NIMBLE Validation

D4.5

NIMBLE Platform Evolvement – Recommendations, Requirements and Roadmap

Project Acronym	NIMBLE
Project Title	Collaboration Network for Industry, Manufacturing, Business and Logistics in Europe
Project Number	723810
Work Package	WP4 Use Case Experimentation, First-Round Validation and Evolution
Lead Beneficiary	LTU
Editors	Diana Chronéer Jeaneth Johansson Michael Nilsson Mari Runardotter
Reviewers	Wernher Behrendt, Violeta Damjanovic-Behrendt Eva Coscia
Contributors	DC, JJ, MN, MR, BM, SW, WB, VDB, SG
Dissemination Level	PU

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 723810

Contractual Delivery Date	30/06/2018
Actual Delivery Date	06/07/2018
Version	V1.0

Abstract

The NIMBLE project aims to perform research leading to the development of a cloud and IoT federated platform specifically targeted to supply chain relationships and logistics. Core capabilities will enable firms to register, publish machine-readable catalogues for products and services, search for suitable supply chain partners, negotiate contracts and supply logistics, and develop private and secure information exchange channels between firms, in a B2B only environment. The intention is to support a federation of such NIMBLE instances, all providing a set of core services, and each potentially specifically tailored to a different aspect (regional, sectorial, topical, etc.).

The main goal of this document is, based on the lessons learned from the first round validation of the NIMBLE Platform, to present an elaborated way forward to capture the second round of validation regarding platform functionality and end-user experience (UX). As such, this deliverable presents lessons learned together with recommendations, the current agile work process, and finally the top-level requirements, that is, the complete scope of the requirements that a commercial platform based on NIMBLE technology should fulfil.

NIMBLE in a Nutshell

NIMBLE is the collaboration Network for Industry, Manufacturing, Business and Logistics in Europe. It will develop the infrastructure for a cloud-based, Industry 4.0, Internet-of-Things-enabled B2B platform on which European manufacturing firms can register, publish machine-readable catalogues for products and services, search for suitable supply chain partners, negotiate contracts and supply logistics. Participating companies can establish private and secure B2B and M2M information exchange channels to optimise business workflows. The infrastructure is being developed as open source software under an Apache-type, permissive license. The governance model is a federation of platforms for multi-sided trade, with mandatory interoperation functions and optional added-value business functions that can be provided by third parties. This will foster the growth of a net-centric business ecosystem for sustainable innovation and fair competition as envisaged by the Digital Agenda 2020. Prospective NIMBLE providers can take the open source infrastructure and bundle it with sectorial, regional or functional added value services and launch a new platform in the federation. The project started in October 2016 and will last for 36 months.

Copyright Notice

Neither the European Commission, nor any person acting on behalf of the Commission, is responsible for any use that might be made of the information in this document.

The views expressed in this document are those of the authors and do not necessarily reflect the policies of the European Commission.

Document History

Version	Date	Comments
V0.1	12/06/2018	Initial version and structure by LTU
V0.2	18/06/2018	Ch. 1, 2. Ch. 3 and 4 started by LTU
V0.3	19/06/2018	Comments, additions and revisions by SRFG/wb
V0.4	19/06/2018	Addressed comments, additions and revision by LTU
V0.5	28/06/2018	Section 5 added. LTU minor updates of other sections
V0.6	29/06/2018	Platform owner requirements added (from D4.4)
V0.7	01/07/2018	All available requirements mapped into the Requirement Summary (see Section 5.6)
V0.8	05/07/2018	Final review and revision
V1.0	06/07/2018	Submission

Table 1 Acronyms

Acronym	Meaning
B2B	Business to Business
NIMBLE	Collaboration Network for Industry, Manufacturing, Business and Logistics in Europe
PaaS	Platform as a Service
UX	User Experience

List of Tables

Table of Contents

1 Introduction

The overall objective of the NIMBLE project is to create a B2B collaborative platform for European businesses that could profit from the sustainable ecosystem and the federation. Through NIMBLE, companies will be able to efficiently search and find required counterparts, initiate negotiation processes, and establish supply chain collaboration, including the creation of private information exchange channels. As the target user group of the NIMBLE platform encompasses a variety of European SMEs, it is important firstly for the platform design, to consider this variety of users and secondly, for the user experience (UX) validation to ensure the differences between user expectations and system implementation are recorded and measured. This is the scope of work package 4, which has 5 deliverables and which marks the transition from the prototype phase of the project into the maturing phase.

D4.1 presents the Validation Methodology and Validation Plan.

D4.2 presents the results of the first round validation of the experience of buyers and suppliers in collaborating through the NIMBLE platform.

D4.3 summarizes the results of logistics and data sharers' views on the platform functionality, which at present, is based on two independent validation workshops organized by the furniture use case and the textile use case, respectively.

D4.4 summarizes the validation results of platform manager's needs to monitor and administrate the platform, including the mechanisms to ensure good governance across the emerging ecosystem. D4.4 also includes as the first step, the requirements capture from the platform manager's point of view.

The purpose of this report (D4.5) is in the first part, to bring together the lessons learned from the first validation phase and in the second part, consolidate all requirements that define the NIMBLE platform and the use cases. This required a comprehensive analysis of the requirements coming from:

- the original description of the action and the technical objectives described there,
- D1.1 "Requirements and Collaboration Design for Manufacturing and Logistics in Four European Use Cases", which established the specific sectorial needs of the use case partners,
- federated platform requirements identified in D2.1 "Platform Architecture Specification and Component Design" and D3.1 "Core Platform Infrastructure".
- D6.1 "Security and Privacy Requirements" presented in [NIMBLE-D6.1],
- D4.4 "Platform User Experience – Platform Manager's Point of View", and
- Technical issues reported as individual user requirements, during the early validation of the platform's releases 1 and 2.

Using a method of step-wise consolidation, we arrived at a consolidated repository of requirements that now allows us to create a project roadmap with clear justifications of the project activities and updated plans for the evolution of the platform in the four use cases and beyond.

1.1 Updates on the Validation Methodology

The initial validation methodology is presented in D4.1, describing the first round validation and evolution processes, including the following two parallel activities:

- *Functionality test* - for validating the performances of business services, and
- *UX-test* – for the validation of user experience related to the use of the NIMBLE platform.

The validation activities in WP4 started in M14, with an initial validation workshop. The original plan of splitting the validation tasks according to the roles, e.g. buyer, supplier, logistics provider, data sharer and retailer, did not manage to significantly differentiate between the specific actor's business models and the supported platform interface modalities, and this motivated the following changes related to WP4 deliverables: :

- □ In D4.1 "Validation Plan and Methodology" we describe our updated validation methodology;
- □ D4.2 "Platform User Experience from Supplier's and Buyer's Point of View" summarizes the validation results of suppliers and buyers using the NIMBLE core platform services, i.e. registration, publishing, search, and negotiation;
- □ D4.3 "Platform User Experience from Logistics and Data Sharers Point of View" summarizes the validation results of logistic providers and data sharers
- □ D4.4 "Platform User Experience – Platform Manager's Point of View" that had not been considered as a deliverable in its own right in the DOA, and
- □ D4.5 "Platform Evolvement - Recommendations, Requirements and Roadmap".

We added a new task to WP4: T4.6 which is about the platform continuous validation of newly integrated platform services over time.

The overall results of the first round validation pointed to various shortcomings of the platform:

- there were usability and functionality gaps (e.g. users did not know how to proceed with the use of the platform),
- there were differences in the quality of individual user functions
- there were response time issues in some features (e.g. publishing) noticeable to the users,
- users complained about the lack of utilities e.g. in case of lost passwords, etc.

The first validation phase also clarified the need for user role management services, which were not completed in the first release, adding to the functionality gaps.

Our proposed validation method of organising workshops in which several users from one use case validate the platform in parallel, and being supported by the NIMBLE development team available via Skype and a validation support mailing list, and with the validation leaders moderating the workshops, proved to be effective. We firstly collected the user experiences by questionnaire, and the workshop leaders communicated issues via the project dedicated wiki page. The development team translated all communicated issues into technical issues on Github (https://github.com/nimble-platform) and structured them further, using ZenHub (see: https://bit.ly/2KfMHeF) to proceed with issue resolution.

The validation process caused the further redesign and improvements of the platform services, which absorbed a fair amount of the development efforts. With the newly introduced task T4.6 for supporting continuous validation of services developed in T2.5 and T3.9, we expect the development and validation to be more agile and informed by each other's results and the user's requirements.

1.2 Matching the Release Schedule with Validation

Following the first project review in July 2017, the development team and the dissemination team had agreed on a quarterly release schedule starting with Release 1 in December 2017 and ending with Release 8 at the end of the project. In response, WP4 went on to set up an agile validation process in for continuous feedback on the latest developed platform functionalities, usability and UX. We expect the validation focus of agile development to improve the communication between WPs dedicated to the technical platform development and WP4. The objective of D4.5 can be seen as follows: (i) to create an aggregated view on the validation phases and (ii) establish an agile approach for continuous validation of the functionality and UX in NIMBLE.

Table 2 NIMBLE Platform Release Plan

Version	Release date	Functionality	Target number of companies	Comments
V8.0	2019-sep-01	V7.0 + ...	2048	(counted as total over all platforms)
V7.0	2019-jun-01	V6.0 + ...	1024	suggested entry point for a NIMBLE platform #3
V6.0	2019-mar-01	V5.0 + ...	512	
V5.0	2018-dec-01	V4.0 + ...	256	suggested entry point for a NIMBLE platform #2
V4.0	2018-sep-01	V3.0 + ...	128	
V3.0	2018-jun-01	V2.0 + ...	64	
V2.0	2018-mar-01	V1.0 + ...	32	
V1.0	2017-dec-01	Basic: registration, catalogue, search, simple business processes for buyers, sellers, logistics providers Detailed functionality is explained at <NIMBLE B2B Platform V1.0 - web page> A detailed release validation plan can be found at <NIMBLE Platform V1.0 Release Gate>	16	NIMBLE platform #1, run by the consortium

One of the difficulties for structured releases came from the fact that requirements and requirement owners were distributed over different partners some of whom had to play double roles as developers and requirements owners. With the structured requirements repository now in place, we are in a position to do validation of every release with specific focus on novel functions. A division of responsibility for validation is sensible, i.e. not all use cases need to validate all functions of all releases, but might distribute the validation amongst them, so that e.g. two use cases validate release 4, and the other two may focus on aspects of release 5 and so on, until all releases of NIMBLE are validated. With the later releases, external partners will also be invited to participate in the validation.

Results from the data gathering in T4.6 will feed into WP5 and WP7 deliverables.

2 Previous work in WP4

This section gives a summary of previous work carried out in WP4 during December 2017-April 2018. The following business services have been validated so far in WP4: (1) Register on platform, (2) Publish a catalogue, (3) Search for product and service, and (4) Negotiate for product and service.

WP4 started with the work with a validation plan including methods for validation and data gathering. The aim of the planning and data gathering phase in WP4 was to gather the use cases' internal end-users' view of NIMBLE and covered both functionality and UX. For efficiency, an intensive data-gathering period was recommended where data from all four internal target groups (buyers, suppliers, logistics, and data sharers), resulting in internal end-users views covering:

- Validation Plan and Methodology (reported in D4.1),
- Buyer and Seller Validation (reported in D 4.2),
- Logistics and Data Sharing Validation (reported in D4.3), and
- Platform Manager's Validation (reported in D4.4).

Following functional and UX criteria were tested:

Here different usability evaluation principles were listed and grouped in larger sets. The main functionality to test was if the tester was able to:

- register properly (easy-difficult, logic-not logic, etc.)
- search for a product or service (easy-difficult, logic-not logic, etc.)
- negotiate for a product or service to buy (easy-difficult, logic-not logic, etc.)
- establish what to buy and then to establish a contract (easy-difficult, logic-not logic, etc.).

Asking about usability is important in UX-methodology. Here are some examples that of common themes and nuances of usability, usability is broken down into principles (ISO 9241):

- Learnability: how easily can a new user learn to navigate the interface?
- Flexibility: in how many ways can a user interact with the system?
- Robustness: how well are we supporting users when they face errors?
- Efficiency: how quickly can users perform tasks?

- Errors: how many errors do users make, and how quickly can they recover from errors?
- Satisfaction: do users enjoy using the interface, and are they pleased with the results?
- Understandability: how well can a user understand what they are seeing?
- Operability: how much control does the user have within the interface?
- Attractiveness: how visually appealing is the interface?
- Usability compliance: does the interface adhere to standards?

Each Use Case carried out the validation of the first version of the NIMBLE platform where the main core services' functionalities were tested in workshops during February-March. In order to carry out the workshops, the Use Cases were provided with a validation plan with attached questionnaires guiding the validation process (see D4.1). The individual use case participants were asked to fill in a questionnaire from the buyer's and supplier's perspective during their experimentation of the core services. As an outcome of the questionnaires, each use case summarized required functions in priority lists (high, medium, low priority). The validations were done on the basis of V1.0 of the platform.

The arranged workshops resulted in a list of issues related to the functionality that needed to be addressed and further developed in main core services: registration, publishing, search and negotiation. In this round, some information resources and supporting texts were considered to lack. Therefore it was crucial to analyse the results of the validation questionnaires filled by the workshop attendants from the buyer and supplier point of view. Examples of issues to further address regarding functionality were the relation between the users and the platform in terms of navigation, flexibility in the interactions, efficiency, speed of response when performing specific tasks, quick recovery from made mistakes, usability, user-friendly interface and user satisfaction in the end. Some summarized feedback to the development team were:

Registration: The most positive views was realising where the users are in the process and understanding the design and names of menus and buttons. The most negative views were about feeling confident that the registration process was successfully fulfilled. Another negative view was that the main screen for registration is not self-explaining. The registration process was perceived as a simple process but a bit immature; the process was not very intuitive.

Publishing: Only four users had an opinion of this service from a buyer's point of view. The publishing process was viewed not easy to understand and three users were disappointed with the service.

Search: The service responded quickly and started quickly. Also users felt confident while searching. The most negative views concerned that the users could not find quickly what they wanted in the search process and that the main screen was not self-explaining. Also, since there was a lack of relevant taxonomy for some of the involved industries, several users had difficulties in stating their needs.

Negotiation: The majority of the views indicated that the negotiation process was not intuitive and it did not respond quickly to commands. The most negative views regards being not confident that the negotiation process is successfully fulfilled, the users could not easily and quickly understand the negotiating process, and that there was too much inconsistency in the process. The users did not feel confident while negotiating. The most positive views regarded the structure of the negotiation functionality, that it was understandable.

The validation team documented all comments on-line and the development team structured the comments further, translated them into software development issues on Github, and prioritized them for further development and improvement. The list of issues is openly visible via:

https://app.zenhub.com/workspace/o/nimble-platform/frontend-service/boards

Also openly visible is all core service development as NIMBLE is a major open source project:

https://github.com/nimble-platform

3 Agile development process

This agile style of development directly addresses the problems of rapid change needed in NIMBLE business service development and its functionality. The dominant idea in agile development is that the development team can be more effective in responding to needed changes in the validation process and hence improve the team's amicability-its sense of community and morale-so that people are more inclined to relay valuable information quickly (cf. Cockburn & Highsmith, 2001). To reduce the time from decision to feedback, the technical development team communicate changes and receive feedback from users (in the validation process) rapid and iteratively. It makes the development process more transparent.

Focus in the continued validation work is still on:

- *Functionality test:* The basic business service functionalities i.e. to register a company in the platform, publish products and services, making them discoverable, and participate in resulting supply chain engagements. During the project these basic functionalities will be enhanced with more advanced functionalities such as enabling the selective sharing of data among partners.
- *UX test:* UX data provides thorough insights in how the users perceive the NIMBLE platform and its business services. Hence, it answers to whether the users are satisfied with the business services, if these answers to their needs and expectations as well as how they feel about using the NIMBLE platform itself. It also covers their perceptions of the practical aspects such as utility, ease of use and efficiency of the system, i.e. the usability of the platform. UX is an area influenced and built on knowledge and experience of the user, the user's concerns, expectations, skills and abilities (Väänänen-Vainio-Mattila, Roto and Hassenzahl, 2008).

All the activities suggested in the agile development process, T4.6, needs to be designed, decided and executed in close collaboration with all four use cases. Different use cases will contribute in different ways depending on available resources. Depending on the number of releases, each use case can choose what releases to test and when in time it is suitable. Some methods to use are:

Workshops: Mix of partners and roles testing the new releases of the NIMBLE platform (demos), documenting positive and negative reflections of the functionality.

Focus Groups: Mix of partners and roles discussing and reflecting on a number of themes related to both functionality and user experience related to current business services. For instance, the tester starts the business service and go through the steps, fill out the survey and it is preferable if the tester "think aloud" so that notes can be taken of specific stops, thoughts, question raised etc.

Interviews: Conducting interviews with SMEs regarding reflection about NIMBLE as such, discussing scenarios etc.

Output from all activities should feed back into the development process of NIMBLE platform, as well as business models and collaboration models development.

Activities:

1. Follow technical development progress, integration and process progression from a UX perspective
   Based on secondary data of material relevance e.g. (GitHub, Slack, Confluence)
   Purpose: Provide UX perspective from buyers, suppliers, logistics, data sharers in the tech development
2. Follow up each platform release e.g. workshops, focus groups, interviews
   Purpose: Identify progression of value creation for feed back into tech dev process
3. Involving SMEs e.g. workshops, focus groups, interviews
   Purpose: External perspectives UX validation.

4 Lessons learned and recommendations

This section sums up the lessons learned, and based upon this we provide recommendations for the second validation round of NIMBLE. As mention earlier, the rationale for the first round validation and evolution rests with the objectives as expressed in the NIMBLE project proposal, where the main objective is to give manufacturing SMEs in Europe a stable and sustainable ecosystem. This is still valid for validation round two. Thus, besides the adopted agile process described above, we intend to interview presumptive external end users. Considering the estimated number of users of the NIMBLE Platform, it is important to gather external end users views, in order to capture their thoughts of what constitutes value for them when using NIMBLE. Hence, we need to get insights in external end users' needs and motivations, both for developing the platform itself, and for development of business models and collaboration models.

4.1 Lessons learned

Lesson learned 1: is to do continuous validation work of the NIMBLE business services, by investigating the usability of NIMBLE in accordance to following themes, broken down into different principles in accordance to ISO 9241 (see p. 3 above).

Lesson learned 2: the NIMBLE platform must reach a level of maturity i.e. it must become an attractive B2B-platform, before external users (SMEs) will want to get involved to validate future possibilities of NIMBLE concerning collaboration and enhanced value throughout the value chain.

Lesson learned 3: most end users are familiar with existing well-known platforms such as Amazon and Ali Baba, and therefore individuals base their expectation of NIMBLE core functions on their previous experiences. This makes it important to handle and meet the expectations in the future releases diminishing the expectation gaps in order to make the users committed. It also points to using current platforms as benchmark for further development of functions for UX.

Lessons learned 4: the governance and ownership of the NIMBLE platform are important aspects for attracting future users and to ensure sustainability of the platform. There is a need to continue the work on investigating "who" will own NIMBLE and how NIMBLE should be governed. However, a process for this is outlined and reported in D4.4 (Section 4.3 – Governance Mechanisms).

Lessons learned 5: It is essential in the development of NIMBLE to continue to involve partners and the use cases in the development process and support a sense-making process for mutual understanding, hence internal communication must improve in order to create engagement, trust and commitment. This is part of the risk management for the project *per se*. The agile work process also mandates close interaction and communication. To support this better, we use besides e.g. e-mail and phone calls:

- **Atlassian Confluence (wiki)** for document sharing, project information, meeting notes, agendas and status reports.

- **Slack** for quick communication during the agile process, for transparency of the different WPs work. Here it is possible to upload documents, write short comments and make calls. In this way, the development process becomes more transparent, and makes it possible to gather fast feedback on various issues, and hence co-creation.

4.2 External end-user validation

UX data provides in-depth insights in how the end users perceive the NIMBLE platform and its business services. The NIMBLE project will need this data to explore whether the users are satisfied with the business services, whether the services answer to their needs and expectations and how they feel about using the NIMBLE platform itself. It also covers their perceptions of the practical aspects such as utility, ease of use and efficiency of the system, i.e. the usability of the platform.

Moreover, targeting European manufacturing SMEs indicates that validation and evolution of initial business services should cover different user groups, in different manufacturing industries, as well as in different countries. This is crucial in order to ensure one of the NIMBLE project high-level objectives: ease-of-entry and ease-of-use (DoA). The UX data is utterly important for future work with developing business models as well as collaboration models in the NIMBLE platform.

This means that the use cases will identify external end-users (SMEs), since they can provide valuable information about the specific use of NIMBLE business services. Thus, these external end users need not, but could be, identified in the supply chain. If the latter applies, the relationship to the use case company should be characterized as low risk.

The aim of this validation is to gather the external end users' (i.e. SMEs) view of NIMBLE concerning UX. The results will contribute to development of NIMBLE's business models and collaboration models. The following themes should be reported upon (see also Appendix A and B);

- □ Context: Where are the users? What are the conditions under which they work?
- □ User's view on NIMBLE's idea: What are their incentives to use the platform? What future situation do they want to reach? "What's in it for me?"
- □ Business services (current): What are their views of NIMBLE's current business services?
- □ Business services (wish list): What type of functionality are they expecting from the NIMBLE B2B platform? Which functions are desirable and which are less important?
- □ NIMBLE collaboration value: What will the value be using a B2B-platform like NIMBLE?
- □ Areas of improvement: Problem formulation? How can a B2B-platform support information exchange and collaboration in the supply chain?

One issue could be whether to use the NIMBLE demo or not during the interviews, and this depends upon how developed the demo is at the time for the interviews. However, we strongly advise each use case to feel free to design their external end user validation as suits them best, while still relying on the interview guide (Appendix B).

The interviews should take place during October-November 2018, since the results must be available when the work with developing business models and collaboration models starts.

4.3 WP4 Results for integration to WP5, WP7 and WP8

The agile process and extended T4.6 ensures that WP5 gets feedback for the NIMBLE value-added services. WP5 is dedicated to develop value-added business services in NIMBLE, beyond the core features, adding new features such as search and categorization, negotiation, analytics, cost and ecological footprint estimations, etc. thus, results from WP4 needs to be incorporated. These results are also important for the creation of reusable business process constructs building on: 1) the well-known collaboration patterns such as CPFR CTM and VMI, 2) collaboration processes required in use cases and 3) the feedbacks gathered from platform users in WP4. This imply taking a holistic view of NIMBLE, looking for generic aspects that will contribute to NIMBLE platform sustainability.

WP7 deals with the validation of the use cases, and rests on the work with validation and evolution done in WP4. In WP7 the segmentation of stakeholders into several target groups will be organised. Further, the identification of stakeholder's interests and strategies (e.g. social objectives, economic aspects) will take place and finally, validation methods including interviews with stakeholders about platform features, its functionality, usability, quality of the results, etc. will take place. Based on these results we will identify main gaps and challenges for future progress of the project and the platform evolution.

In addition, the objective for WP8 is to develop robust and timely dissemination, communication and exploitation plans with measurable outcomes. Therefore, results from WP4, WP5 and WP7 will lead the platform development towards its adoption, a task assigned to, and performed in, WP8.

5 NIMBLE Requirements Summary

One of the weaknesses of the design, development and validation process so far, was that no formal deliverable was defined, which covered **all requirements** – from use cases to platform owners, cloud service providers and other stakeholders, e.g. the Commission wanting broad access of SMEs to such platforms. Hence, our motivation in this chapter is to summarise at least at the top-level, the complete scope of the requirements that a commercial platform based on NIMBLE technology should fulfil. It serves as our starting point for the second phase of the NIMBLE project. We state the full scope of requirements for the planned platform and we will need a management process to prioritise further development in the best interest of the project and its stakeholders.

5.1 General End User and Platform Requirements as of DoA

The table below summarizes the main project commitments as defined in the DoA.

Table 3 NIMBLE platform requirements, platform-related business applications and user requirements as defined in the DoA

REQUIREMENT ID	DESCRIPTION	WHERE IN THE DoA
Platform reqs.		
DoA-PL-01	*...federated platform providers give different sectors or regions **a platform instance for B2C, B2B and M2M collaboration**.*	*pp. 5*
DoA-PL-02	*The regional or sectoral platform instance is capable of interoperating with other platforms in the **federation, via semantic interoperability services**.*	*pp. 5, 8*
DoA-PL-03	*Specialisations would be necessary to account for **sector specific practices and standards**...*	*pp. 5*
DoA-PL-04	*... and localisations may be necessary to deal with **national laws, regional practices** and language preferences.*	*pp. 5*
DoA-PL-05	*NIMBLE objective: To create a platform ecosystem to **attract early adopters***	*pp. 5*
DoA-PL-06, DoA-PL-16	*NIMBLE objective: To ensure **ease of entry and initial ease of use** with quick rewards*	*pp. 5*
DoA-PL-07	*NIMBLE objective: To **grow platform usage** by showing the benefits and by adding services where the need arises*	*pp. 5*

DoA-PL-08	*NIMBLE objective: To master the usage of the platform step-by-step to* ***evolve business cooperation***	*pp. 5*
DoA-PL-09	*NIMBLE objective: To* ***ensure trust, security and privacy.***	*pp. 5*
DoA-PL-10	*Objective 1: Develop the NIMBLE collab. infrastructure with* ***core services*** *(subscribe, publish/search, negotiate and execute tasks, monitor and control the collab.)*	*pp. 7*
DoA-PL-11	*1.1 Establish with stakeholders, the* ***requirements for core services*** *of the platform.*	*pp. 7*
DoA-PL-12	*1.2 Design the* ***top-level architecture and modules****.*	*pp. 7*
DoA-PL-13	*1.3* ***Use permissive open source software*** *wherever possible.*	*pp. 7*
DoA-PL-14	*1.4 Deploy the basic infrastructure with core services, to use case partners*	*pp. 7*
DoA-PL-15	*1.5 Learn from early validation.*	*pp. 7*
DoA-PL-17	*2.1 A company can* ***publish its product catalogue*** *in bulk or via semantic product descriptions*	*pp. 7*
DoA-PL-18	*2.2 Two companies can establish* ***private, encrypted information channels*** *for a business collaboration. In NIMBLE phase two, arbitrary supply chains can be established between any number of firms.*	*pp. 7*
DoA-PL-19	*2.3 Services for* ***matchmaking*** *between producers and consumers are available to establish business collab. fast.*	*pp. 7*
DoA-PL-20	*2.4 Gaining mutual benefits from shared information leading to* ***optimized re-planning****.*	*pp. 7*
DoA-PL-21	*2.5 Data collection, management and* ***analytics****.*	*pp. 7*
DoA-PL-22	*Objective 3: Growing the use of the platform*	*pp. 7*
DoA-PL-23	*3.1 Each of the use cases demonstrates benefits for businesses leading to a "me too" effect*	*pp. 7*
DoA-PL-24	*3.2 Start early adopter scheme, recruiting external users of the platform.*	*pp. 7*
DoA-PL-25	*3.3. Provide a core software tool set to initiate the software supply side of the platform.*	*pp. 7*
DoA-PL-26	*3.4 Improve business integration between different sectors*	*pp. 7*

DoA-PL-27	*Objective 4: Enhance platform functionality from the core services and ensure that firms master it on their own*	*pp. 7*
DoA-PL-28	*Objective 5: Ensure trust in the platform*	*pp. 8*
DoA-PL-29	*5.1. Support user-adjustable levels of security and privacy & maintain customer trust in balance with ease of use*	*pp. 8*
DoA-PL-30	*5.2. The platform will be designed* ***modular and resilient*** *so that security breaches can never "sink the whole ship"*	*pp. 8*
DoA-PL-31	*5.3.* ***Data storage*** *must be entirely at the owner's control - from cloud to storage on personal devices.*	*pp. 8*
DoA-PL-32	*5.5.* ***Grow trust*** *on the platform by a) fair gain distribution among the platform sides; b) maintaining strict interoperability; c) providing privacy in B2B communication and data exchange*	*pp. 8*
DoA-PL-33	*5.6.* ***Information quality*** *will be a fundamental value to be maximised in the platform.*	*pp. 8*
Business Applications		
DoA-APP-01	*The Product / Service Publishing and Search (T3.2, T3.3)*	*pp. 11, 53*
DoA-APP-02	*The Collaborative Process Modelling Tool (T3.4)*	*pp. 11, 20, 53*
DoA-APP-03	*The Negotiation Tool (T3.4)*	*pp. 11, 53*
DoA-APP-04	*The Matchmaking Tool (T3.4)*	*pp. 11, 53*
DoA-APP-05	*The Data Channels (T3.5)*	*pp. 54*
DoA-APP-06	*Product Lifecycle Data Management (T3.6)*	*pp. 13, 20, 54*
DoA-APP-07	*User front-ends (T3.7)*	*pp. 54*
DoA-APP-08	*The Interoperability Testing Tool (T3.8)*	*pp. 54*
DoA-APP-09	*The Benchmarking Toolset (T5.5)*	*pp. 12, 57*
DoA-APP-10	*Operational Supply Chain Management (T5.4)*	*pp. 12, 57*
DoA-APP-11	*Object level applications (T5.4)*	*pp. 12, 57*
DoA-APP-12	*NIMBLE Enterprise Tier: Dev-Ops Center (T5.2)*	*pp. 12, 56*
DoA-APP-13	*Agent Supported negotiation for Optimization in the Value Network (T5.6)*	*pp. 20, 57*

DoA-APP-14	*Asset Virtualization (T2.2)*	*pp. 13*
DoA-APP-15	*The Big Data Toolset (T3.1, T5.1, T5.2, T5.3)*	*pp. 12, 13, 56, 57*
DoA-APP-16	*The use of prefabricated business process templates and tools for layered trust models that allow different degrees of cross-company information sharing (T5.7)*	*pp. 20, 57*
DoA-APP-17	*(Cross-) Instance API and B2B Interoperability (T2.2, T2.4) (semantic interoperability to enable cross-platform and cross-sector business transactions. This will make enterprises more agile to move into new markets).*	*pp. 13, 20*
DoA-APP-18	*Use of standard security controls for features such as data integrity, confidentiality, identity and key management, authentication as well as fine-grained authorization and access (T6.2).*	*pp. 14, 58*
DoA-APP-19	*Novel security features will include management of reputation metrics and management of data quality (also including automated measures). (T6.3, T6.4)*	*pp. 14, 58, 59*
End user reqs.		
DoA-UC-01	*WP6 to aggregate security, privacy, reputation and information quality aspects so that the platform is trusted.*	*pp. 20*
	Whirlpool Europe srl	
DoA-UC-02	*NIMBLE will enable data aggregation, advanced analytics, smart decision support systems and self-learning capabilities, monitoring and exploiting history logs (reports) and customer complaints, and other relevant data*	*pp. 17, 87*
DoA-UC-03	*NIMBLE will support KPI management and dynamic correlation of all KPI available at production level (FOR index, Q index, etc) with Quality KPIs coming from the field (SIR, 12MIS etc.). Correlation of CRM reports with production data analysis;*	*pp. 17, 30, 87*
	Lindbäcks	
DoA-UC-04	*Supply chain flexibility.*	*pp. 17, 30*
DoA-UC-05	*Dynamically establishing new logistics chain.*	*pp. 18, 30*
DoA-UC-06	*Dynamic logistics negotiation tool.*	*pp. 30*
DoA-UC-07	*Monitoring of transport logistics, on-site construction, and environmental conditions during transportation.*	*pp. 18, 30*

DoA-UC-08	*Relaying quality information of supplier's products from the construction site back to Lindbäcks.*	*pp. 18, 30*
DoA-UC-09	*Tracing all materials, work steps and intermediate products throughout the building's life cycle*	*pp. 30*
DoA-UC-10	*Automated coordination of reliable data exchange among supply network partners*	*pp. 30*
	Piacenza	
DoA-UC-11	*Collaborative design and development of high-end fabrics for the textile markets.*	*pp. 17*
DoA-UC-12	*Access to supplier virtual catalogues and inventories for fast design development*	*pp. 30, 91*
DoA-UC-13	*Monitoring of production via mobile. Complete traceability of all materials and production phases.*	*pp. 17, 19, 91*
DoA-UC-14	*Automatic creation of the origin certificate declaration.*	*pp. 30*
DoA-UC-15	*Full manufacturing and product traceability, including ethical and environmental fulfilment.*	*pp. 30*
DoA-UC-16	*Protection from fraud and unauthorized use within the company and through the value chain.*	*pp. 91*
	Micuna, s.l.	
DoA-UC-17	*Legal compliance of production, based on access to local market regulations, safety, and trade standards regulation.*	*pp. 18, 30*
DoA-UC-18	*Smart supply chain management.*	*pp. 19*
DoA-UC-19	*Dynamic, real-time access to supplier catalogues and inventories.*	*pp. 30*
DoA-UC-20	*Assessment of product lifecycle phases and environmental impact of entering a new market.*	*pp. 30*
DoA-UC-21	*Capturing lifecycle performance data.*	*pp. 30*

5.2 General End User Requirements as of D1.1

Table 4 NIMBLE General use case requirements as defined in D1.1.

REQUIREMENT ID	DESCRIPTION	RESPECTIVE COMPONENTS
D1.1_UC_01	*Platform supports user management*	*Registration service / identity*
D1.1_UC_01_01	*User can manage user roles*	*Registration service / access controls*
D1.1_UC_01_02	*User can manage user access rights*	*Registration service / access controls*
D1.1_UC_01_03	*User can register a company*	*Registration service*
D1.1_UC_02	*User can upload product information*	*Catalogue service / Platform front-end*
D1.1_UC_03	*User can upload service information*	*Catalogue service / Platform front-end*
D1.1_UC_04	*User can upload context information*	*Catalogue service / Platform front-end*
D1.1_UC_05	*User can publish product information*	*Publish service / Platform front-end*
D1.1_UC_06	*User can publish service information*	*Publish service / Platform front-end*
D1.1_UC_07	*User can specify target group for published products*	*Access controls / Data sharing service*
D1.1_UC_08	*User can specify target group for published services*	*Access controls / Data sharing service*
D1.1_UC_09	*User can search for other companies*	*Search service / Platform front-end*
D1.1_UC_10	*User can search for services*	*Search service / Platform front-end*
D1.1_UC_11	*User can search for products*	*Search service / Platform front-end*
D1.1_UC_12	*User can create and execute search filters for companies*	*Search service / Matchmaking / Platform front-end*
D1.1_UC_13	*User can create and execute search filters for services*	*Search service / Matchmaking / Platform front-end*
D1.1_UC_14	*User can create and execute search filters for products*	*Search service / Matchmaking / Platform front-end*
D1.1_UC_15	*Platform protects process flows*	*Security service/ Data integrity*

D1.1_UC_16	*Platform protects product data*	*Security service/ Data integrity*

5.3 NIMBLE Federated Ecosystem Requirements as of D2.1.2

Table 5 NIMBLE federated platform requirements and their mapping to the platform components.

REQUIREMENT ID	DESCRIPTION	RESPECTIVE COMPONENTS
FED-APP-01	*Register (user / company)*	*Registration service / identity service*
FED-APP-02	*Role based registration*	*Registration service / identity service*
FED-APP-03	*Role based ACL to platform services*	*Security / identity service*
FED-APP-04	*Update and delete registered users*	*Registration service / identity service*
FED-APP-05	*Publish single item / bulk*	*Catalogue*
FED-APP-06	*Add / modify / delete published items*	*Catalogue*
FED-APP-07	*Standard categories for publishing*	*Catalogue*
FED-APP-08	*Simple Search*	*Search*
FED-APP-09	*Semantic Search*	*Search, Registry (annotated products)*
FED-APP-10	*Collaboration - Addition. info. request*	*Business Process*
FED-APP-11	*Negotiation*	*Business Process*
FED-APP-12	*Matchmaking*	*Business Process*
FED-APP-13	*Order*	*Business Process*
FED-APP-14	*Generic data exchange*	*Communication / Collab. services*
FED-APP-15	*Data processing / management*	*Offline and online data processing*
FED-APP-16	*Real-time dynamic data sharing*	*Data channels*
FED-APP-17	*IoT data ingestion and processing*	*Data channels (and advances platform services)*
FED-APP-18	*Simple Data analytics*	*Data analytics*
FED-APP-19	*Notification*	*Cloud service bus*
FED-APP-20	*Federation*	*Open API*
FED-APP-21	*Scalability*	*Run-time; cloud service bus; data management*

FED-APP-22	*Security: authentication, authorization and role-based ACL*	*Security components (identity service)*
FED-APP-23	*Trust and reputation*	*Trust and reputation components*
FED-APP-24	*High availability*	*Cloud based deployment and associated services*
FED-APP-25	*Ease-of-use*	*Platform front-end*
FED-APP-26	*Web based single point of access*	*Platform front-end*

5.4 NIMBLE Security, Privacy and Trust Requirements as of D6.1

The summary of security, privacy and trust requirements in NIMBLE is based on D6.1 "Security and Privacy Requirements" report [NIMBLE-D6.1], which refers on the following tasks and their reports:

- *D1.1 "Requirements and Collaboration Design for Manufacturing and Logistics in Four European Use Cases",*
- *D2.1 "Platform Architecture Specification and Component Design", and*
- *D3.1 "Core Platform Infrastructure".*

NIMBLE D6.1 identifies and specifies use case-centric security and privacy requirements (based on D1.1), platform-centric security and privacy requirements (based on D2.1 and D3.1) and designs the NIMBLE Privacy Requirements Framework for addressing additional privacy related questions, including the General Data Protection Regulation (GDPR). The mapping between GDPR requirements and the platform-centric security and privacy requirements is given in D6.1 Appendix 1.

In NIMBLE D6.1, we performed mapping of the use case-centric and platform-centric security requirements, to eliminate inconsistencies between the requirements and to provide their final prioritization and specification before finalizing the design and development of security controls for core services in task T6.2 (D6.2). Finally, the requirements evaluation in D6.1 is done through data flow analysis of the core processes running over the platform, following the STRIDE threat modelling principles.

In this Section, we extract the summaries of (1) use case-centric security and privacy requirements, and (2) platform-centric security and privacy requirements. For the visual representation of mapping between (i) the use case-centric security and privacy requirements and (ii) specific use case requirements as of D1.1, please see Section 5 of D6.1 [NIMBLE-D6.1].

5.4.1 Summary of Use Case-Centric Security and Privacy Requirements

Table 6 Summary of functional use case-centric security requirements (FUN_SEC_x).

Sec. Req. ID	Name	Priority	Description	Security controls
FUN_SEC_UC_01	*Secure access to the platform*	*MUST*	*Establishing secure connection between users and the platform. Preventing unauthorized access to the platform.*	*Identification & authentication methods for secure access services;*
FUN_SEC_UC_02	*Secure access to data to support search and analytics*	*MUST*	*Establishing secure access to product data and provenance information, e.g. for tracking purposes*	*Authentication methods for secure search services;* *Authorization & access control management;*

FUN_SEC_UC_03	Secure data manipulation	MUST	Performing secure data manipulation, e.g. comparison of providers and products, filtering and ordering providers and products according to specific criteria, configuration of products, etc.	Authorization methods for data manipulation services; Access control management;
FUN_SEC_UC_04	Secure access to data to support negotiation	MUST	Establishing secure access to sensitive data (financial data, delivery data) required for negotiation	Authentication mechanisms for negotiation services; Authorization & access control management;
FUN_SEC_UC_05	Secure information exchange	MUST	Establishing secure information exchange (file sharing, platform email exchange sys., notifications)	Identification & access control management;
FUN_SEC_UC_06	Secure user communication via the platform	MUST	Exchanging messages among the platform's users	Identification & authentication mechanisms for secure access services;
FUN_SEC_UC_07	Secure publishing & maintaining of the product catalogues	MUST	Establishing secure services and privacy controls for publishing & maintaining product catalogues	Authentication methods for product catalogues; Authorization & access control management;
FUN_SEC_UC_08	Access to the normative and legislation repositories	COULD	Establishing secure access to support the compliance check with normative and legislations in the destination country, (see AIDIMME"s UC)	Authentication mechanisms for accessing a repository of normative and legislations; Authorization & access controls;

Table X: Summary of non-functional use case-centric security requirements (NFUN_SEC_x).

Sec. Req. ID	Name	Priority	Description	Security controls

NFUN_SEC_01	Confidentiality	MUST	Information is not made available or disclosed to unauthorized individuals, entities, services.	Authorization and access control management
NFUN_SEC_02	Integrity	MUST	Data accuracy and data completeness need to be assured.	Authorization and access control management; Data accuracy check; Data completeness check
NFUN_SEC_03	Availability	MUST	Security methods for services and data must be functional and available when they are needed.	Data accuracy check; Data completeness check
NFUN_SEC_04	Authenticity	MUST	The proof of identity can be based on a password, a key card, or biometric method.	User identification & authentication followed by the verification
NFUN_SEC_05	Reliability	MUST	Information to support search and negotiation is reliable (operable under designed operating conditions, for a designed period of time).	Notification services in place in case of problems appeared
NFUN_SEC_06	Trust and reputation	MUST	Trust and reputation of actors must be automatically assessed	Trust and reputation mechanisms (e.g. based on mutual evaluation of business actors)
NFUN_SEC_07	Compliance to normative and legislations	SHOULD	Privacy and access to information and laws are primary areas of concern	Validation of extracted requirements for consistency and compliance to normative and legislation
NFUN_SEC_08	Usable security	SHOULD	The platform must be usable when security and privacy related methods are executed	Efficiency of the platform: speed, learnability, preferences, memorability.

Table 7 Summary of use case-centric privacy requirements in NIMBLE

Priv. Req. FINAL ID	Priority	Name	Description	Privacy controls

PRIV_UC_001	*SHOULD*	*Normative and legislation awareness*	*Establishing privacy awareness mechanisms for the normative and legislation repositories*	*Privacy awareness services should be easy to subscribe to, easy to change subscription preferences;*
PRIV_UC_002	*MUST*	*Privacy controls for product catalogues and data*	*Sharing corporate and product data with third parties; Access controls for sharing production data;* *Insecure data transfer;*	*Privacy controls and penetration tests with a focus on privacy;*
PRIV_UC_003	*SHOULD*	*Privacy methods related to the creation of the Textile Certificate of Origin*	*The Textile Certificate of Origin can contain confidential information e.g.“available upon request”; It must be signed by the legal entities; It includes legal information of the fabric producer.*	*Privacy certification application for dealing with specific privacy and security requirements related to certification process. Managing certification process with pre- and post-certification.*
PRIV_UC_004	*MUST*	*Privacy compliance (e.g. compliance with the GDPR requirements)*	*- Specification of entities with the rights to access the data;* *- User interface comp. with links to privacy policies.* *- Links for users to send privacy related questions.* *- Data protection compliance.*	*Privacy tests, e.g. test for deletion requests, create, maintain and test incident response plan;*

5.4.2 Summary of Platform-Centric Security and Privacy Requirements

In this Section, we summarize platform-centric security and privacy requirements according to their priorities: MUST, SHOULD, COULD, as identified in [NIMBLE D6.1].

5.4.2.1 Core Security and Privacy Requirements

Table 8 Core Security and Privacy Requirement: Priority - MUST

Sec. Req. ID	Name	Type	Priority	Security functionality	Implement. task
SEC_IDM_01	*Identification Policy and Procedures*	*NFR*	*MUST*	*Identity Management*	*T6.2, T6.4*
SEC_ACM_01	*Access Control Policy and Procedures*	*NFR*	*MUST*	*Access Control Management*	*T6.2, T6.4*

SEC_AAM_01	*Authentication Policy and Procedures*	*NFR*	*MUST*	*Authentication and Authorization Management*	*T6.2, T6.4*
SEC_DIDQ_01	*Data Integrity and Data Quality Policy*	*NFR*	*MUST*	*Data Integrity and Data Quality Management*	*T6.2, T6.4*
SEC_IDM_02	*Federated Identity Management and SSO*	*FR*	*MUST*	*Identity Management*	*T6.2*
SEC_IDM_02_1, SEC_IDM_02_3	*Federated Identity Management for network/ local access to privileged accounts*	*FR*	*MUST*	*Identity Management*	*T6.2*
SEC_IDM_02_2, SEC_IDM_02_4	*Federated Identity Management for network/ local access to non-privileged accounts*	*FR*	*MUST*	*Identity Management*	*T6.2*
SEC_ACM02	*Access Enforcement mechanisms*	*FR*	*MUST*	*Access Control Management*	*T6.2*
SEC_ACM02_1	*Mandatory access controls*	*FR*	*MUST*	*Access Control Management*	*T6.2*
SEC_ACM02_2	*Discretionary access controls*	*FR*	*MUST*	*Access Control Management*	*T6.2*
SEC_ACM02_3	*Role-based access controls*	*FR*	*MUST*	*Access Control Management*	*T6.2*
SEC_ACM02_4	*Access to privileged functions*	*FR*	*MUST*	*Access Control Management*	*T6.2*
SEC_ACM_03	*Information Flow Enforcement mechanisms*	*FR*	*MUST*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM_03_1	*Domain authentication*	*FR*	*MUST*	*Access Control Management*	*T6.2*
SEC_ACM_03_2	*Validation of metadata*	*FR*	*MUST*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM_04	*Account Management*	*FR*	*MUST*	*Access Control Management*	*T6.2*
SEC_ACM_04_1	*Dynamic account creation*	*FR*	*MUST*	*Access Control Management*	*T6.2*

SEC_ACM_04_2	*Dynamic privilege management*	*FR*	*MUST*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM_04_3	*Account monitoring*	*FR*	*MUST*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM_04_4	*Account maintenance*	*FR*	*MUST*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM_05	*Access Control for Mobile Devices*	*FR*	*MUST*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM07	*Access Controls for Information Sharing*	*FR*	*MUST*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM07_1	*Information Search and Retrieval*	*FR*	*MUST*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM07_2	*Decision Support*	*FR*	*MUST*	*Access Control Management*	*T6.2, T6.4*
SEC_AAM_02	*Authentication of Users, Devices and Services*	*FR*	*MUST*	*Authentication and Authorization Management*	*T6.2, T6.4*
SEC_AAM_02_1	*User Authentication for network access to privileged accounts*	*FR*	*MUST*	*Authentication and Authorization Management*	*T6.2, T6.4*
SEC_AAM_02_2	*User Authentication for network access to non-privileged accounts*	*FR*	*MUST*	*Authentication and Authorization Management*	*T6.2, T6.4*
SEC_AAM_02_3	*User Authentication for local access to privileged accounts*	*FR*	*MUST*	*Authentication and Authorization Management*	*T6.2, T6.4*
SEC_AAM_02_4	*User Authentication for local access to non-privileged accounts*	*FR*	*MUST*	*Authentication and Authorization Management*	*T6.2, T6.4*
SEC_AAM_02_5	*Group Authentication*	*FR*	*MUST*	*Authentication and Authorization Management*	*T6.2, T6.4*
SEC_AAM_03	*Authentication Management*	*FR*	*MUST*	*Authentication and Authorization Management*	*T6.2, T6.4*
SEC_AAM_03_1	*Password based authentication*	*FR*	*MUST*	*Authentication and Authorization Management*	*T6.2*

SEC_AAM_03_2	*Cross-organization credential management*	*FR*	*MUST*	*Authentication and Authorization Management*	*T6.2*
SEC_PROV_01	*Recording information on data origin*	*FR*	*MUST*	*Data Provenance Management*	*T6.2, T6.3, T6.4*
SEC_PROV_02	*Recording information on data modification*	*FR*	*MUST*	*Data Provenance Management*	*T6.2, T6.3, T6.4*
SEC_TRM02	*Reputation of users and services must be automatically estimated*	*FR*	*MUST*	*Trust and Reputation Management*	*T6.3*
SEC_DIDQ_02	*Data input validation*	*FR*	*MUST*	*Data Integrity and Data Quality Management*	*T6.2, T6.4*
SEC_DIDQ_03	*Data and metadata protection*	*FR*	*MUST*	*Data Integrity and Data Quality Management*	*T6.2, T6.4*
SEC_DIDQ_03_1	*Data protection at rest*	*FR*	*MUST*	*Data Integrity and Data Quality Management*	*T6.2, T6.4*
SEC_DIDQ_03_2	*Data protection in shared resources*	*FR*	*MUST*	*Data Integrity and Data Quality Management*	*T6.2, T6.4*
SEC_DIDQ_05	*Informed consent by Design*	*NFR*	*MUST*	*Data Integrity and Data Quality Management*	*T6.2, T6.4*
PRIV_PLAT_01	*Data privacy*	-	*MUST*	*Privacy*	*T6.2, T6.3, T6.4*
PRIV_PLAT_02	*Platform code and services privacy*	-	*MUST*	*Privacy*	*T6.2, T6.3, T6.4*
PRIV_PLAT_03	*Preventing unauthorized access*	-	*MUST*	*Privacy*	*T6.2, T6.3, T6.4*
PRIV_PLAT_04	*Informed Consent*	-	*MUST*	*Privacy*	*T6.2, T6.3, T6.4*
PRIV_PLAT_05	*Data minimization principle*	-	*MUST*	*Privacy*	*T6.2, T6.3, T6.4*
PRIV_PLAT_06	*Prohibiting interaction with children or non-business entities*	-	*MUST*	*Privacy*	*T6.2, T6.3, T6.4*

Table 9 Core Security and Privacy Requirement: Priority - SHOULD

Sec. Req. ID	Name	Type	Priority	Security functionality	Implem. task
SEC_ACM02_5	*Dual authorization*	*FR*	*SHOULD*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM02_6	*Review of user privileges*	*FR*	*SHOULD*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM02_7	*Control of user privileges*	*FR*	*SHOULD*	*Access Control Management*	*T6.2, T6.4*
SEC_ACM_03_3	*Security policy filters*	*FR*	*SHOULD*	*Access Control Management*	*T6.2, T6.4*
SEC_AAM_02-6	*Cryptographic bidirectional network authentication of devices*	*FR*	*SHOULD*	*Authentication and Authorization Management*	*T6.4*
SEC_AAM_03_3	*Expiration of cached authentication*	*FR*	*SHOULD*	*Authentication and Authorization Management*	*T6.4*
SEC_AAM_03_4	*Authentication feedback*	*FR*	*SHOULD*	*Authentication and Authorization Management*	*T6.4*
SEC_AAM_03_5	*Re-Authentication support*	*FR*	*SHOULD*	*Authentication and Authorization Management*	*T6.4*
SEC_DIDQ_04	*Notification of data integrity violations*	*FR*	*SHOULD*	*Data Integrity and Data Quality Management*	*T6.4*
SEC_TRM01	*Electronic Trust Services (eTS) regulation*	*FR*	*SHOULD*	*Trust and reputation Management*	*T6.3*

Table 10 Core Security and Privacy Requirement: Priority - COULD

Sec. Req. ID	Name	Type	Priority	Security functionality	Implem. task
SEC_ACM_06	*Access Control for Security Attributes Management*	*FR*	*COULD*	*Access Control Management*	*T6.4*

SEC_ACM06_1	*Security value changes*	*FR*	*COULD*	*Access Control Management*	*T6.4*
SEC_ACM06_2	*Security value maintenance and configuration*	*FR*	*COULD*	*Access Control Management*	*T6.4*

5.4.2.2 Platform Service Provider Security Requirements

The following is a checklist of security controls to be implemented at the platform provider side.

Table 11 Platform Service Provider Security Requirement: Priority - MUST

Sec. Req. ID	Name	Type	Priority	Security functionality
SEC_PLAT_01	*Security Monitoring*	*NFR*	*MUST*	*Platform provider*
SEC_PLAT_04	*Security Planning*	*NFR*	*MUST*	*Platform provider*
SEC_PLAT_06	*Contingency Plan*	*NFR*	*MUST*	*Platform provider*
SEC_PLAT_06_1	*Information system backup and recovery mechanisms*	*NFR*	*MUST*	*Platform provider*

Table 12 Platform Service Provider Security Requirement: Priority - SHOULD

Sec. Req. ID	Name	Type	Priority	Security functionality
SEC_PLAT_02	*Security Assessment*	*NFR*	*SHOULD*	*Platform provider*
SEC_PLAT_03	*Risk Assessment*	*NFR*	*SHOULD*	*Platform provider*
SEC_PLAT_05	*Audit Event Controls*	*NFR*	*SHOULD*	*Platform provider*
SEC_PLAT_05_1	*Audit recording and storing*	*NFR*	*SHOULD*	*Platform provider*
SEC_PLAT_05_2	*Audit review and analyses*	*NFR*	*SHOULD*	*Platform provider*
SEC_PLAT_05_3	*Audit correlations with other sources*	*NFR*	*SHOULD*	*Platform provider*
SEC_PLAT_05_4	*Protection of audit information*	*NFR*	*SHOULD*	*Platform provider*
SEC_PLAT_06_2	*Incident response*	*NFR*	*SHOULD*	*Platform provider*

SEC_PLAT_07	*Malicious code protection*	*NFR*	*SHOULD*	*Platform provider*
SEC_PLAT_08	*Spam protection*	*NFR*	*SHOULD*	*Platform provider*

5.4.2.3 Cloud Service Provider Security Requirements

In the following, we summarize cloud service provider security requirements, according to their priority criteria (MUST, SHOULD).

Table 13 Cloud Service Provider Security Requirement: Priority - MUST

Sec. Req. ID	Name	Type	Priority	Description
SEC_CC_01	*Data protection*	*NFR*	*MUST*	*Cloud provider*
SEC_CC_01_1	*Avoid unintended distribution of sensitive data*	*NFR*	*MUST*	*Cloud provider*
SEC_CC_01_2	*Avoid insecure or incomplete data deletion*	*NFR*	*MUST*	*Cloud provider*

Table 14 Cloud Service Provider Security Requirement: Priority - SHOULD

Sec. Req. ID	Name	Type	Priority	Description
SEC_CC_01_3	*Encrypted data transfer and application interaction*	*NFR*	*SHOUL D*	*Cloud provider*
SEC_CC_02	*System integrity check of cloud-hosted applications*	*NFR*	*SHOUL D*	*Cloud provider*
SEC_CC_03	*Key management*	*NFR*	*SHOUL D*	*Cloud provider*
SEC_CC_04	*Handling of security incidents*	*NFR*	*SHOUL D*	*Cloud provider*

5.5 Platform Owner's Management Requirements as of D4.4

The following table summarizes the requirements from D4.4.

Table 15 Platform Owner's Management Requirements

Req. ID	Description
Platform Accountability	
PM_ACC_01	*Keep a registry of users that can be (re-)connected to official records if necessary (e.g. for auditing historical data for fraud detection or taxation issues)*
PM_ACC_02	*Provide a list of business transaction types (negotiating, buying, supplying, etc.)*
PM_ACC_03	*Provide a taxonomy of user roles associated with business transaction types*
PM_ACC_04	*Keep a registry of user roles and actions: e.g. user U acting for firm F in role R doing action A at time T. Note keeping this type of information has privacy implications and requires data anonymization strategies to be put in place.*
PM_ACC_05	*Keep a record of all business transactions that happen via the platform; offer different levels of aggregation / anonymity for these, keeping to strict rules of privacy*
PM_ACC_06	*Make visible to users, a record of the number of platform transactions per user, per company (aggregates over hours, day, week, month, year)*
PM_ACC_07	*Keep a record of the monetary value of the transactions per company, etc.*
PM_ACC_08	*Provide any user with an immediate feedback option that also records the user context in which the feedback was given*
PM_ACC_09	*Allow any form of feedback and try to index the feedback according to a taxonomy (feature request, bug report, help request, complaint ...)*
Security Management	
PM_SEC_01	*The platform manager must be able to comply with his/her obligations as a GDPR Data Processor.*
PM_SEC_02	*The platform manager's account must be auditable to ensure compliance with GDPR rules and with other regulatory compliance (e.g. taxation rules)*
PM_SEC_03	*The platform manager's account must be retrievable and there must be a substitute available at all times, to ensure that there is not a "single point of failure" in the system.*
PM_SEC_04	*It should be possible to configure "honey pots" as a pro-active security strategy.*
PM_SEC_05	*Data storage should be designed in a modular and segmented manner to make data theft*

	"expensive" for the attacker (small rewards for high effort).
PM_SEC_06	*The platform manager role subsumes the following sub-roles: privacy management; platform security management; platform operational management*
PM_SEC_07	*The platform's security officer should have access to a dashboard that shows the threat vectors which the platform is experiencing.*
Federation Management	
PM_FED_01	*The NIMBLE Open API must, as a minimum requirement, support search, negotiation, contracting and fulfilment across platform instances of NIMBLE.*
Trust Management	
PM_TRUST_01	*There must be an algorithm that measures an overall level of trust for the platform. Can possibly be done as a confidence rating for a transaction to be successful. 100% would be the maximum.*
PM_TRUST_02	*There should be an algorithm that measures the perceived trust of non-users, concerning transactions happening on NIMBLE (platform reputation).*
PM_TRUST_03	*There must be an algorithm to calculate the trust level between any two entities (A and B, and B and A) respectively.*
PM_TRUST_04	*There should be an algorithm to detect trust imbalances that go beyond individual firms and that point to larger-scale discrepancies between constituencies on the platform*
PM_TRUST_05	*There must be a measure of effectiveness for firms getting from the state of entering negotiation, to the state of closing a deal successfully.*
PM_TRUST_06	*There must be a measure of satisfaction for firms, for getting from the state of having closed a deal, to fulfilment of its terms, i.e. a measure of how well the contract was honoured by both sides.*
PM_TRUST_07	*There should be a measure of quality for any information exchange happening inside the platform, and also for any information exchange happening between platform and external, non-users. The platform must be perceived as a constituency of highly trustworthy partners.*
Information Management	
PM-INF-01	*(Info-Flow-Monitoring) Platform manager must be able to monitor any B2B information flow that is originally enabled by NIMBLE*
PM-INF-02	*(Info-Flow-Control) Platform manager must be able to halt / restart any B2B information flow that is originally enabled by NIMBLE.*
PM-INF-03	*Any intervention in B2B processes at platform level must be auditable.*

PM-INF-04	*The platform manager must have access to a repository of local edge devices that are or have been, used in B2B data exchanges between companies, via NIMBLE. Current connectivity must be monitorable and past connectivity must be accessible through logs. This implies a need for an* ***asset virtualisation framework*** *that helps NIMBLE to keep maps of local edge devices and their connectivity with NIMBLE.*
Platform Manifesto	
PCS-ASV-01	***The ecosystem is the new warehouse:*** *Users must be able to achieve* ***asset virtualisation*** *in order to automate information flows in business transactions.*
PCS-DC-01	***The ecosystem is the new warehouse:*** *NIMBLE must provide* ***data channels for informational exchange*** *at M2M, O2O and B2B levels, for transparency over supply chains.*
PCS-UBL-01	***The ecosystem is also the new supply chain*** ***UBL*** *and eClass based business processes can be executed partly automatically*
PCS-ECL-01	***The ecosystem is also the new supply chain*** *UBL and* ***eClass*** *based business processes can be executed partly automatically*
PCS-NEG-01	***The network effect is the new driver for scale*** *Users must be able to engage in* ***business negotiations*** *that lead to formal contracts.*
PCS-NEG-02	***The network effect is the new driver for scale*** *Users must be able to close items of agreement in an iterative manner. Closed items of agreement shall be called* ***clauses of a contract****.*
PCS-CON-01	***The network effect is the new driver for scale*** *Users must be able to receive formalised contracts as the result of negotiations. This will be a core asset of NIMBLE because it now enables business transactions according to UBL.*
PCS-CON-02	***The network effect is the new driver for scale*** *Users must be able to view each element of agreement in a contract. These elements of agreement shall be called* ***clauses of the contract****.*
PCS-BTX-01	***The network effect is the new driver for scale*** *Users must be able to specify an* ***execution plan for a business transaction****. NIMBLE shall provide default execution plans for standard business transactions.*
PCS-BTX-02	*Given a company policy, a NIMBLE agent should be able to partially* ***automate the negotiation*** *and execution of standard business transactions.* *(NIMBLE T5.6: Agent supported negotiation)*
PCS-INF-01	***Data is the new dollar*** *The platform as data processor, needs to gather behavioural data from all participants in order to ensure good governance.*

PCS-INF-02	***Data is the new dollar*** *The platform needs to share a good proportion of behavioural data with the data subjects in order to support value creation*
PCS-PRV-01	***Data is the new dollar*** *The platform as data processor, needs to ensure that data subjects are protected from damages caused by data leakages.*
PCS-BAS-01	***Community management is the new human resources management*** ***User registration****: All users must first be registered before any activity can be done, except for search in public catalogues (can be done anonymously)*
PCS-BAS-02	***Community management is the new human resources management*** ***Company registration****: All companies must first be registered before they can become active on the platform*
PCS-BAS-03	***Community management is the new human resources management*** ***Catalogue publishing****: A company must be able to publish a product or service catalogue*
PCS-BAS-04	***Community management is the new human resources management*** ***Entity search****: a registered user from a registered company must be able to search for: Companies, Products, Services, and Users in specific roles (e.g. contacting the sales person)*
PCS-BAS-05	***Community management is the new human resources management*** ***Contract negotiation****: a registered user from a registered company must be able to engage in a contract negotiation leading to a closed deal, in the case of mutual agreement.*
PCS-ADV-01	***Community management is the new human resources management*** *Specialised interactions: when new interactions are designed then they must either be defined via UBL constructs or via the NIMBLE open API. Advanced services that break the basic interaction mechanisms may be disabled by the platform owner□ cross-reference with PM-GOV-05.*
PM_LIQ_01	***Liquidity management is the new inventory control*** *Measuring high quality interactions between participants.*
From (PM_TRUST_01 to PM_TRUST_07)	***Curation and reputation are the new quality control*** *Reputation and trust: metrics and rankings to foster good governance□ cross-reference trust; governance; information quality*
PCS-ADV-02	***User journeys are the new sales funnels (and they are often non-linear vs. pipelined)*** *NIMBLE must provide matchmaking on the basis of relevant supply chain partner information, together with relevant product characteristics and possibly, logistics options. (see NIMBLE T5.6)*
PCS-USR-01	***Behaviour design is the new loyalty programme (from lock-in to opt-in)***

	Users must have a convincing B2B workflow User Experience. *(This is at present, a severe weakness of the system!)*
PCS-DAT-01	***Data science is the new business process optimisation*** *The system must have tools to analyse user behaviour during core interactions.* *(see: NIMBLE Task 3.6)*
PCS-DAT-02	***Data science is the new business process optimisation*** *The system must have tools to analyse company behaviour over time* *(see: NIMBLE Task 3.6)*
PCS-DAT-03	***Data science is the new business process optimisation*** *The system must have tools to analyse production data* *(see: NIMBLE Task 3.6)*
PCS-USR-02	***Social feedback is the new sales commission*** *User feedback must be supported directly, must be analysed and should result in trust, reputation and ranking.*
PM-GOV-06	***Algorithms are the new decision makers*** *All algorithmic decision making should be auditable.* *(There are likely to be conflicts of interest concerning the degree of transparency)*
ADV-CFG-01	***Real-time customisation is the new market research*** *With asset and product virtualisation, end consumers can influence actual production and design of new products. Companies should be able to connect configuration tools to the NIMBLE platform*
PCS-API-01	***Plug and play is the new business development*** *There must be a set of API calls to extend NIMBLE functionality without breaking core interaction mechanisms. In NIMBLE, this should be called "plug and create value". The open API and data channels are our current answer.*
PM_GOV_06	***The invisible hand is the new iron fist*** *Since the "invisible hand" also decides whether the playing field is fair to everyone, it should become more visible!□ see above: algorithms must be auditable.*
Viral Growth	
PM_VG_01	*Product and service catalogue items should be accessible by public URLs and indexable for search engines in order to attract outside interest to NIMBLE*
PM_VG_02	*Company descriptions should be accessible by public URLs and indexable for search engines in order to attract outside interest to NIMBLE*
PM_VG_03	*"Units-of-value" could be tenders addressed to players in specific supply chains – in order to qualify for tender they would have to join NIMBLE*
Governance Requirements	

PM-GOV-01	Gate-keeping: the registration process must include checks to ensure that only trustworthy entities join the platform
PM-GOV-02	Process: entities on the platform must have serious intention to use the platform. Trial phases must be possible but must be signaled to others.
PM-GOV-03	Metrics: all metrics used by the platform should be auditable by regulators.
PM-GOV-04	Relational: the values to be shared for NIMBLE platforms are kept up-to-date by an independent regulatory entity that is governed by the NIMBLE mission statement.
PM-GOV-05	Gate-keeping: The platform manager must be able to switch off and remove services that break basic interaction mechanisms of the platform.
Requirements for metrics	
PM-LIQ-01	The platform manager must be able to see the "Liquidity" of the platform as a metric comprising the following figures: • Number of participants (companies) • Number of successfully agreed contracts • Number of successfully fulfilled contracts • Number of companies not having taken part in any contracts Ranking of interaction pairs according to frequency, trading volume, satisfaction level.
PM-MQL-01	The platform manager must be able to assess the matching quality of the platform as a metric comprising the following figures: • Number of successfully agreed contracts • Number of successfully fulfilled contracts • Number of unsuccessful negotiations with no follow-up • Number of unsuccessful negotiations vs agreed contracts Number of fulfilled contracts with quality complaints
PM-P2C-01	The platform manager must be able to assess participation trends on the platform through metrics comprising the following figures: • Number of products offered on the platform • Coverage of eClass and distribution of sales over eClass items • Number and kind of products offered but not sold Number and kind of products sought but not offered
PM-IAF-01	The platform manager must be able to search for root causes of interaction failures through metrics comprising the following information: • For stopped negotiations: which side stopped the negotiation? • For stopped negotiations: what caused stopping the negotiation? • For unfulfilled contracts: which side complained about what? • For unfulfilled contracts: what caused the transaction to fail? The above must be supported by questionnaires to the parties, with "closed" questions (selectable standard options) and "open" questions for analysis by humans or AI techniques.

PM-IAF-02	*The platform manager must be able to assess participation intensity on the platform through metrics collected per company:* • *Number of published catalogue items, over time* • *Number of initiated product or service searches, over time* • *Trading volume as supplier, over time* • *Trading volume as buyer, over time* *Aggregated figures can be used to derive participation intensity vs. platform growth, either in terms of participation or trading volume.*
PM-MAT-01	*The platform manager must be able to assess participation trends on the platform through metrics comprising the following figures:* • *Size of companies joining over time* *Number of companies joining over time*
PM-INN-01	*The platform manager must be able to assess behaviour changes on the platform through metrics comprising the following figures* • *Hot-spots: changes in transactional behaviour of groups* • *Requests for changes, improvements of the platform* • *Interaction types falling into disuse* • *Companies leaving the platform* • *Companies reducing activity on the platform* *Companies strengthening activities outside the platform*
Platform Customer Requirements	
PC-INF-01	*The platform customer should have access to the following* ***general information*** *about prospective business partners:* • *complete details (name, address, sector of activity, etc.), main activity, area of influence, VAT number,* • *Type of company, history and commercial references (other providers / other clients, reputation) the competition, habitual providers and company brief history.* • *Production capacity, turnover, growth expectations.* • *Potential consumption, purchase specifications, machinery, facilities, and production location.* • *Contact information / mail head buyer* • *Quality and safety guarantees* • *Troubleshooting channel*
	The platform customer should have access to the following information about ***Terms and Conditions*** *of the prospective business partner:* • *payment method,* • *packaging, transport,* • *Incoterms,* • *deadlines delivery,* • *delivery address,* • *purchase volume,*

	- *special requirements if they exist,*
PC-INF-03	*The platform customer should have access to the following information about the* ***Economic Situation*** *of the prospective business partner:* - *Balance sheets, current profits, reputation reports,* - *Commercial and financial report, commercial solvency information* - *Solvency and risk classification* - *Payment method*
PC-INF-04	*The platform customer should have access to the following information about the* ***Product Portfolio*** *of the prospective business partner:* - *Type of product, style, complete portfolio of products / services. Product Catalogue with technical data sheets* - *Type of components* - *Operative from Pre-purchase / sale, buy / sell and post-purchase / sale* - *Furniture designs in AutoCAD* - *Price and delivery time per product*

5.6 NIMBLE Requirements Summary

The project requirement summary is given in Table X (below) and includes the following mapping steps, respectively:

STEP 1: Mapping between three categories of the DoA requirements (from Section 5.1): (i) DoA platform requirements, (ii) DoA application requirements and (iii) DoA user requirements;
STEP 2: Mapping D1.1 use case requirements (from Section 5.2) to the requirements summary from step 1;
STEP 3: Mapping of federated ecosystems requirements (from Section 5.3) to the requirements summary from step 2;
STEP 4: Mapping security requirements (from Section 5.4) to the requirements summary from step 3;
STEP 5: Mapping Platform Owner requirements (from Section 5.5) to the requirements summary from step 4.
The following fFigure illustrates the mapping steps in more detail.

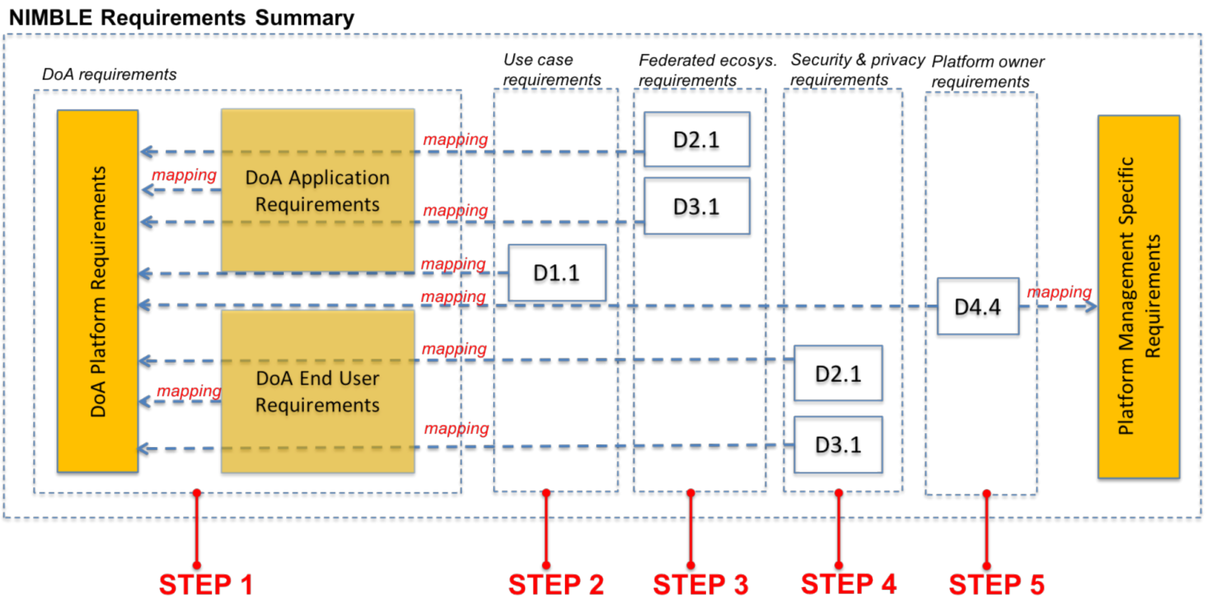
NIMBLE Requirements Summary
DoA requirements
Use case requirements
Federated ecosys. requirements
Security & privacy requirements
Platform owner requirements
DoA Platform Requirements
DoA Application Requirements
DoA End User Requirements
mapping
D2.1
D3.1
D1.1
D4.4
D2.1
D3.1
Platform Management Specific Requirements
STEP 1
STEP 2
STEP 3
STEP 4
STEP 5

Figure: Requirements mapping steps for the NIMBLE Requirements Summary.

Table 16 NIMBLE requirements summary

Platform reqs. (DoA)	DESCRIPTION	Business apps (DoA)	End user reqs. (DoA)	End user reqs. (D1.1)	Federated platform reqs.	Sec. reqs. (D6.1)	Platform owner reqs. (D4.4)
DoA-PL-01	*...federated platform providers give different sectors or regions **a platform instance for B2C, B2B and M2M collaboration**.*	*DoA-APP-17, DoA-APP-12, DoA-APP-10,*	*DoA-UC-12, DoA-UC-19,*		*FED-APP-20, FED-APP-26*		*PCS-DC-01*
DoA-PL-02	*The regional or sectoral platform instance is capable of interoperating with other platforms in the **federation, via semantic interoperability services**.*	*DoA-APP-17, DoA-APP-14, DoA-APP-08,*	*DoA-UC-19, DoA-UC-18, DoA-UC-12, DoA-APP-12*		*FED-APP-20, FED-APP-21, FED-APP-24*	*SEC_CC_04 (handling of sec incidents by CC), SEC_CC_01-3 (encrypted data transfer & app interaction), SEC_IDM_02 (feder. identity. mngm.)*	*PCS-ASV-01, PCS-API-01 ("plug and create value"),*
DoA-PL-03	*Specialisations would be necessary to account for **sector specific practices and standards**...*	*DoA-APP-08*	*DoA-UC-10, DoA-UC-17*				*PCS-DC-01, PCS-UBL-01, PCS-ECL-01,*
DoA-PL-04	*... and localisations may be necessary to deal with **national laws, regional practices** and language preferences.*		*DoA-UC-12, DoA-UC-17*			*FUN-SEC-UC-08 (authen. mechanisms for accessing a repository of normative and legislations), NFUN-SEC-07 (val. of consist. and compliance to legislations)*	*PCS-ADV-01, PM-GOV-05*

DoA-PL-05	NIMBLE objective: To create a platform ecosystem to **attract early adopters**	DoA-APP-16, DoA-APP-07, DoA-APP-02,				NFUN-SEC-08 (usable security)	
DoA-PL-06, DoA-PL-16	NIMBLE objective: To ensure **ease of entry and initial ease of use** with quick rewards	DoA-APP-17, DoA-APP-12, DoA-APP-11, DoA-APP-07, DoA-APP-01			FED-APP-25, FED-APP-26	NFUN-SEC-08 (usable security)	PCS-ASV-01, PCS-BAS-01, PCS-BAS-02, PCS-USR-01
DoA-PL-07	NIMBLE objective: To **grow platform usage** by showing the benefits and by adding services where the need arises	DoA-APP-12, DoA-APP-09, DoA-APP-07, DoA-APP-05,	DoA-UC-04, DoA-UC-05, DoA-UC-06, DoA-UC-10, DoA-UC-11, DoA-UC-12, DoA-UC-20, DoA-UC-21		FED-APP-24	NFUN-SEC-08 (usable security)	Monitoring: PM-ACC-05, PM-ACC-06, PM-ACC-07, Feedback: PM-ACC-08, PM-ACC-09 PCS-ASV-01, PCS-INF-01, PCS-INF-02, PM-LIQ-01
DoA-PL-08	NIMBLE objective: To master the usage of the platform step-by-step to **evolve business cooperation**	DoA-APP-17, DoA-APP-13, DoA-APP-12, DoA-APP-11, DoA-APP-10,	DoA-UC-10, DoA-UC-12, DoA-UC-19		FED-APP-20, FED-APP-21		PCS-ASV-01, PCS-DC-01, PCS-UBL-01, PCS-ECL-01, PM-LIQ-01

		DoA-APP-05, DoA-APP-04					
DoA-PL-09	*NIMBLE objective: To* ***ensure trust, security and privacy.***	*DoA-APP-18, DoA-APP-19*	*DoA-UC-01, DoA-UC-16*	*D1.1-UC-01, D1.1-UC-01_01, D1.1-UC-02, D1.1-UC-03, D1.1-UC-15, D1.1-UC-16*	*FED-APP-01, FED-APP-02, FED-APP-03, FED-APP-22, FED-APP-23*	*All D6.1 security & privacy reqs. with MUST priority: (1) use case-centric sec & pr. reqs. (2) core sec & pr. reqs., (3) platform service provider sec. reqs., (4) cloud service provider sec. reqs.*	*PM-ACC-03, PM-ACC-04,* *From (PM-SEC-01 to PM-SEC-07)* *From (PM-TRUST-01 to PM-TRUST-07), PCS-PRV-01, PCS-BAS-01, PCS-BAS-02, PM-GOV-01*
DoA-PL-10	*Objective 1: Develop the NIMBLE collab. infrastructure with* **core services** *(subscribe, publish/search, negotiate and execute tasks, monitor and control the collab.)*	*DoA-APP-14, DoA-APP-10, DoA-APP-07*	*DoA-UC-04, DoA-UC-05, DoA-UC-06, DoA-UC-07, DoA-UC-08, DoA-UC-09, DoA-UC-13, DoA-UC-15*	*D1.1-UC-01, D1.1-UC-01-01, D1.1-UC-01_02, D1.1-UC-01-03, from (D1.1-UC-02 to D1.1-UC-14)*	*FED-APP-04, FED-APP-05, FED-APP-06, FED-APP-07, FED-APP-08, FED-APP-09, FED-APP-10, FED-APP-11, FED-APP-12, FED-APP-13, FED-APP-14*	*FUN-SEC-UC-01 (sec. access to the platform), FUN-SEC-UC-02 (sec. access to data), FUN-SEC-UC-03 (sec data manipulation), FUN-SEC-UC-04 (secure negotiation), FUN-SEC-UC-05, FUN-SEC-UC-06, FUN-SEC-UC-07*	*PM-ACC-01, PM-ACC-02, PM-ACC-03, PM-ACC-04, Monitoring: PM-ACC-05, PM-ACC-06, PM-ACC-07, Feedback: PM-ACC-08, PM-ACC-09; PM-FED-01,*

							PM-INF-01, PM-INF-02, PM-INF-03, PM-INF-04, PCS-ASV-01, PCS-NEG-01, PCS-NEG-02, PCS-CON-01, PCS-CON-02, PCS-BTX-01, PCS-BTX-02, PCS-INF-01, PCS-INF-02, From (PCS-BAS-01 to PCS-BAS-05), PM-GOV-01
DoA-PL-11	1.1 Establish with stakeholders, the **requirements for core services** of the platform.		From (DoA-UC-01 to DoA-UC-21)	All use case-centric reqs from D1.1 From (D1.1-UC-01 to D1.1-UC-16)		All use case-centric sec & pr. Reqs.: (FUN-SEC-UC-01 to FUN-SEC-UC-08) and (NFUN-SEC-UC-01 to NFUN-SEC-UC-08) and (PRIV-UC-001 to PRIV-UC-004 (privacy compliance with GDPR))	Monitoring: PM-ACC-05, PM-ACC-06, PM-ACC-07, Feedback: PM-ACC-08, PM-ACC-09; Security: From (PM-SEC-01 to PM-SEC-07) Inf. management: From (PM-INF-01 to PM-INF-04),

							PCS-ADV-01, PM-GOV-05
DoA-PL-12	*1.2 Design the* ***top-level architecture and modules****.*	*DoA-APP-11*			*FED-APP-20, FED-APP-21*		
DoA-PL-13	*1.3* ***Use permissive open source software*** *wherever possible.*						
DoA-PL-14	*1.4 Deploy the basic infrastructure with core services, to use case partners*	*DoA-APP-17, DoA-APP-12 ,*	*DoA-UC-12, DoA-UC-13, DoA-UC-15*				
DoA-PL-15	*1.5 Learn from early validation.*						
DoA-PL-17	*2.1 A company can* ***publish its product catalogue*** *in bulk or via semantic product descriptions*	*DoA-APP-01*		*D1.1-UC-05, D1.1-UC-06*	*FED-APP-05, FED-APP-06, FED-APP-07*		*PCS-BAS-03*
DoA-PL-18	*2.2 Two companies can establish* ***private, encrypted information channels*** *for a business collaboration. In NIMBLE phase two, arbitrary supply chains can be established between any number of firms.*	*DoA-APP-05, DoA-APP-17, DoA-APP-11*	*DoA-UC-12,*	*D1.1-UC-15, D1.1-UC-16*	*FED-APP-22, FED-APP-23*	*SEC-CC-01 (data protection), SEC-CC-01-01 (avoid unintended distribution of sensitive data)*	*PCS-PRV-01*

DoA-PL-19	2.3 Services for **matchmaking** between producers and consumers are available to establish business collab. fast.	DoA-APP-13, DoA-APP-04, DoA-APP-03	DoA-UC-04, DoA-UC-05, DoA-UC-06	D1.1-UC-12, D1.1-UC-13, D1.1-UC-14	FED-APP-08, FED-APP-09, FED-APP-10, FED-APP-11, FED-APP-12		PCS-ADV-02
DoA-PL-20	2.4 Gaining mutual benefits from shared information leading to **optimized re-planning**.	DoA-APP-13, DoA-APP-10, DoA-APP-06	DoA-UC-18		FED-APP-14,FED-APP-15, FED-APP-16, FED-APP-18		Monitoring: PM-ACC-05, PM-ACC-06, PM-ACC-07, Feedback: PM-ACC-08, PM-ACC-09; Analytics: PCS-DAT-01, PCS-DAT-02, PCS-DAT-03, PM-GOV-06, ADV-CFG-01
DoA-PL-21	2.5 Data collection, management and **analytics**.	DoA-APP-09, DoA-APP-15, DoA-APP-06	DoA-UC-02, DoA-UC-03, DoA-UC-07, DoA-UC-08, DoA-UC-09, DoA-UC-18, DoA-UC-20, DoA-		FED-APP-14, FED-APP-15, FED-APP-16, FED-APP-18		PCS-INF-01, PCS-INF-02, PCS-DAT-01, PCS-DAT-02, PCS-DAT-03, PM-GOV-06

			UC-21				
DoA-PL-22	Objective 3: Growing the use of the platform	DoA-APP-17	DoA-UC-10				Monitoring: PM-ACC-05, PM-ACC-06, PM-ACC-07, Feedback: PM-ACC-08, PM-ACC-09; PCS-DC-01, PM-LIQ-01, PCS-API-01 ("plug and create value"), PM-VG-01, PM-VG-02, PM-VG-03
DoA-PL-23	3.1 Each of the use cases demonstrates benefits for businesses leading to a "me too" effect	DoA-APP-05, DoA-APP-04	DoA-UC-12, DoA-UC-18				PCS-DC-01, PCS-UBL-01, PCS-ECL-01, PCS-ADV-02, PCS-USR-02, PCS-API-01 ("plug and create value")
DoA-PL-24	3.2 Start early adopter scheme, recruiting external users of the platform.		DoA-UC-10				PM-LIQ-01

DoA-PL-25	*3.3. Provide a core software tool set to initiate the software supply side of the platform.*	*DoA-APP-16, DoA-APP-12, DoA-APP-10, DoA-APP-02,*	*DoA-UC-10,*		*FED-APP-05, FED-APP-06, FED-APP-07, FED-APP-08, FED-APP-09, FED-APP-10, FED-APP-11, FED-APP-12, FED-APP-13, FED-APP-14, FED-APP-15, FED-APP-16, FED-APP-18*		*PM-ACC-02, PM-ACC-03, PM-ACC-04, Monitoring: PM-ACC-05, PM-ACC-06, PM-ACC-07, Feedback: PM-ACC-08, PM-ACC-09; PCS-DC-01, PCS-UBL-01, PCS-ECL-01*
DoA-PL-26	*3.4 Improve business integration between different sectors*	*DoA-APP-17, DoA-APP-16. DoA-APP-12, DoA-APP-11, DoA-APP-08, DoA-APP-02*	*DoA-UC-12,*	*D1.1-UC-12, D1.1-UC-13, D1.1-UC-14*	*FED-APP-10, FED-APP-11, FED-APP-12, FED-APP-13, FED-APP-14, FED-APP-24*	*CIA principles: NFUN-SEC-01, NFUN-SEC-02, NFUN-SEC-03*	*PM-INF-01, PM-INF-02, PM-INF-03, PM-INF-04, PCS-ASV-01, PCS-DC-01, PCS-UBL-01, PCS-ECL-01, PCS-ADV-02, PCS-API-01 ("plug and create value")*
DoA-PL-27	*Objective 4: Enhance platform functionality from*	*DoA-APP-17, DoA-APP-16,*	*DoA-UC-02, DoA-*		*FED-APP-05, FED-APP-06,*		*PM-ACC-01, Monitoring:*

	the core services and ensure that firms master it on their own	DoA-APP-14, DoA-APP-13, DoA-APP-12, DoA-APP-07, DoA-APP-05, DoA-APP-02	UC-07, DoA-UC-08, DoA-UC-09, DoA-UC-11, DoA-UC-13, DoA-UC-15		FED-APP-07,		PM-ACC-05, PM-ACC-06, PM-ACC-07, Feedback: PM-ACC-08, PM-ACC-09; PCS-ASV-01
DoA-PL-28	Objective 5: Ensure trust in the platform	DoA-APP-18, DoA-APP-19	DoA-UC-01		FED-APP-23	All platform service provider sec & pr. reqs., e.g.SEC-PLAT-01 (monitor.), SEC-PLAT-06 (contingency plan.), SEC-PLAT-06 (backup and recovery)	From (PM-TRUST-01 to PM-TRUST-07), PCS-ADV-01, PM-GOV-05, PCS-USR-02
DoA-PL-29	5.1. Support user-adjustable levels of security and privacy & maintain customer trust in balance with ease of use	DoA-APP-18, DoA-APP-19, DoA-APP-07	DoA-UC-01	D1.1-UC-15, D1.1-UC-16	FED-APP-01, FED-APP-02, FED-APP-03, FED-APP-22, FED-APP-23	All core sec & pr. reqs with MUST category, e.g. SEC_ACM02 (access enforc. mechanisms)	PM-ACC-03, PM-ACC-04, From (PM-SEC-01 to PM-SEC-07); PCS-ADV-01, PM-GOV-05, PM-GOV-01, From (PM-TRUST-01 to PM-TRUST-07); PCS-PRV-01

DoA-PL-30	*5.2. The platform will be designed* ***modular and resilient*** *so that security breaches can never "sink the whole ship"*	*DoA-APP-18, DoA-APP-10*				*NFUN-SEC-05 (Reliability - notification services in place)*	*PCS-API-01 ("plug and create value")*
DoA-PL-31	*5.3.* ***Data storage*** *must be entirely at the owner's control - from cloud to storage on personal devices.*	*DoA-APP-15*				*SEC-DIDQ-03-1 (data protection at rest), SEC-DIDQ-03-2 (data protection in shared resources), PRIV-PLAT-01 (data privacy)*	*PCS-PRV-01*
DoA-PL-32	*5.5.* ***Grow trust*** *on the platform by a) fair gain distribution among the platform sides; b) maintaining strict interoperability; c) providing privacy in B2B communication and data exchange*	*DoA-APP-17, DoA-APP-19, DoA-APP-11, DoA-APP-07, DoA-APP-05*	*DoA-UC-01*		*FED-APP-22, FED-APP-23*	*SEC-PLAT-03 (risk assesm.), SEC-PLAT-04 (sec planning), PRIV-PLAT-01 (data privacy), SEC-TRM02 (user reputat.)*	*From (PM-TRUST-01 to PM-TRUST-07), PCS-PRV-01, PCS-USR-02*
DoA-PL-33	*5.6.* ***Information quality*** *will be a fundamental value to be maximised in the platform.*	*DoA-APP-09, DoA-APP-08,*	*DoA-UC-10*			*SEC-DIDQ-02 (data input validation), SEC-DIDQ-03 (data & metadata protection)*	*PM-INF-01, PM-INF-02, PM-INF-03, PM-INF-04,*
	Platform management specific requirements						
	Measuring interactions between participants (from D4.4)						*PM-LIQ-01, PM-MQL-01, PM-P2C-01, PM-IAF-*

							01, PM-IAF-02, PM-MAT-01, PM-INN-01
	Reputation & trust metrics (from D4.4)						*From (PM-TRUST-01 to PM-TRUST-07)*
	Platform customer's search functionality and insight into business characteristics of the potential partners (from D4.4)						*PC-INF-01 (general information), PC-INF-02 (terms & conditions), PC-INF-03 (economic situation), PC-INF-04 (product portfolio)*
	Process: entities on the platform must have serious intention to use the platform. Trial phases must be possible but must be signaled to others. (from D4.4)						*PM-GOV-02*
	Metrics: all metrics used by the platform should be auditable by regulators (from D4.4)						*PM-GOV-03*

	Relational: the values to be shared for NIMBLE platforms are kept up-to-date by an independent regulatory entity that is governed by the NIMBLE mission statement (from D4.4)						*PM-GOV-04*
	Gate-keeping: The platform manager must be able to switch off and remove services that break basic interaction mechanisms of the platform. (from D4.4)						*PM-GOV-05*
	All algorithmic decision making should be auditable (from D4.4)						*PM-GOV-06*

6 Conclusions

At the time of writing D4.5 (in Month 21) we were only just coming to the end of the first experimentation and validation round of NIMBLE, owing to an overall delay in development of approximately 4 months.

The high ambitions of the project, namely to provide a working cloud-based internet platform that includes facilities ranging from product catalogues to business process support, formal representation of contracts and connectivity with shop-floor machinery and sensors for monitoring purposes, were not achievable in the time originally planned. Nonetheless, the development teams did manage to build the required services but had to make compromises partly in terms of detailed functionality and partly in terms of UX ease of use.

The validation phase brought the pain points of the current system clearly into focus and the post-hoc analysis of the full scope of requirements has made it clear to all parties that the infrastructure requirements for building NIMBLE are as important as fulfilling the use case specific expectations and in many cases (as expected) that infrastructure is exactly what moves some use case scenarios from being "specific" and thus, expensive to implement, to "general" and thus, easier to implement thanks to a sufficiently rich infrastructure that is reachable via open API calls. Examples are the data channels, the (future) inclusion of product configurators, and the use of an integrated security model implemented via *keycloak*. Also, the use and adaptation of an open source business process engine (*Camunda*) is an important element of this infrastructure.

An important contribution of D4.5 is the above-mentioned repository of system and user requirements which gives us a handle on managing development in the second phase of the project. The lesson learned here is that stakeholders who are not part of the user population will also not be represented adequately in the requirements documentation. We rectified the notable problem of underrepresentation of the platform owner, by letting the coordinator play the role of platform owner and by introducing a new deliverable (D4.4) to spell out these requirements.

We also learned through the first validation, the weaknesses we had in visually structuring the user interaction and in separating out pure information, from changeable parameters (e.g. in negotiation) and from actionable items (e.g. buttons to proceed to the next step).

By bringing on two additional developers and an interface designer devoted to improving the user experience we have begun to address the issues encountered. Whereas the first version of Release 3 still had mostly the initial interface (albeit improved also), the latest version is already moving to the new UI/UX and this will be fully available in Release 4 (September 2018) when we plan to include external early adopters through the AMBASSADOR programme.

7 Bibliography

Arvola, M. (2014). Interaktionsdesign och UX: om att skapa en god användarupplevelse. Studentlitteratur.

Barut, M., Faisst, W. & Kanet, J.J. (2002). Measuring supply chain coupling: an information system perspective. European Journal of Purchasing and Supply Management, 8(3), 61-171.

Esslinger, H. (2013). Design forward: creative strategies for sustainable change. Arnoldsche Art Publishers.

Fawcett, S. E., Wallin, C., Allred, C., Fawcett, A. M., & Magnan, G. M. (2011). Information technology as an enabler of supply chain collaboration: a dynamic-capabilities perspective. Journal of Supply Chain Management, 47(1), 38-59.

Goodwin, K. (2011). Designing for the digital age: How to create human-centered products and services. John Wiley & Sons.

ISO - International Standards Organization (1998). ISO 9241-11 Ergonomic requirements for office work with visual display terminals (VDTs) Part 11: Guidance on Usability. ISO.

ISO - International Standards Organization (2009). ISO FDIS 9241-210 Human-centred design process for interactive systems. ISO.

ISO - International Standards Organization (2008a). ISO 9241-20: Ergonomics of humansystem interaction – Part 20: Accessibility guidelines for information/communication technology (ICT) equipment and services. Geneva: International Standards Organization.

ISO - International Standards Organization (2008b). ISO 9241-171: Ergonomics of humansystem interaction. Part 171: Guidance on software accessibility. Geneva: International Standards Organization

[NIMBLE-D6.1] D6.1 "Security and Privacy Requirements", (2017). Online available from:https://www.nimble-project.org/wp-content/uploads/NIMBLE-D6.1_submitted.pdf

[NIMBLE-D1.1] D1.1 "Requirements and Collaboration Design for Manufacturing and Logistics in Four European Use Cases" (restricted)

Löwgren, J., & Stolterman, E. (2004). Thoughtful interaction design: A design perspective on information technology. Mit Press.NIMBLE_Proposal-SEP-210334790.pdf

Preece, J., Sharp, H., & Rogers, Y. (2015). Interaction design: beyond human-computer interaction. John Wiley & Sons.Simonsen, J., & Robertson, T. (Eds.). (2012). Routledge international handbook of participatory design. Routledge.

Sahay, B.S. (2003). Supply chain collaboration: the key to value creation. Work Study, 52(2), 76-83,

Tatikonda, M.V. & Stock, G.N. (2003). Product technology transfer in the upstream supply chain. The Journal of Product Innovation Management, 20(6), 444-467.

Väänänen-Vainio-Mattila, K., Roto, V. and Hassenzahl, M. (2008). Towards Practical User Experience Evaluation Methods. In: Proceedings of the International Workshop on Meaningful Measures: Valid Useful User Experience Measurement (VUUM) (eds.) Law, E., Bevan, N., Christou, G., Springett, M. and Lárusdóttir, M.; Institute of Research in Informatics of Toulouse (IRIT) - Toulouse, France.

Appendix A: Method for End users' UX validation of NIMBLE

The validation of the business services in relation to external end-users (SMEs) would provide valuable feedback for future development. The validation process is suggested to be carried out as follows;

What, How, Who do what?

The validation process consists of following steps: Preparation, Set-up, Initiation, Performing, and Termination.

What will be validated?

The aim is to gather the use cases' external end-users' (SMEs) view of NIMBLE concerning UX. The results will contribute to NIMBLE's collaboration and business model development.

Preparation

1. Identify and invite external end-users from relevant SMEs.
2. Preparation and training for interviews.

Setup

The setting for the validation at the use case company must be prepared by arranging:

1. A room.
2. Access to Appendix B (Interview Guide)
3. Prepare for how to document (preferable on computer)
4. One moderator of the validation process (instructor) and preferable one person taking notes.

Initialization

The validation of the NIMBLE-platform and its value starts with informing the external end-user that they will be treated with confidentiality (no specific names and companies will be revealed or disclosed).

Inform of NIMBLE and the purpose with the validation (e.g. the services to be validated (if so), and the themes of questions).

If the NIMBLE demo will be used: a computer with the demo is accessible (so that the demo can be shown).

Performing the interviews

Data gathering from external end-users (SMEs):

The interviewer goes through the interview guide (see below). It is of utterly importance to have follow-up questions and to ask the informants to elaborate and motivate their answers.

Termination

Ask the informants of their overall impressions of the NIMBLE business services and their benefits. Also ask if they have anything to add.

Report results.

Conduct an analysis covering SMEs view as external end-users.

The findings could be taken on board as additional requirements for further development in which value added services will be included in the platform.

Appendix B: Validation Interview Guide – Questions

This step of validation will focus on evaluating the early version of the platform from a user experience perspective. The core business services are validated together with the NIMBLE-platform concepts as a whole. This survey captures the bridge between user experience and the experiences of needs and benefits expected from the platform in order to generate values by the platform. Of importance is to capture the end-users perceived needs and wants in terms of value in relation to business and collaboration models, to ensure NIMBLE's continuity as well as sustainability. (The survey serves as such as a bridge between WP 4 and WP8 as well.)

Start by explaining the NIMBLE-platform and the NIMBLE idea. Then ask;

Context:

1. Where are the users? In which branch? What are the conditions under which they work? What does their business processes look like?

User's view on NIMBLE's idea:

2. What would/could motivate you to start using the NIMBLE B2B-platform?
3. What would/could prevent you from using the NIMBLE platform?

Business services – current:

4. If you would register on NIMBLE:
5. What information do you regard as reasonable to share?
6. Is there any information that you definitely not would share?
7. If you would publish on NIMBLE:
8. What would you like to publish?
9. In what format would you like to publish? (text, pictures)
10. What do you want to be able to search for? (Product | Service | Company | Person-in-role | Configuration)
11. What do you see as possible to negotiate for via a platform?

Business services – wish list:

12. What business processes would trigger your use of NIMBLE?
13. What business processes would you want to get support for in your supply chain?
14. In what ways do you collaborate with other companies/stakeholders?
15. Which of these could be performed in a collaboration platform? (Please give motivation)
16. Which collaboration activities would be most beneficial to perform via a platform such as NIMBLE? (Please give motivation)

NIMBLE collaboration value:

17. What do you regard to be most valuable – rank these (please give motivation):
18. Save time
19. Save money
20. Networking
21. Idea generation
22. Other (please suggest other values)

Areas of improvement:

23. Can you give an example of one of your business processes that is specific problematic today and that could be improved? If so, in what ways?
24. For to strengthen your business, what other kinds of services would you like to see? (Value-added services).
25. In what type of relations?
26. Other functions?
27. How can collaboration be strengthen with NIMBLE?
28. After the project ends, minimum criteria/ function on the platform that would make you use the platform.