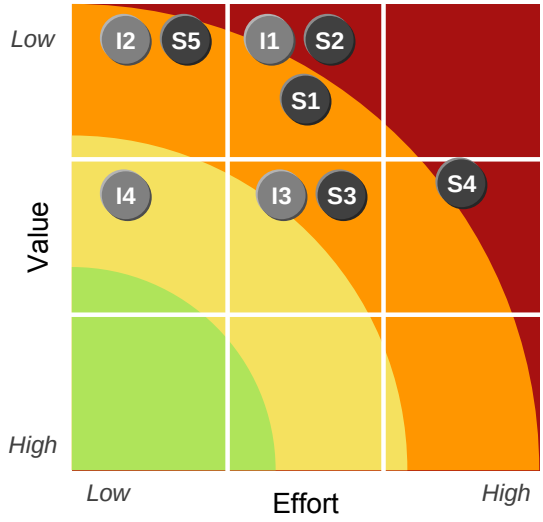

Figure 7 Assessment of value vs. effort for the identified additional services

6.0 Transformation Options

The previous chapters indicated the potential improvements and additional services for CCN. The chapters also assessed the expected value of those improvements and additional services as "low" to "medium". This chapter will look into options that have to potential to deliver "high" value, i.e. provide a means to transformational change.

6.1 Overview of Options

Figure 8 shows the different transformation options this study identified.

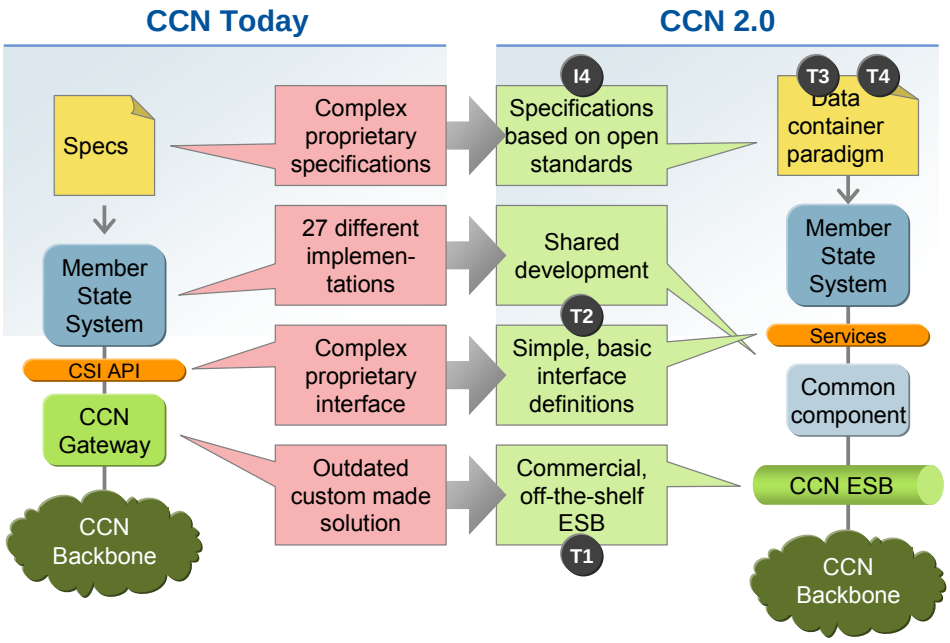

Figure 8 CCN Transformation Options

- **T1 – Commercial, off-the-shelf ESB**
  Today, the CCN Gateway is an outdated custom made solution. Maintenance is expensive, functional options are limited. One way to resolve this is to replace the custom made CCN gateways by a single commercial, off-the-shelf Enterprise Service Bus (ESB);
- **T2 – Common components**
  Today CCN Participants execute independent implementations of a CCN application specification. Sharing development by developing common logic only once will reduce development cost and also maintenance cost with a factor of 30+. Furthermore the implementations use a complex and proprietary interface to communicate over the CCN backbone. A common component can hide the communications complexity by providing a simple, basic interface (e.g. based on web services);
- **T3 – Data container paradigm**
  A second step is to bring the specifications to a higher abstraction level by using a paradigm we dubbed the "data container". Using this paradigm CCN Participants no longer exchange messages but create, read and update data containers when business events occur.
- **T4 – Unified storage**
  Today, there is a customs union, there is common data but the data is only shared

when needed. A unified database accessible by all CCN Participants would simplify the implementation of the data container paradigm dramatically.

The following sections will explain the options in detail.

6.2 Commercial, off-the-shelf ESB (T1)

Description

The CCN gateways are still running on the same IT platform as in 1999. Estimates by Gartner suggest that an IT platform — when defined as a major release — can rarely persist for a period of longer than seven years without a migration to a newer version. The outdated technology becomes even more apparent when we look at Figure 9. This figure shows the evolution of the functionality of the CCN gateway versus the functionality of COTS (commercial, off-the-shelf) ESB solutions. Over time ESB solutions have overtaken the functionality provided by the CCN gateways. This means that today COTS ESB solutions offer more functionality at a lower price than the CCN gateways. This includes the ESB solution currently in use by the European Commission: Oracle BEA WebLogic. Therefore, it is a valid option to investigate if there is a business case for the replacement of today's gateway by standard technology.

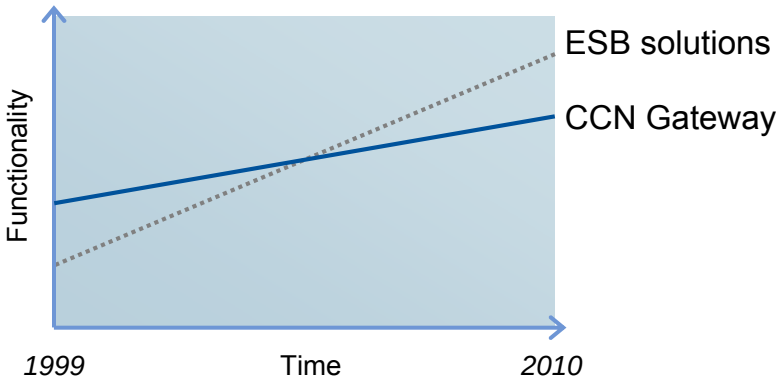

Figure 9 Evolution of functionality of the CCN Gateway and ESB solutions

Technology

An ESB is a middleware solution that enables interoperability among heterogeneous environments using a service-oriented model. An ESB allows a developer to build a service that is completely independent from the technology that will be used to expose its capabilities. Today the service can be exposed using web services; tomorrow, with a slight adjustment to the service's configuration, it can be exposed using a different protocol. Figure 10 illustrates the architecture of the next generation application server that enables the separation of application and infrastructure concerns.

The service agent running in the platform's agent container is completely separated from the technology used to expose its capabilities to the outside world. The message pipeline processor and policy enforcer can expose the service through any number of communication channels, supporting a wide assortment of client systems, including rich Internet applications (RIAs) and mashups, web services, JMS, remote service endpoints, and others. The pipeline processor also mediates access to the service agent by enforcing whatever policies apply to the service, such as security, reliability, or transformational policies.

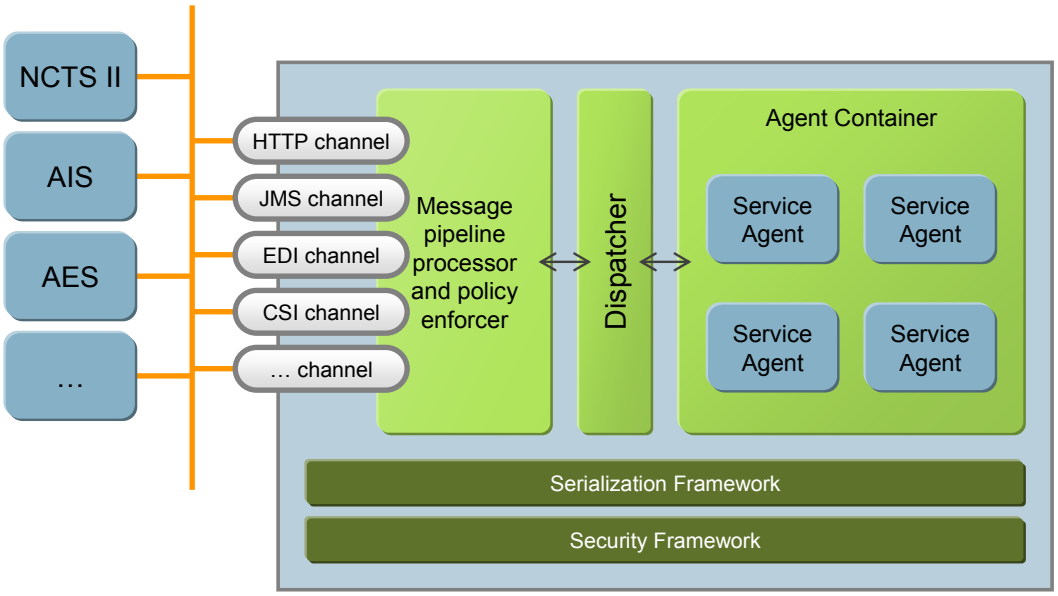

Figure 10 ESB as the Next-Generation Application Platform

ESBs often come with additional functionalities:

- *Resource adapters* – Many ESB vendors provide resource adapters that developers can use to implement connections to various legacy applications and data sources, and then expose these connections as services. Resource adapters are often sold separately;
- *Composition* – Many ESB products include tooling and frameworks that enable developers to wire services together to create a simple composite application;
- *Orchestration* – Some ESB products support the development of composite services using an orchestration model. An orchestrated service is a service that calls other services in a predefined execution pattern or workflow. An orchestration engine coordinates the execution of the pattern at runtime;
- *Reliable messaging* – Many ESB products support reliable message delivery semantics, including best effort, persistent queuing, at least once, at most once, exactly once, and ordered messaging;
- *Event processing* – Many ESB products support an event-driven interaction pattern via publish and subscribe capabilities;
- *Business Activity Monitoring* – EBSs provide built-in support for monitoring events on the network and providing management information generation;
- *Transactions* – Some ESB products support transactional integrity. The persistent queuing systems that enable reliable messaging and event processing typically operate as transactional data resources, and these queuing systems can participate in heterogeneous transactions. In addition, an ESB product may supply a distributed transaction manager that can coordinate a distributed transaction across heterogeneous data resources using a two-phase commit (2PC) protocol or compensating transactions;
- *Security mediation* – In a few rare cases, the ESB can mediate an interaction that crosses security domains by mapping credentials from one domain to credentials that are acceptable by the second domain. (All ESBs can control access to services through authentication, but only a few products support federation across security domains);

- *Tooling* – An ESB typically provides tooling for design, development, configuration, deployment, operation, and management of services. Tooling may be model-driven, graphical, or invoked using a batch command. Some ESBs come pre-populated with models and metadata related to specific commercial application or domain-specific models and schemas.

Adherence to Requirements

Table 15 demonstrates that an ESB adheres to the key high-level requirements.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	A specific "channel" can be implemented on top of the ESB to provide continued support for the CSI API
	Today's and tomorrow's applications are mission critical	ESBs provide functions to ensure messages arrive and do not get lost
	Proven technology	ESBs have reached the plateau of productivity a long time ago
Scalability	Volume will increase (40% YOY volume growth so far)	ESBs provide a scalable architecture that facilitates the addition of new applications and the growth of message volumes
Security	Refined access layers, also access for smaller local community offices	Security is an integral aspect of the functionality of an ESB. ESBs may even support federated identities

Table 15 COTS ESB adherence to the high-level requirements

Development/Sourcing

There are two options to migrate from today's CCN gateway infrastructure towards a COTS ESB: gateway first or gateway last.

- *Gateway first* – This scenario implies to first roll-out a modern ESB with a CSI adapter that mimics today's CCN gateway. New applications can immediately leverage the capabilities of a modern ESB. Maintenance of the existing CCN gateways is limited to the CCN gateway adapter and CSI APIs until the last CCN application has been replaced;
- *Gateway last* – In this scenario a "common component" (see next section) is developed first that encapsulates today's CCN gateway. Once all CCN applications have been upgraded to use the common component (instead of CSI) the CCN gateway is replaced with an ESB.

Gartner renders the "gateway last" scenario as non feasible. It takes too long before all CCN applications have been replaced. All new developments will have to be based on the outdated CCN gateway infrastructure. Maintenance of the existing CCN gateway infrastructure will have to continue for a long period.

The ESB roll-out and development of the CCN gateway adapter could be made part of the contract with the new CCN distributed data center operator.

Deployment/Maintenance

Today, the distributed CCN gateways run on standardized TAXUD provided hardware. Gartner identifies two possible routes to deploy the ESB:

- *Virtual machines* – Standardized virtual machines running on hardware provided by CCN Participants. The advantage of this route is that the CCN Participant can run his data center according to his standards. No alien hardware requires to be fitted in. The CCN Participant executes his own operational processes to ensure the availability of the virtual machines. TAXUD is given the control over the virtual machines to host the ESB and possible other components.
- *CCN Appliance* – This route takes the TAXUD provided hardware to the next level with the help of server provisioning and configuration management tools. The CCN appliance is a stand-alone, self-supporting hardware appliance that runs all the components, and that is centrally monitored and managed. This so called CCN appliance is for the CCN Participants like a black box.
  The appliance can be delivered to the CCN Participants' data centers as a 19" rack. All maintenance activities are TAXUD responsibility. Almost all maintenance activities (including back-ups) are executed remotely by the CCN distributed data center operator.

Dependencies

I1 (Improve Data Center Management) is a prerequisite to facilitate the maintenance of the ESB.

The ESB itself is a strong enabler for S2 (Business Activity Monitoring) and S4 (Federated Identity) as these functionalities come more or less out-of-the-box. Furthermore scenarios T2 and T3 can be better executed with an ESB in place as many of the required functionalities are readily available in an ESB.

Risks

Possible risks of the T1 option include:

- Gateway adapter appears to be too complex to be developed;
- Usage of ESB specific functionalities lead to another vendor lock-in.

Effort

Depending on the deployment concept the ESB should be made part of the contract of the CCN 2.0 distributed data center operator. This external service provider is responsible for designing, developing and deploying the CCN Participant provided virtual machines or CCN appliances on top of which the ESB (and other components) can run.

The ESB itself together with the CCN gateway emulator can be implemented within 1 year. The rerouting of the existing CCN applications towards the ESB CCN gateway emulator may take another 2 years. This means that after three years the existing CCN gateway infrastructure can be completely switched off.

Therefore, we assess the effort for T1 as **high**.

Value

For the CCN Participants a COTS ESB would mean the end of developing applications that rely on the proprietary CSI API. A COTS ESB would support a wide range of communication protocols. The CCN Participant can choose the most suitable protocol.

We assess the value of the ESB as follows:

- The overall maintenance of the CCN ecosystem will be reduced with less than 5%;

- Development cost of new CCN applications can be reduced with 10 to 30% as the ESB interface will be more standardized and straightforward than the CSI API;
- The speed-to-market of new CCN applications can be reduced with less than 1 year.

The overall value of the T1 scenario is therefore **low**. However, we need to keep in mind that T1 is an crucial enabler for S2, S4, T2 and T3. T1 is a necessary step to replace a 15 year old solution.

6.3 Common Components (T2)

Description

Today applications running on CCN share the specification. The specification is implemented by each CCN Participant separately. This is a highly inefficient situation. First of all, the same logic is implemented 30+ times. Ambiguities in the specification lead to different interpretations leading to unexpected errors in the message exchanges. The removal of these ambiguities consumes significant effort. And last but not least, the same logic needs to be maintained 27 times. Significant cost savings and speed-to-market gains are possible if the CCN Participants could somehow share the development of the core logic fulfilling the information exchange.

The idea is that TAXUD, in close collaboration with the CCN Participants, not only drafts the specification but also develops the common logic that implements the specification (i.e. shared development). With the current message oriented paradigm of the specification the common logic may include:

- message parsing;
- message validation;
- message workflow handling (i.e. orchestration).

The common logic will lead to a higher-level abstraction interface for the CCN Participant systems than the current CSI API easing the development of new CCN applications. The remaining burden of the CCN Participants is to implement an interface to their system that can be invoked from the common component and to implement the proper invocation of the interface of the common component when business events occur.

TAXUD already has experience with distributed common components. For example the MCC/ECN/ECN+ have been provided as common components to the CCN Participants. Table 16 shows three lessons learned that have been identified by stakeholders that should be taken into for CCN 2.0.

Lesson	CCN 2.0 Resolution
The functionality of the software was not easy to extend locally	Follow the open source software (OSS) paradigm that enables CCN Participants to tailor the code to their specific needs
The code was of poor quality	Ensure continued competition between external parties that develop parts for CCN
The solution was platform specific and therefore difficult to integrate into local infrastructure	Use a platform independent programming language

Table 16 Lessons learned of the MCC/ECN/ECN+ common component

Technology

The common component can be delivered in two parts:

- *CCN Service Agents* – As a generic service agent running on the T1 introduced ESB to simplify ESB communications. This can be regarded as a next generation CSI API. Elementary messaging operations and certain generic workflow functions could be provided by this component hiding ESB complexity and leveraging ESB functionality. This is TAXUD responsibility. Service Agents also enable other possibilities. T3 (section 6.4) provides an example;
- *OSS solution* – As a platform independent piece of open source software that further implements a CCN application specification. This piece of software can interface with existing CCN Participant systems with web services. Initial development and maintenance of the open source code base is TAXUD responsibility. Deployment and optional enhancement is CCN Participant responsibility.

By providing these two levels of common components, CCN Participants can choose at which level they want to connect: at the generic top ESB level (using CCN Service Agents) or at the level of business functions related to the CCN application specification at hand (OSS solution).

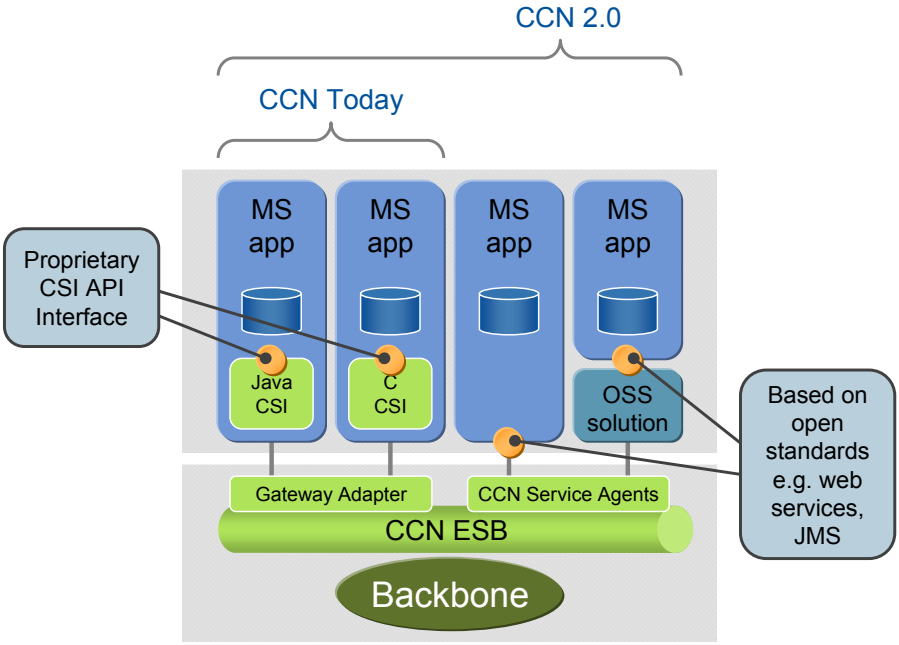

Figure 11 Position of the generic CCN API and OSS solution in the CCN infrastructure

Adherence to Requirements

Table 17 demonstrates that common components based on an ESB infrastructure adhere to the key high-level requirements.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	The common component runs in parallel to applications still using the existing CSI APIs
	Today's and tomorrow's applications are mission critical	Based on robust and proven ESB technology the common components can support mission critical applications
	Proven technology	ESBs have reached the Gartner "plateau of productivity" all ready for a long time
Scalability	Volume will increase (40% YOY volume growth so far)	ESBs provide a scalable architecture that facilitates the addition of new applications and the growth of message volumes
Security	Refined access layers, also access for smaller local community offices	Security is an integral aspect of the functionality of an ESB. ESBs may even support federated identities

Table 17 Common component based on ESB adherence to the high-level requirements

Development/Sourcing

It is obvious that delivering common components to CCN Participants is one step beyond what has been custom since the start of CCN. There will be a certain learning curve to accommodate the required shift in responsibilities.

From a TAXUD perspective it would be most logical to have the party responsible for developing the ESB also be made responsible for the CCN Service Agents. After the CCN gateway adapter for the new ESB has been delivered the CCN Service Agents for the new ESB can be developed.

The OSS solutions for specific CCN applications can be developed using CCN Participant resources where TAXUD acts as the choreographer or using an external service provider using a framework contract for development. If there is no interest from the CCN Participants in a common solution for a specific CCN application no OSS solution will be developed.

Deployment/Maintenance

The most practical way would be to deploy common components on top of the ESB at the site of every CCN Participant. The CCN appliance (introduced in the previous section) could provide an infrastructure to deploy and maintain common components with relative ease.

The maintenance of the CCN Service Agents could become part of the contract of one of the CCN maintenance providers (see section 7.4).

The OSGi framework could prove to be an open alternative to proprietary ESB deployment mechanisms. OSGi stands for Open Services Gateway initiative. This initiative aims to provide a common platform on which modularized Java applications can be deployed. The initiative stems from the set-top box industry looking for a vehicle to maintain the software running on the box. Today OSGi also applies to mobile phones, automotive appliances, PDAs, fleet management and last but not least application servers.

The maintenance of specific OSS solutions can be coordinated by TAXUD but executed at a local level depending on the specific CCN application at hand.

In order to ensure proper OSS development and maintenance a common set of guidelines and technology choices needs to be made.

Dependencies

An optimal implementation of the T2 scenario requires T1 (COTS ESB) to be in place.

The I3 (Common Testing Framework) improvement has a close relation with T2. The framework should be tightly integrated with the CCN Service Agents and also specify requirements for the OSS solutions in order to facilitate testing.

Risks

All CCN Participant systems functionally rely on the common component. Errors in the common component affect all CCN Participants.

Effort

The effort to develop the generic CCN API will take 9 to 18 months. The effort to develop a single OSS solution on top of the generic CCN API may take another two years. Therefore, the effort of T2 is considered as **high**.

Value

Common components will ease the live of CCN Participants as a large chunk of programming activity is shared with other participants. Furthermore, as CCN Participants start to share code, the reliability of the code will improve leading to less errors and incidents. T2 will enable the CCN Participants to focus more on the specifics of their local systems.

T2 will have the following impact:

- The total maintenance cost will decrease with more than 15% if common logic is only maintained once;
- The development cost of new CCN applications will decrease with more than 30% if common logic is only developed once;
- The speed-to-market is likely to come down to two years instead of four.

Therefore, the value of T2 is assessed as **high**.

6.4 Data Container Paradigm (T3)

Description

Today, CCN applications are specified using a *Message oriented paradigm*. However, instead of exchanging messages one could achieve the same result by publishing, updating, searching and fetching "data containers." A data container holds all data that is relevant to share between CCN Participants. Figure 12 shows the different sections of data elements that may constitute a data container.

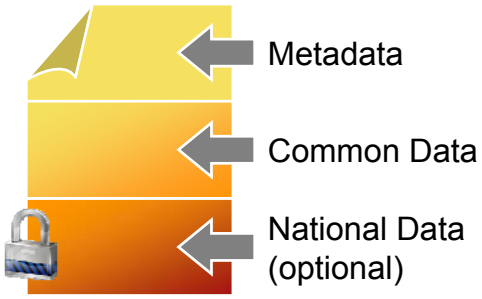

Figure 12 Sections that constitute a data container

A data container consists of three sections of elements:

- *Metadata* – shared, includes various identifiers of the document, status information, expiration date, security and access control information;
- *Common data* – shared between all concerned CCN Participants and institutions;
- *National data (optional)* – managed by single CCN Participant. Can include local processing information (officials involved, etc) and information for other national agencies (for single window implementation).

Data containers go beyond traditional Master Data Management that focuses on keeping non-transactional data in sync. Data containers hold the transactional data in a uniform and consistent manner across the CCN Participants.

Technology

Figure 13 shows a possible logical architecture of two layers of common components to implement the data container paradigm. The base layer is a universal implementation of the data container that provides the following services:

- *Create data container* – To create a new data container when a specific business event occurs;
- *Update data container* – To update an existing data container when a specific business event occurs;
- *Search data container* – To search for a specific data container based on a number of characteristics;
- *Retrieve data container* – To retrieve specific data elements of a specific data container.

On top of the universal data container component specific common components are developed for each CCN application. These common components provide a set of application tailored basic interfaces towards the CCN Participant systems.

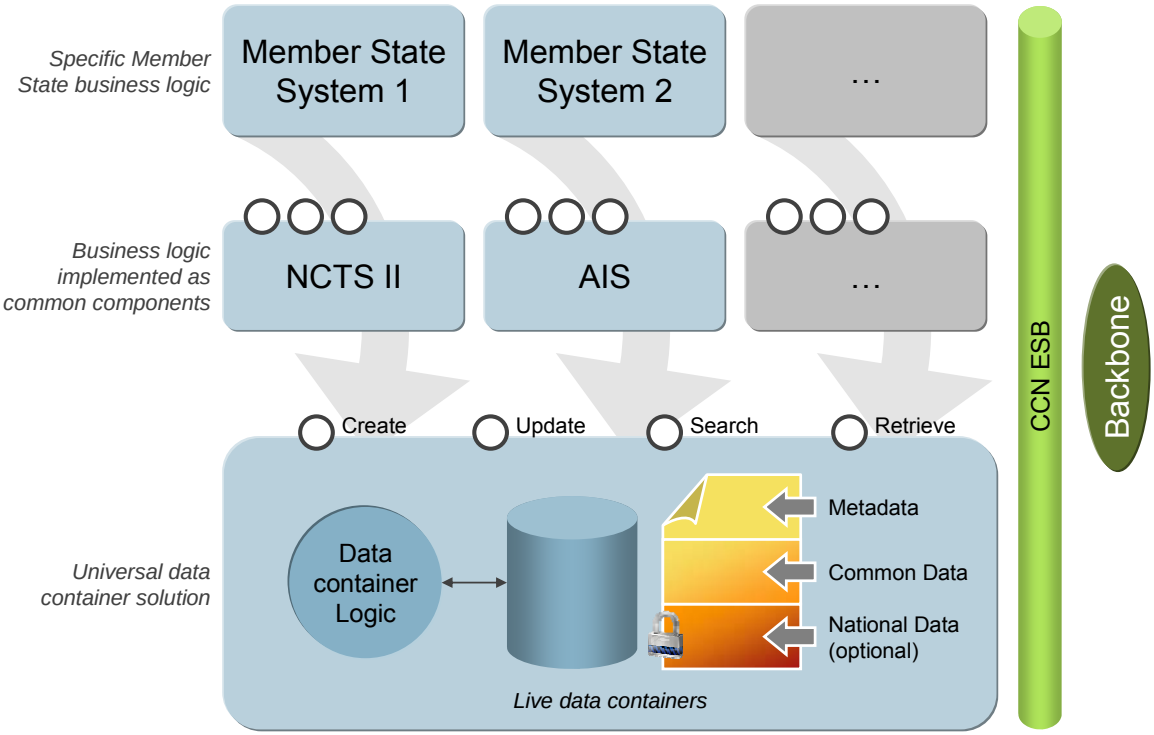

Figure 13 Logical architecture of the common component to implement the data container paradigm as deployed within one CCN Participant

Let's illustrate the architecture with a simple example: a truck passes an office of transit. There is a customs officer with an information system. After clearing the truck he will press a button in the user interface that will record the fact the truck has passed the particular customs office. Instead of invoking the primitives of the data container directly which would lead to complex CCN Participant applications the customs office information system invokes a specific method (e.g. "truckPassed(String customsOffice)") of the common component. All the handling of retrieving and storing the right data container is dealt with in this component and hidden from the CCN Participant information system. A common component for a specific CCN application will consist of lots of similar tiny functions.

Once created by a CCN Participant a data container stays within the universal data container component deployed in that CCN Participant. CCN Participants are free to store a copy of the data container in their local systems. They may even add specific information. However, the single source of truth is always the data container kept in the common component in the originating CCN Participant.

Information in a data container is never deleted. Information is only added. Furthermore, the metadata section of the data container provides information on who added and who accessed what data when.

A central index of data containers facilitates the search function. This index should not only include simple identifiers but also fingerprinting technologies to enable rapid search on different characteristics.

The data container can be implemented as a service agent running on the ESB. It is also possible to use existing distributed caching platforms (DCPs) but these have to be tailored to ensure data containers are kept within the originating CCN Participant.

Adherence to Requirements

Table 18 demonstrates that the data container paradigm adheres to the key high-level requirements.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	A data container enabling common component would run in parallel to applications still using the existing CSI APIs
	Today's and tomorrow's applications are mission critical	The data container paradigm requires real-time connectivity to other CCN Participants leading to a higher dependency on the availability of the infrastructure then the message oriented paradigm
	Proven technology	The paradigm can be implemented using conventional technology only
Scalability	Volume will increase (40% YOY volume growth so far)	A pilot should bring insight in how to achieve scalability. Scalable solutions along this paradigm already exist in distributed population administrations and electronic health records
Security	Refined access layers, also access for smaller local community offices	Metadata and encryption are the means to ensure only authorized access to data containers

Table 18 Data container paradigm adherence to the high-level requirements

Development/Sourcing

A data container enabling common component can be developed in two ways:

- As an effort by TAXUD leading to a common component owned, maintained and deployed by TAXUD as part of the CCN infrastructure;
- As a joint effort of TAXUD and the CCN Participants leading to an OSS solution which is coordinated by TAXUD but maintained and deployed by the CCN Participants.

The first option will lead to a more maintainable common component. The second option provides possibilities to CCN Participants to enhance the data container concept with local insights.

Deployment/Maintenance

The data container enabling common component and the specific CCN application common components are deployed in each CCN Participant separately. If TAXUD owns, maintains and deploys the data container the data container components can be deployed in the same way as the ESB leveraging the CCN appliance introduced with T1.

Dependencies

T3 requires T1 and I1 to be in place.

Risks

The data container paradigm is a shift from today's way of working. This may lead to misunderstandings and different expectations of how the concept should work in practice. This may influence the implementation of this paradigm in a negative way.

Effort

T3 can only be pursued after a successful pilot has been executed. Implementation of the data container enabled common component will take more than 18 months. Therefore, the effort is assessed as **high**.

Value

T3 has a similar positive impact on the CCN Participants as T2. T3 also holds the promise to make local system development even more easy as the complex message flows are a thing of the past.

The T3 scenario provides the following value:

- Maintenance cost will go gown with more than 15% because only one common component needs to be maintained that can implement service different CCN application specifications. CCN Participant systems become more simple as the interface to the common component is straightforward;
- Development cost of new applications will go down with more than 30% because a large chunk of the logic is already implemented in the common component;
- Speed-to-market can be brought back with more than two years because the effort to adopt the CCN Participant systems to the data container paradigm will be much simpler.

Therefore, the value of the T3 scenario is assessed as **high**.

6.5 Unified Storage (T4)

Description

The T3 data container paradigm creates a virtual pan-European database of transactions. Data containers are kept in the data container implementation at the CCN Participant where they are first created. The implementation of the data container paradigm could be much more simplified if a there were a unified storage mechanism where data containers are simply available and the exact location of the data containers is irrelevant. T4 envisions such a unified storage mechanism.

As with T3 common components could be developed for specific CCN applications to ease the usage of the unified storage mechanism. It is also possible for CCN Participants to access the unified storage primitives directly.

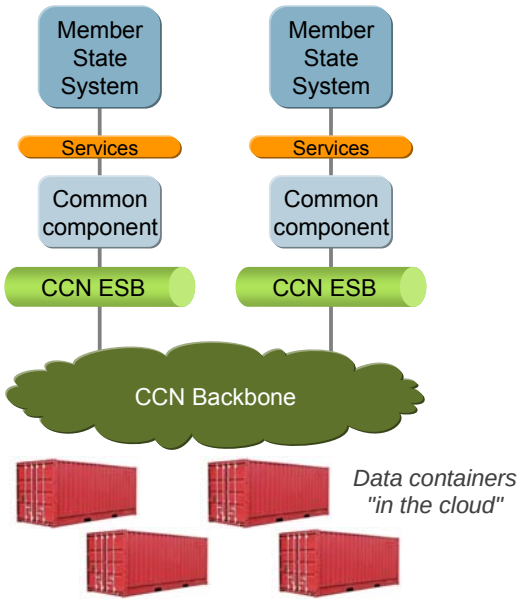

Figure 14 Unified storage provides a standard mechanism to access shared data

Technology

T4 can be implemented using the same technologies as T3. However, instead of storing data containers locally, data containers are stored "in the cloud", i.e. in a unified storage mechanism. This mechanism can be made available using the service agents running on the ESB. Here, it is eminent to leverage existing distributed caching platforms (DCPs). Also called "in-memory data grid," "data fabrics" or "information fabrics" by some vendors, DCPs are middleware products that provide an in-memory, distributed object store, called "cache" or "space," in which multiple, distributed applications can place, retrieve and exchange large volumes of data objects.

To prevent data loss in the event of a system crash and to optimize performance, DCPs enable the creation of a "distributed virtual space" — the union of the individual spaces managed by the multiple DCPs deployed across multiple networked servers (whether on-premises or in the cloud). The content of a given space can be partially or totally replicated across clustered spaces through flexible, asynchronous, high-performance and transactional (to preserve data consistency and integrity) replication mechanisms.

Applications manipulate data objects in the cache via specific or generic APIs (for example, JPA, JavaSpaces, Java Database Connectivity and Java Message Service), but some products can plug transparently beneath an application through declarative properties. The DCP runtime is responsible for initially loading the cache, synchronizing the cache state with original data sources, locking cache data objects, managing transactions and emitting cache event notifications. DCPs provide clustering and failover management, as well as cache partitioning, security and management features. These products also enable object sharing across multiple platforms (for example, Java EE and .NET) through the distributed cache and are therefore, at times used also as low-latency, very fast "publish and subscribe" engines. Vendors such as Alachisoft, GemStone Systems, GigaSpaces, IBM, Oracle and ScaleOut Software have proven commercial products in this space. Gear6, Terracotta and JBoss offer open-source distributed caching technology.

Adherence to Requirements

Table 19 shows how unified storage adheres to the key high-level requirements.

Requirement	Criteria	Adherence
Continuity	Continued support for CCN/CSI interface	Unified storage would run in parallel to applications still using the existing CSI APIs
	Today's and tomorrow's applications are mission critical	The unified storage mechanism depends on real-time connectivity leading to a higher dependency on the availability of the infrastructure
	Proven technology	Distributed caching platforms are becoming more and more mature.
Scalability	Volume will increase (40% YOY volume growth so far)	Distributed caching platforms provide highly scalable solutions
Security	Refined access layers, also access for smaller local community offices	Metadata and encryption are the means to ensure only authorized access to data containers

Table 19 Unified storage adherence to the high-level requirements

Development/Sourcing

The development of the unified storage mechanism can be best realized using a pilot approach where two or three DCP vendors are requested to demonstrate their skills. The competitive dialog procedure of the European tendering regulation supports this approach.

Deployment/Maintenance

Once the mechanism is implemented on top of the ESB the CCN distributed data center operator could be made responsible for maintaining the solution. Of course unified storage would imply more responsibilities for TAXUD in ensuring the availability of data containers. This will have an impact on the governance, organization and financing of CCN.

Dependencies

T4 depends on T1 and I1.

Risks

There may be legal issues that do not allow CCN Participants to store their data beyond the physical borders of their territory. Another risk is the dependency on real-time connectivity to the unified storage mechanism.

Effort

The implementation of the unified storage mechanism itself probably will take more than 18 months and cost more than 5 million euro. Therefore, Gartner assesses the effort as **high**.

Value

The value of T4 is comparable with T3. However, as T4 can be fully based on a COTS distributed caching platform the savings on maintenance cost can be even higher than T3's. Therefore, Gartner assesses the value of T4 as **high**.

6.6 Conclusions

Option	Effort	Value	Maintenance	Development	Speed2M
T1 - COTS ESB	High	Low	Low	Medium	Low
T2 - Common components	High	High	High	High	Medium
T3 - Data container	High	High	High	High	High
T4 - Unified storage	High	High	High	High	High

Table 20 Assessment of the identified transformational options

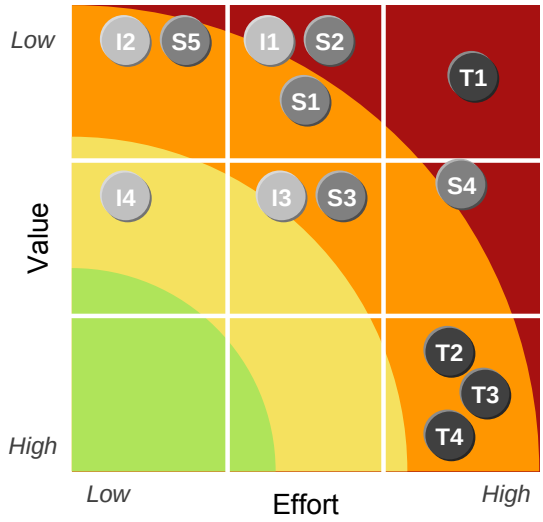

Figure 15 Assessment of value vs. effort for the identified transformation options

7.0 Roadmap and Sourcing

Now that we have discussed and assessed the different options to evolve from CCN 1.0 toward CCN 2.0, this chapter puts things in perspective. First, the roadmap and work packages are introduced that are needed to evolve. Then, the impact of today's IT industry on good IT stewardship is presented. This results in the need of strong vendor management. The key aspects of vendor management are presented in the following section. Finally, this chapter concludes with an overview of the lots for the CCN 2.0 tender.

Hence, this chapter discusses the CCN 2.0 roadmap and sourcing aspects in general. The activities needed to execute Iteration 2 of this study are presented in Appendix C.0.

7.1 Roadmap and Work Packages

When we examine the resulting assessment for the improvements, additional services and transformation options as depicted in Figure 15 it becomes obvious that there is no low hanging fruit. The road towards CCN 2.0 will be a tough road. The transformation options that deliver high value require a high effort. Furthermore, they require an initial investment in other options that provide less value at first.

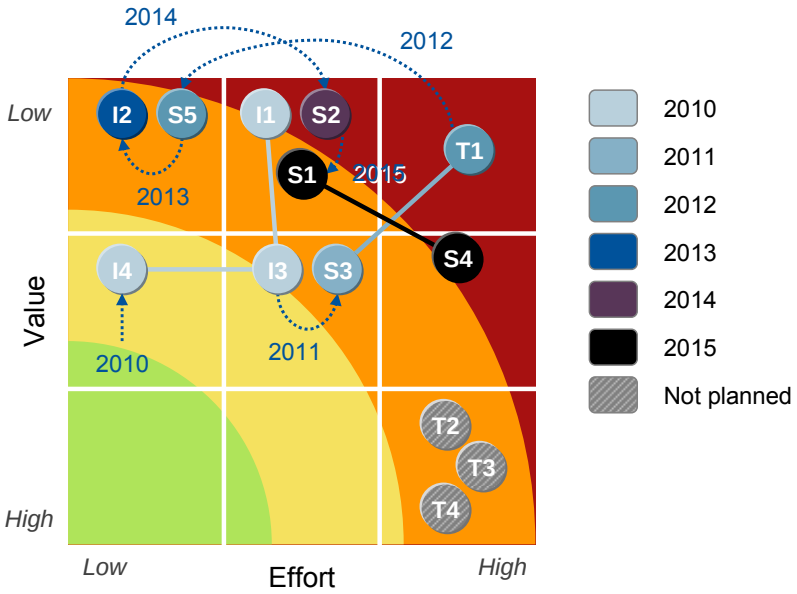

Figure 16 Tentative Roadmap of options – hence, the European tendering procedure and pilot project are not depicted in this diagram

The work packages for the evolution towards CCN 2.0 look like:

- *Data center operations (I1)* – Improve the current data center operations by implementing available best practices and COTS solutions;
- *Establish Common Testing framework (I3)* – Improve the existing test solution to ease testing of CCN applications for the CCN Participants;
- *Implement Master data management (S3)* – Implement MDM technology to synchronize non-transactional data across CCN Participants;
- *Tender new CCN 2.0 contract* – Start the European tendering procedure to acquire service providers for the network, data center operations, maintenance and development activities needed to evolve towards CCN 2.0;

- *COTS ESB & Gateway adapter development (T1)* – Design, develop en deploy the CCN appliance while at the same time design, develop the ESB and CCN gateway emulator. This is the most critical work package and is most likely to last more than 3 years;
- *Use Internet as fail-over and non-mission critical traffic (I2)* – Implement Internet connectivity next to the MPLS cloud;
- *Business Activity Monitoring (S2)* – Leverage built-in ESB functionality by deploying business activity monitoring;
- *Develop Infra services (S1)* – Leverage the CCN appliance by providing Infra services;
- *Pilot on specification paradigm (determine T2 or T3)* – The viability of the data container paradigm needs to be proven in a pilot;
- *Federated identity (S4)* – Implement federated identity functionality.

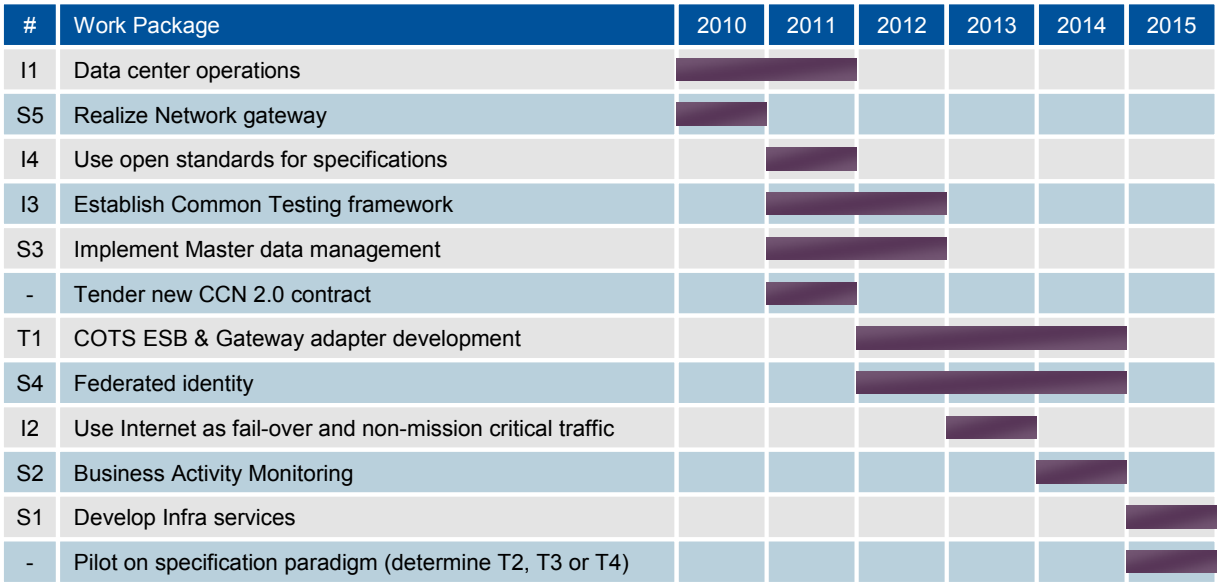

Figure 17 Tentative Gantt chart for the CCN 2.0 evolution

7.2 Good IT Stewardship

In this section we will explain why vendor lock-in will continue to occur why it is important to have strategic relationships with the key service providers. CCN products and services cannot be acquired fully independently. Although open standards (see footnote 4) that would

4) Although a formal definition of an "open standard" does not exist, it is generally understood that a standard is to be considered "open" when it complies with the following criteria: There are no constraints on the re-use of the standard. The standard has been published and the specification is publicly available. The standard is adopted and maintained by a not-for-profit organization. The development of the standard occurs on the basis of an open decision-making procedure available to all interested parties. The intellectual property of the standard is irrevocably made available on a royalty-free basis.

It is important to realize there are quite a number of standards that belong to a "gray" area, i.e. they comply with a limited number of criteria. E.g. Adobe PDF is a semi-open standard. It only complies with the first two criteria. The more criteria a standard complies with, the less vendor-dependent it becomes.

allow the mix-and-match of IT products from different vendors are emerging this is still a far cry from today's practice where optimally functional product stacks are made-up of products of a single vendor. Trying to combine products of different vendors, for the sake of avoiding lock-in to one specific stack, might lead to integration challenges hampering IT stewardship objectives to provide reliable, continuous and cost-effective IT services. Also, vendors continue to offer products that feature significant richer functionality when combined with other products following their own proprietary standards (see footnote 5).

Good IT stewardship implies that TAXUD carefully selects an IT platform (see footnote 6) to fit within the existing portfolio. In order to adhere to the reliability, continuity and cost-effectiveness principle TAXUD should limit the number of platforms to support to the minimal amount necessary. For the same reasons also the amount of platform switches should be kept to a minimum.

Once a platform has been chosen stewardship implies that TAXUD can only change the platform if one of the following fundamental reasons occurs:

- The platform has become out of date or is not supported anymore;
- A fundamental paradigm shift occurs with the IT ecosystem;
- The requirements of the users are no longer met or the new platforms offer so many new features as to have an important positive impact on the 'users' (user might be a developer, a system administrator, etc);
- The TCO, including migration costs, is no longer reasonable or competitive.

In other words, good IT stewardship imposes to enter a long term strategic marriage with the vendors that offer the platforms that cover the IT product stack best. This, of course, may conflict with some of the objectives of the public procurement directive, namely the promotion of market access and competition.

One could compare the situation with that of a child that started to build a crane using Lego Technic and because his parents did not take the strategic relation with Lego into account is now forced to finish his crane using K'Nex. This will not work and the child ends up frustrated, or worse.

7.3 Vendor Management

In practically every government agency in the world, the cost trend is to replace staff costs with supplier costs. This trend is observably strong in the IT function, where IT outsourcing transfers significant cost from staff to suppliers. The prevailing management culture in many organizations suggests that "real" management is about managing teams of people — and the larger the team, the "bigger" the manager. The fundamental transition that is required is to move management culture from managing people to **managing outcomes**. As more of the cost base moves to suppliers it will become obvious — vendor management is far too important to be left to the procurement team. It will be what management does.

21st century management is about the management of outcomes. However, the allocation of management overhead in an organization remains disproportionately biased toward managing internal costs. So, a team of six Java programmers will have a full-time manager, but a supplier that costs 20 times the cost of the six programmers will have practically no dedicated management resources. This is illogical, irrational and just plain wrong. The allocation of management resource needs to be more balanced with regard to budget and desired outcomes. The skills of 21st century management are related to how well a manager

5) A "proprietary standard" is a standard that is not open, i.e. vendor specific.

6) An IT platform is defined as a group of tightly integrated IT products.

can deliver outcomes using a budget. Many outcomes will critically depend on third-party organizations, so a lot more management time is going to have to be devoted to driving value from external spending.

Vendor management especially applies for services that deliver high value and come with a high switching cost (see previous section). The CCN "service" typically requires vendor management.

Supplier management versus vendor management

The challenge for an enterprise management team is to define precisely what constitutes "sufficient" management of suppliers to optimize value. Ignoring all suppliers is clearly "insufficient" management and would lead to sub-optimal value. Over-investing in managing all suppliers simply increases management overhead without necessarily increasing the value delivered.

Therefore, it is necessary to have a portfolio of techniques for managing suppliers: Vendor management is only one component of this portfolio. However, irrespective of where a supplier fits into the portfolio of management options, certain aspects of supplier management remain constant. At the very least, the purchase ledger needs to be accurately maintained with up-to-date supplier name and address details. Every supplier should be part of a vendor appraisal program. Mechanisms should exist to measure the performance of all suppliers, but these measures should be appropriate to the value and risk associated with the services delivered.

Although all suppliers need some basic supplier management services, vendor management should only be used for suppliers where there is high value to the business and where the nature of the relationship makes changing suppliers an expensive and disruptive option as with CCN. All suppliers need supplier management — only a small number of suppliers need vendor management.

Knowledge management

Vendor management is not achieved through the creation of a bureaucracy. Although there will be some processes involved, vendor management is not really a process-driven discipline; it is a knowledge discipline. Process-driven activities can usually be distributed throughout an organization, with many roles participating in individual process steps, with the integrity of the process creating the desired result. By contrast, knowledge-driven activities need individual ownership. The tacit knowledge of the individual, which is constantly updated and filtered, enables a knowledge-driven activity to be optimized.

However, it is important that the knowledge — about the relationship, the services delivered, the strategy, the people, the contracts, the commercial arrangements and numerous other information points — should be documented in a consistent manner. It should be a goal of the initial pilot activities in vendor management to define the various components of the information repositories that will act as a permanent record of the relationship. For example, although "the contract" is a pivotal document, it is practically meaningless without the additional context and interpretation created by the side letters, e-mails and meeting minutes that are exchanged between the two parties.

The vendor manager

The most effective way to start introducing vendor management is to select one specific relationship that needs transformation, and then to find the right individual manager to transform it. This individual will need to be given strong support, sponsorship and mentoring,

with unfettered access to all of the key CCN stakeholders. The lessons learned by this individual may be used to shape a larger program.

In many respects, vendor management must be, first of all, an internal-facing role to be effective as an outward-facing role. The vendor manager is at the hub of a virtual team, consisting of all of the stakeholders in the relationship. Developing and servicing this virtual team is not an ancillary activity for a vendor manager — it is a critical, core function.

It is vital that the vendor manager has a clear understanding of the position of the supplier in all the markets in which the supplier participates — not just in the specific CCN domain of the goods or services that TAXUD acquires from the supplier. The broader understanding is needed to form judgements about the propensity of the supplier to invest or disinvest in the areas of activity that are important to TAXUD.

A "natural" vendor manager — someone with a background in sales and an understanding of the dynamics of relationship developments — will know how to identify the possibilities and will gently nudge the supplier toward making a desirable decision.

7.4 New CCN 2.0 Framework Contract

A new CCN 2.0 contract may consist of the following lots:

- *CCN Network operator* – 1 provider to cater for a MPLS-based backbone and optional Internet connectivity;
- *CCN Distributed data center operator* – 1 provider provide standardized platforms, responsible for daily operation of the entire network. ITIL, provisioning, et cetera. This provider typically delivers and maintains the CCN appliance and the ESB;
- *Component development* – 3 providers, new developments require a mini competition;
- *Component maintenance* – 3 providers, newly developed components that are transferred to maintenance require a mini competition.

The separation between maintenance and development ensures that code is well documented and not vendor dependent. Furthermore, maintenance and development are different types of processes that require different skills.

Gartner defines maintenance as:

- Bug fixes of any size or duration;
- Maintenance of hard-coded data or tables (including field size changes) embedded within the programs (any size or duration);
- Functional enhancements to current code that take less than two person-weeks and typically add fewer than eight function points;
- Any project that produces no new functionality for the user;
- Large refactoring exercises are not included in maintenance.

Development is defined as adding new functionality or features to existing applications outside the maintenance area.

For development and maintenance Gartner strongly advises not to engage in cascading contracts but to use framework contracts with a maximum of 3 providers to ensure committed providers.

Vendor management typically applies to the CCN Network operator and the CCN Distributed data center operator.

8.0 Conclusions and Recommendations

For the evolutionary roadmap towards CCN 2.0 the study revealed the following categories of options:

- *Improvements* – These improve the current functionality of CCN;
- *Additional Services* – These add new functionalities to CCN;
- *Transformation Options* – These options provide transformational change to CCN.

Improvements

Improvement 1, better data center management, uses a mature process framework for operational and maintenance processes, as well as leveraging proven tools to support these processes, resulting in increased flexibility and lower costs.

Improvement 2, leveraging the Internet for connectivity and fail-over, uses the ubiquity and low costs of the Internet to complement the present private (and expense) WAN for non-mission critical traffic.

Improvement 3, the implementation of a common testing framework, uses modern test automation and management tools to provide a virtualized, consistent testing environment to Participants.

Improvement 4, the usage of open standards to make specifications, will lead to easier to maintain and understand specifications that can be reused by CCN Participants and may even be used for application generation.

These improvements bring some value to the Participants, however the benefits are limited. Only the testing framework provides medium value, albeit at medium realization costs as well.

Improvement	Effort	Value	Maintenance	Development	Speed2M
I1 - Data center	Medium	Low	Low	Low	Low
I2 - Internet	Low	Low	Low	Low	Low
I3 - Testing	Medium	Medium	Low	High	Low
I4 - Open Specs	Low	Medium	Low	Medium	Medium

Table 21 Assessment of the identified improvements

Additional Services

Additional service 1, common infrastructure services, explores the option of combining infrastructure demands of several Participants into a single data center, enabling Participants to enjoy economies of scale and high quality operational processes.

Additional service 2, business activity monitoring, proposes a centrally managed monitoring environment that aims to provide real time information about the status and results of various operations, processes, and transactions. For example to alert customs if a truck passes the German border just 20 minutes after loading goods in Antwerp.

Additional service 3, master data management, addresses the present situation where common data is currently sometimes duplicated, sometimes replicated, but not managed actively. Off-the-shelf MDM tooling is used to define a single source of the truth and enable sharing of high quality, consistent data.

Additional service 4, federated identity, aims to standardize and enable the sharing of user identities across the network, enabling distributed applications to reuse existing authentication mechanisms of the various Participants.

Additional service 5, the central Internet gateway, proposes a centrally managed gateway between CCN and the Internet. It can be realized either in a basic router/firewall mode, or as a more advanced message transformation platform.

The additional services provide interesting and beneficial new functionality to the Participants. However, there are no quick wins, as realization efforts are generally significant, and the added value of the services remains limited.

Additional service	Effort	Value	Maintenance	Development	Speed2M
S1 - Infra services	Medium	Low	Medium	Low	Low
S2 - Activity mon.	Medium	Low	Low	Low	Low
S3 - Master data	Medium	Medium	Medium	Medium	Low
S4 - Federated id.	High	Medium	Medium	Medium	Low
S5 - Internet gatew.	Low	Low	Low	Low	Low

Table 22 Assessment of the identified additional services

Transformation Options

Transformation 1, off-the-shelf ESB, proposes to replace the present, custom and outdated CCN middleware with a commercial, off-the-shelf Enterprise Service Bus, which can be deployed as a complete appliance in the data centers of the Participants. The ESB itself is a strong enabler for S2 (Business Activity Monitoring) and S4 (Federated Identity) as these functionalities come more or less out-of-the-box. Furthermore scenarios T2 and T3 can be better executed with an ESB in place as many of the required functionalities are readily available in an ESB.

Transformation 2, common components, introduces the notion of commonly developed components, where CCN Participants share the burden of implementing common logic, reducing development cost and also maintenance cost with a factor of 27. A common component can also hide the communications complexity by providing a simple, basic interface (e.g. based on web services).

Transformation 3, data containers, addresses the present dependency on a complex proprietary specification based on message exchange. The use of open standards such as BPMN and XML Schema are a first step to more openness. A second step is to bring the specifications to a higher abstraction level by using a paradigm we dubbed the "data container". Using this paradigm CCN Participants no longer exchange messages but create, read and update data containers when business events occur.

Transformation 4, unified storage, takes the data container paradigm and brings the virtual pan-European database into a unified storage mechanism. On top of this unified storage workflow management can implement common operational processes.

The transformation options are the true high-value steps toward CCN 2.0. However, the realization effort of all three options is high. In addition, the low-value ESB is a prerequisite for the high-value options T2 and T3, requiring significant investments before the true value of CCN 2.0 can be delivered to the Participants.

Option	Effort	Value	Maintenance	Development	Speed2M
T1 - COTS ESB	High	Low	Low	Medium	Low
T2 - Common components	High	High	High	High	Medium
T3 - Data container	High	High	High	High	High
T4 - Unified storage	High	High	High	High	High

Table 23 Assessment of the identified transformational options

Roadmap

When we examine the resulting assessment for the improvements, additional services and transformation options it becomes obvious that there is no low hanging fruit. The road towards CCN 2.0 will be a tough road. The transformation options that deliver high value require a high effort. Furthermore, they require an initial investment in other options that provide less value at first. Gartner identified a list of work packages that will take six years of execution before TAXUD can start implementing the transformation options that lead to high value.

It is important to realize that vendor lock-in will continue to occur. This is especially the case for the data center operations and the necessary ESB infrastructure. In these areas Gartner recommends TAXUD to invest in vendor management. Vendor management is the management discipline that focuses on managing outcomes instead of people.

The new framework contract for CCN may consist of four lots: one for the operator, one for the distributed data center operator, one for component development and one for component maintenance. Separation between development and maintenance will lead to less vendor dependency. Engaging in "mini competitions" between the vendors in the development and maintenance lots ensures vendors stay committed offering high quality at low prices.

Appendices

A.0 References

A.1 Workshops

02-12-2009	Vision workshop	To discuss trends and technologies
19-12-2010	Second vision workshop	To translate trends and technologies to CCN
09-02-2010	Architecture workshop	To discuss improvements, additional services and transformation options
10-03-2010	Roadmap workshop	To discuss migration and sourcing options

A.2 Interviews

For this study Gartner interviewed the following persons.

26-10-2009 Mr. Jean-Michel Grave, Head of Unit C2, TAXUD

11-11-2009 Mr. Karel de Vriendt, Head of Unit IDABC, DIGIT

11-11-2009 Mr. Deasy Declan, Director Directorate B, DIGIT

11-11-2009 Mr. Theodoros Vassiliadis, Head of Unit A4, TAXUD

12-11-2009 Mr. Marinus de Graaff, Director Directorate A, TAXUD

12-11-2009 Mr. Paul Hervé Theunissen, Head of Unit A3, TAXUD

12-11-2009 Mrs. Maria Manuela Cabral, Head of Unit C1, TAXUD

18-11-2009 Mr. Guido de Jaegher, CCN SME, Unit A4, TAXUD

18-11-2009 Mr. Donato Raponi, Head of Unit D4, Mr. O'Drisoll, SME D4, TAXUD

21-12-2009 Mr. Hervé de Halleux, Mr. Bennet Heirwegh, Atos Origin

B.0 MS Questionnaire

The objective of this questionnaire is to discover what the key issues and priorities for the CCN Participants are and to get feedback on the proposed evolution for CCN 2.0. Your response is much appreciated and very valuable.

Your situation

1. What systems and platforms (relevant/connected to CCN/CSI) do you currently have?
2. How are your applications are currently integrated with CCN/CSI from a technical architecture perspective?
3. What are your top architectural challenges?
4. Do you have plans for major implementations/changes in the coming years?

Today's issues with CCN

5. Please indicate the severity of these issues as experienced by you on a scale from low (1) to high (5).

	1	2	3	4	5
Complex proprietary specifications					
30+ different implementations					
Complex proprietary interface (CSI)					
Outdated custom made middleware solution (CCN)					

6. Are there any other important issues that you would like to have addressed?

Requirements for CCN 2.0

7. Please indicate how relevant and important these requirements are for you on a scale from low (1) to high (5).

	1	2	3	4	5
Do more with less					
Continuity – ensure that current operations continue to be up-and-running					
Scalability – ensure that the volumes can grow					
Agility – ensure that choices facilitate innovation and avoid lock-in					
Security – ensure availability, data integrity and confidentiality					

8. Are there any other important requirements that you would like to have met?

Assessment of CCN evolution options

9. Please indicate your expected realization effort and beneficial value for you on a scale from low (1) to high (5).

	Effort						Value				
	1	2	3	4	5		1	2	3	4	5
Improve Data Center Management (I1)											
Leverage Internet for Connectivity and Fail-Over (I2) [a]											
Implement Common Testing Framework (I3) [b]											
Common Infrastructure services (S1)											
Business Activity Monitoring (S2) [c]											
Master Data Management (S3)											
Federated Identity (S4)											
Central Internet Gateway (S5)											
Custom-off-the-shelve ESB (T1)											
Common components (T2)											
Data Container Paradigm (T3)											

   a. What is your opinion on routing non-critical CCN traffic over the Internet (appropriately secured)?

   b. What areas of testing would you see fit for automation?

   c. What is your opinion on allowing a central business activity monitoring tool to (partly) analyze CCN messages?

10. Would you suggest alternative or additional evolution options?

11. Do you have any other comments with regard to the proposed evolution options?

Migration roadmap to CCN 2.0

12. Do you have any comments on the time scale? Could some (or all) tasks be realized more quickly? Or is more time needed? Why?

13. Would the proposed approach be successful or not? Why?

14. What do you regard as being the critical success factors for the migration?

Closing

15. Do you have any other comments or suggestions?

C.0 Plan for Iteration 2

This appendix holds the plan for the execution of Iteration 2. We present a tentative objective, tasks and planning.

C.1 Objective

The objective for Iteration 2 is twofold:

- Refine the Program Plan to evolve towards CCN 2.0
- Build consensus among the stakeholders on the CCN 2.0 evolution plan

C.2 Tasks

Derived from the objectives there are two work streams in Iteration 2: (A) Refine Program Plan and (B) Build Consensus

Refine Program Plan

The implementation of CCN 2.0 is not a single project. It will be a complex schema of different projects running in parallel that must be coordinated to realize the CCN 2.0 vision. Gartner suggests to use a best practice approach to coordinate the effort. In this appendix we take the methodology "Managing Successful Programs" (MSP) of the UK Office of Government Commerce (OGC) as the foundation. MSP provides guidance on how to establish and organize a program.

The content of this report is a starting point for the definition of the program plan. Taking MSP as a base the following tasks should be executed to draft the program plan. MSP terminology is written in *italics*.

- Task A.1 – Refine *Vision Statement* (section 3.2) – Brief future state description compelling to heart and mind
- Task A.2 – Refine *Blueprint* (the "description" and "technology" sections of I1-3, S1-5, T1-3) – Current state, future state and gap analysis
- Task A.3 – Define *Stakeholder Profiles*
- Task A.4 – Refine *Project Dossier* (the "development/sourcing" and "effort" sections of I1-3, S1-5, T1-3) – Overview of all projects and their interdependencies
- Task A.5 – Refine *Benefit Profiles* (the "value" sections of I1-3, S1-5, T1-3) – Detailed description of each benefit
- Task A.6 – Define *Benefit Realization Plan* – Schedule when benefits are expected to be realized
- Task A.7 – Refine *Program Plan* (chapter 8.0) – Schedule of the entire program
- Task A.8 – Define the program organization and governance – Who is responsible for what? How are decisions made?
- Task A.9 – Refine *Risk Log* (the "risks" sections of I1-3, S1-5, T1-3) – Potential risks: probability, impact and proximity
- Task A.10 – Refine *Business Case* (the "effort" and "value" sections of I1-3, S1-5, T1-3) – Rationale behind the program

Build Consensus

Building consensus is about informing and understanding the various stakeholders. Task A.3 provides the foundation to execute this work stream.

- Task B.1 – Distribute this report among the stakeholders
- Task B.2 – Refine questionnaire (appendix B.0)
- Task B.3 – Send-out questionnaire to stakeholders
- Task B.4 – Consult Member States by organizing Member State visits to different types of Member States (8 visits in total)
- Task B.5 – Process questionnaire and Member States visit results in all relevant parts of the program plan
- Task B.6 – Organize Member State meeting to present and discuss the CCN 2.0 Evolution Program Plan

C.3 Planning

#	Task	Jul	Aug	Sep	Oct	Nov	Dec
A.1	Refine Vision Statement						
A.2	Refine Blueprint						
A.3	Define Stakeholder Profiles						
A.4	Refine Project Dossier						
A.5	Refine Benefit Profiles						
A.6	Define Benefit Realization Plan						
A.7	Define Program Plan						
A.8	Set-up Program Organization and Governance						
A.9	Refine Risk Log						
A.10	Refine Business Case						
B.1	Distribute Report						
B.2	Refine Questionnaire						

Figure 18 Tentative Gantt chart for Iteration 2 (in months in 2010)

Any questions regarding this report should be addressed to:

Gilles Pellegry
Gartner, Inc.
Telephone: +32 49 953 4683
E mail: gilles.pellegry@gartner.com

TAXUD Contact Information

Theodoros Vassiliadis
Telephone: +32 2 296 1739
E mail: theodoros.vassiliadis@ec.europa.eu