

# **D4.4 – Platform User Experience – Platform Manager's Point of View**

| Project Acronym            | NIMBLE   |
|----------------------------|--|
| Project Title              | Collaboration Network for Industry, Manufacturing,<br>Business and Logistics in Europe |
| Project Number             | 723810 (H2020)   |
| Work Package 4:            | Use Case Experimentation, Validation and Evolution                                     |
| D4.4                       | Platform User Experience – Platform Manager's<br>Point of View                         |
| Responsible author         | Wernher Behrendt (SRFG)  |
| <b>Dissemination Level</b> | Public   |
| Contractual Delivery Date  | 31.03.2019   |
| Actual Delivery Date       | 31.03.2019   |
| Version                    | V2.0   |
|                            |  |







# **Table of contents**

| Tał | ole of | contents   | 2   |  |
|-----|--------|--|-----|--|
| Doo | cumei  | nt Information   | 3   |  |
| 1   | Exec   | cutive Summary   | 4   |  |
| 2   | Intro  | oduction   | 5   |  |
| 3   | Requ   | quirements for managing a B2B Internet Platform5             |     |  |
|     | 3.1    | Platform Accountability Requirements                         | 6   |  |
|     | 3.2    | Security Management Requirements                             | 7   |  |
|     | 3.3    | Federation Management Requirements                           | 8   |  |
|     | 3.4    | Trust Management Requirements                                | 8   |  |
|     | 3.5    | Information Management Requirements (Monitoring and Control) | 9   |  |
| 4   | Gov    | ernance Mechanisms and Metrics                               | 9   |  |
|     | 4.1    | "Platform Manifesto"   | 10  |  |
|     | 4.2    | Viral Growth Requirements                                    | 15  |  |
|     | 4.3    | Governance Mechanisms  | 15  |  |
|     |        | 4.3.1 Governance Tools and Algorithms                        | .16 |  |
|     |        | 4.3.2 Applying "Lessons learned" so far, to Governance       | .16 |  |
|     | 4.4    | Management Metrics   | 18  |  |
|     |        | 4.4.1 Requirements for Metrics of the Start-up Phase         | .18 |  |
|     |        | 4.4.2 Metrics for the Growth Phase                           | .18 |  |
| 5   | Busi   | ness Needs of Platform Customers                             | 20  |  |
| 6   | Man    | agement Dashboards available in NIMBLE                       | 21  |  |
| -   | 6.1    | User Activity Report   | 21  |  |
|     | 6.2    | Service Health Report  | 22  |  |
|     | 63     | Security Dashboard   | 22  |  |
|     | 64     | Log Analysis Desk  | 23  |  |
| 7   | Vali   | dation of the Management Facilities of NIMBLE Release 7      | 24  |  |
|     | 7.1    | Platform Accountability - Validation                         | 24  |  |
|     | 7.2    | Security Management - Validation                             | 25  |  |
|     | 7.3    | Federation Management - Validation                           | 25  |  |
|     | 74     | Trust Management - Validation                                | 26  |  |
|     | 7.5    | Information Management - Validation                          | 26  |  |
|     | 7.6    | Governance Mechanisms - Validation                           | 27  |  |
|     | 77     | NIMBLE Platform Management Metrics - Validation              | 27  |  |
| 8   | Con    | rusions  | 29  |  |
| 9   | Refe   | rences   | 29  |  |
| -   |        | ~  |     |  |



# **Document Information**

| Project                      | NIMBLE (H2020-723810)   |  |
|------------------------------|---|--|
| Identifier                   | NIMBLE-D4.4   |  |
| Author(s):                   | SRFG  |  |
| Document title:              | Validation Report – Platform Manager's Point of View  |  |
|                              |   |  |
| Source Filename:             | NIMBLE_D4_4_Validation_Platform_manager_PoV_v2.0.docx   |  |
| Dissemination level          | Public  |  |
| Document context information |   |  |
| Work package/Task            | WP4 – Use case experimentation, validation and evolution                                      |  |
| Responsible person and       |   |  |
| project partner:             | Wernher Behrendt (SRFG)   |  |
| Quality Assurance / Review   |   |  |
| Name / QA / Release /        | Michael Nilsson (LTU)   |  |
| Citation information         |   |  |
| Official citation            | NIMBLE Consortium (2019), D4.4 NIMBLE Validation Report<br>– Platform Manager's Point of View |  |
|                              |   |  |

#### **Document History**

| V   | Name     | Date       | Remark   |
|-----|----------|------------|--|
| 0.1 | SRFG/wb  | 10/05/2018 | Basic structure and analysis of platform manifesto |
| 0.2 | SRFG/wb  | 30/05/2018 | Using findings from Ambassador questionnaire       |
| 0.3 | SRFG/wb  | 22/06/2018 | Validation of current P/F manager's functionality  |
| 0.4 | SRFG/wb  | 26/06/2018 | Refinement of high-level metrics                   |
| 0.5 | SRFG/vdb | 30/06/2018 | Cross-indexing with D4.5 Requirements Repository   |
| 0.6 | SRFG/wb  | 01/07/2018 | Validation write-up                                |
| 0.7 | SRFG/wb  | 02/07/2018 | Inclusion of final comments                        |
| 0.8 | SRFG/wb  | 04/07/2018 | Final edits  |
| 1.0 | SRFG/wb  | 05/07/2018 | Submission of V1.0 for Review 2018                 |
| 2.0 | SRFG/wb  | 29/03/2019 | Revision according to review findings 2018         |

#### **Copyright Notice**

This document contains material, which is the copyright of certain NIMBLE consortium parties, and may not be reproduced or copied without permission. The commercial use of any information contained in this document may require a license from the proprietor of that information. Neither the NIMBLE consortium as a whole, nor a certain party of the NIMBLE consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and accepts no liability for loss or damage suffered by any person using this information.

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.



# 1 Executive Summary

Most Internet Platforms are built to exploit digitalisation as a means of drastically reducing transaction costs that before the emergence of the platform, were considered "givens" in the respective market.

The notion of (technology) platforms emerged in the 1990s when economists observed various market phenomena of the expanding ICT markets, e.g. a certain standardisation in computer peripherals in order to co-create and co-innovate in ecosystems ranging from microprocessor manufacturers to memory manufacturers and builders of storage devices, graphics cards, etc.

The more recent notion of platforms moves from the hardware realm to the purely softwarepowered platform that not only creates its own ecosystem, but also plays the role as market place as well as market actor, which creates a potential conflict of interest with other market actors who may not have a say in how to shape the market place. To deal with this conflict of interest and with other possible imbalances in these artificially created markets, platforms establish governance rules whose aim it is to balance the interests of the actors on the platform.

In this deliverable, we present the point of view of a manager of a NIMBLE platform, who is on the one hand, responsible for the success of that platform (success being defined by whoever owns the platform) and on the other hand, also responsible for those participants who have taken a stake in the platform by investing time and effort to be able to interact with others on the platform.

That platform manager is interested in ensuring accountability, security, trust, monitoring and control and – special in NIMBLE – in being able to connect to similar platforms to form a loose federation of specialised market places. Apart from the above, the manager has further requirements concerning success factors of platforms and depending on the maturity of the platform, different metrics need to be used as KPIs to assess whether the platform is becoming a success or whether it is in danger of losing its participant base.

At a high level, the manager is also interested in the pain points of the customers because these are the places where the platform may add value through addressing these pain points.

For the NIMBLE development team, the challenge is to not only create the interaction capabilities of the platform for the customers by e.g. implementing the execution of standardised business processes, but also to create the machinery that will allow the platform manager to exert power in the form of applying governance rules to the platform. Therefore, the initial management dashboards are not very sophisticated yet, because more effort went into developing primary customer-facing tools. In line with this, our initial validation was a pen-and paper exercise going through the requirements collected in sections 3 to 5 and determining whether there exists an implementation and to assess its usability.

With the dashboards being mainly informative, but not supporting any larger degrees of interaction, validation was mainly determining the existence of features and less so, the usability and user-friendliness of the user interface. It is important to point out that this initial validation will be the basis for implementation of further management functionality, and that this document combines requirements capture and validation, making it the reference point for all issues related to NIMBLE platform management.



# 2 Introduction

This deliverable was originally not planned for NIMBLE, because the original plan focused on the roles of the user companies while the role of the platform provider was assumed to be a "given". As our understanding of the workings of Internet Platforms grew, we realized the importance of Platform Governance and that much of the success of such a platform rests on how well the behaviour of users can be firstly, monitored and secondly, managed – if necessary through changes in the interactions between the communities that participate in a multisided platform. We therefore restructured the set of deliverables in WP4 as follows: the original D4.4 (Logistics providers' point of view) was merged into D4.3 to make space for a validation from the "Platform Manager's point of view".

Also, since the project does not have specific platform providers as partners in the consortium, this aspect was under-represented in the requirements phase. The present deliverable rectifies this problem by covering three aspects:

- 1. The *requirements* of a NIMBLE platform provider and manager.
- 2. The design and implementation of a platform managers' dashboard or control room.
- 3. A validation of Release 3 of the platform, from a platform manager's point of view.

Requirements for platform management were stated in several places, starting with the original proposal, a short section in D1.1 (use case requirements) and conclusions from workshops with early adopter companies. Further requirements came from the extensive literature on Internet Platforms, where many aspects are covered under the theme of platform governance. In sections 3, 4,and 5 of this deliverable, we collect all of these requirements to have them in one place. Section 6 presents the functionality that is currently implemented in support of platform management tasks and section 7 gives a critical appraisal of these tools at present and indicates what will need to be done beyond the current state of play.

The requirements presented in V2.0 of this deliverable have been synchronized with the overall requirements list presented in D4.5 (Validation Summary) and mapped to functionality offered by the platform or planned for releases after R3.0 (June 2018).

# **3** Requirements for managing a B2B Internet Platform

We distinguish the following groups of requirements for the Platform Manager:

- Accountability Requirements
- Security Management Requirements
- Federation Management Requirements
- Trust Management Requirements
- Information Management Requirements (Monitoring and Control)

In the following subsections, each group is briefly described and then further refined into lower level requirements. From those, a translation into development issues or a mapping to existing functionality should be possible.

## 3.1 Platform Accountability Requirements

The platform owners may be held responsible for the actions of organisations using the platform unless they can prove that they exercise due diligence in managing user organisations and their behaviour. In order to exercise this due diligence, a number of things must be known through direct inspection or must be derivable from data trails left by the actors. The following three higher level descriptions illustrate the range of platform management tasks and the tables that follow, break these up into concrete requirements.

#### Audit (Transactions) of-Company (Buyer, Supplier, 3<sup>rd</sup> Party)

The platform manager should be able to review transactions between parties for the purposes of security or compliance audits. The possible depth of insight must be specified by applicable law (e.g. GDPR in Europe) and by governance rules given by the platform.

#### Show platform dashboard (# of Companies, # of Transactions, Trading Volume, ...)

The platform manager should be able to view important metrics of the platform in order to do business assessments relating to the economic strength of the platform. Applicable law and governance rules of the platform should ensure a fair balance of power between the platform owners and the platform users.

# Manage user feedback (all user-facing functions should provide usability statistics and a back-channel to the development team)

The platform's customer support should have access to usability metrics gathered from the users of the platform, for the purpose of improving the user experience. The users should have a direct feedback-channel to the platform's customer support.

| PM-ACC-01 | Keep a registry of users that can be (re-)connected to official records if nec-<br>essary (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, paying, etc)   |
| PM-ACC-03 | Provide a taxonomy of user roles associated with business transaction types  |
| PM-ACC-04 | Keep a registry of user actions: user U <i>acting_for</i> firm F in role R doing ac-<br>tion A at time T<br>[acting_for(U.F.R.A.T)]                                      |
|           | Keeping this type of information has privacy implications and requires data anonymisation  |
| 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<br>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)                                  |

Note: a business transaction (on the platform) is any single service that the platform provides and that a user company would view as a "unit of value". E.g. searching for a supplier of some



product is a service; closing a deal after some negotiation is a service; monitoring a production machine is a service; etc.

## 3.2 Security Management Requirements

Security has to be managed at four levels:

- Cloud services
- Platform services
- Participant company level
- Participant user level

Here, we focus on those security aspects that must be managed at platform level and that can neither be delegated upwards, to the cloud provider, nor down, to the participant company or user level. A very important group of requirements is connected to GDPR: since the platform gathers user and company it is a *data processor* and therefore subject to GDPR.

| 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              |
| (NFR)     | 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 man-          |
| (NFR)     | agement; 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.                      |

Note that the above list shows only the perspective of the platform manager and that a much larger number of security requirements has actually been collected in WP6 (Security). For a consolidated mapping of requirements over the whole project, we refer readers to deliverable D4.5. Section 5 of that deliverable is devoted to a tabular consolidation of all requirements that were specified in the first phase of the NIMBLE project. That consolidated list shows mappings between equivalent or similar requirements coming from the DoA, from the use cases, from the platform manager, and from analyses of technical specifications of the backend services for existing Internet Platforms.

## **3.3 Federation Management Requirements**

It is foreseen in the design of NIMBLE that platforms instances need to be kept interoperable in order to strengthen the notion of an eco-system in which social and socio-economic values are shared. There is an open API that supports collaboration between different NIMBLE-based platform instances, as well as connection with third party services.

| PM-FED-01 | The NIMBLE Open API must, as a minimum requirement, support search,       |
|-----------|---|
| (NFR)     | negotiation, contracting and fulfilment across platform instances of NIM- |
|           | BLE.  |

Further, more detailed federation management requirements can be found in D2.1.2 (2018) and – as mappings – in the summary of all NIMBLE requirements, in D4.5, Section 5.

### 3.4 Trust Management Requirements

Trust measures and trust algorithms are dealt with in the on-going task T6.3. From a high level view, the platform manager is interested in the following trust measures:

- Overall trust-level of users in "their" platform
- Trust perception of non-users, vis-à-vis the platform (e.g. likelihood of joining)
- Binary trust measures (company to company)
- Trust asymmetries: 1-to-1, group-to-group (e.g. manufacturers vs. logistics providers)
- Quality of negotiation (from initial query to closed contract)
- Quality of contract fulfilment (compared with agreed terms)
- Quality of information exchange (possibly also exchanges to/with users outside)

| PM-TRUST-01 | There must be an algorithm that measures an overall level of trust for<br>the platform. Can possibly be done as a confidence rating for a transac- |
|-------------|--|
|             | tion 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.  |
| PM-TRUST-03 | There must be an algorithm to calculate the trust level between 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   |
|             | should be perceived as a constituency of highly trustworthy partners   |
|             | and the metrics must objectively measure that level of trustworthiness.  |



#### 3.5 Information Management Requirements (Monitoring and Control)

The need to manage information flows leads to the following requirements:

- 1. At the level of companies, technical administrators should be able to connect digital output of machine sensors, to the data channel functionality so that the contractual data channel management is supported.
  - (Cross-reference to data channel requirements)
- 2. Also at the level of companies, local management should be able to monitor which data channels are open, and should be able to control them (i.e. open/close).
- 3. At the level of platform management, the platform manager should also have the ability to monitor and control such information flow. This is needed e.g. for the case where breaches of security at local level are putting other users and the platform itself, at risk.

Implementationally, information channels can be used for M2M, O2O (software objects, e.g. through API calls), and B2B communication. For the platform manager it must therefore be possible to monitor and control these channels in a case of emergency. At the same time, access to these functions must be audited and restricted in order to avoid misuse. For M2M and O2O information channels, it is unclear whether the platform manager needs any management rights. However, where B2B information channels are involved (i.e. via NIMBLE), the Platform Manager's responsibilities do require these rights.

| 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-3  | Any intervention in B2B processes at Platform level must be auditable   |  |

Declaring connectivity between sensors and machines at local level in order to later connect them to NIMBLE-supported business processes requires NIMBLE to keep a map of assets of that company. This is – according to current design – an element of NIMBLE that would run locally, as an adapter between the platform API and any local ERP/MES. Therefore, there is a need for an *asset virtualisation framework* that helps NIMBLE to keep maps of local edge devices and their connectivity with NIMBLE.

| PM-INF-4 | 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 monitor-able    |
|          | and past connectivity must be accessible through logs.              |

# **4** Governance Mechanisms and Metrics

The notion of "platforms" is by no means new, and it typically involves some form of technological standardisation and modularization in order to make it feasible for third parties to invest in additional products that will be interoperable with the platform and thus strengthen the ecosystem of the platform.

Gawer & Cusumano (2002) give the example of Intel's development of the PCI bus (Peripheral Component Interface) to make it possible for third parties to develop add-ons such as sound cards and graphics cards. A leading technologist of Intel at that time in the 1990s

pointed out that Intel were dependent on external innovation in order for Intel's own innovations to even give value to end customers.

Ballon & van Heesvelde (2011) are among the first to point at the regulatory issues that need to be considered in conjunction with ICT platforms. They propose a typology of platforms along two dimensions: control (or not) over assets; control (or not) over customers. This gives rise to four types of platform:

- Neutral: no control over assets and no control over customers (e.g. PayPal)
- **Broker**: no control over assets, but control over customers (e.g. eBay)
- Enabler: control over assets, but no control over customers (e.g. Intel)
- Integrated: control over (most) assets and control over customers (e.g. iPhone)

According to the above classification, we would see NIMBLE as an enabler platform with some integrator capabilities because it has control over most of the assets, but is by and large, agnostic about the customers. However, since joining the platform does require a certain investment on the part of the customer, there is also a degree of control over the customer. Evans and Gawer (2016) offer a different taxonomy, distinguishing between:

- **Transaction platforms** a technology, product or service that acts as a conduit (or intermediary) facilitating exchange or transactions between different users, buyers, or suppliers.
- **Innovation platforms** a technology, product or service that serves as a foundation on top of which other firms (loosely organized into an innovative ecosystem) develop complementary technologies, products or services.
- Integrated platforms a technology, product or service that is both a transaction platform and an innovation platform. This category includes companies such as Apple, which has both matching platforms like the App Store and a large third-party developer ecosystem that supports content creation on the platform.
- **Investment platforms** Investment platforms consist of companies that have developed a platform portfolio strategy and act as a holding company, active platform investor or both.

With its focus on business processes in supply chains, NIMBLE would qualify as a *transaction* platform with significant provisions to be also an *innovation* platform.

### 4.1 "Platform Manifesto"

In the Internet Platform literature of today, hardware is not at the focus of attention, but rather, social interactions that are enabled by networked services, irrespective of the communication devices. This has led to some important abstractions that are also relevant for NIM-BLE. Choudary (2015) describes a number of characteristic features of platforms in his "Platform Manifesto" (Choudary 2015, p35-47). We have taken the theses from this manifesto and mapped them to NIMBLE. This gives us a starting point to assess whether as a platform, NIMBLE is on the right path and whether we can e.g. influence the actors on the platform in order to induce "good governance". The following table is the result of this exercise:



| <b>Platform Manifesto Thesis</b> | Where in NIMBLE?  |
|----------------------------------|---|
| The ecosystem is the new         | Asset virtualisation helps to optimise the size of physical in- |
| warehouse                        | ventories – NIMBLE data channels enable transparency over       |
|                                  | multi-level supply chains                                       |
| The ecosystem is also the        | Ready-made business processes to be executed partly auto-       |
| new supply chain                 | matically   |
| The network effect is the        | We offer core interactions and services – however, the net-     |
| new driver for scale             | work effects are yet to be seen on NIMBLE                       |
| Data is the new dollar           | Data as a means of reducing transaction cost for the commu-     |
|                                  | nity – NIMBLE has a cautious approach in light of pri-          |
|                                  | vacy/security concerns  |
| Community management is          | Has to be organised for each platform instance separately –     |
| the new human resources          | we should identify interaction mechanisms that can be sup-      |
| management                       | ported across platforms   |
| Liquidity management is the      | Inventories can be kept small if supply and demand are bal-     |
| new inventory control            | anced – the platform can mediate to achieve this balance        |
| Curation and reputation are      | Reputation and trust measures, metrics and rankings to foster   |
| the new quality control          | good governance   |
| User journeys are the new        | NIMBLE is potentially disruptive here: current linear supply    |
| sales funnels (and they are      | chains are fixed because of trust amongst established part-     |
| often non-linear vs. pipe-       | ners and high risk / friction of changing supply chain.         |
| lined)                           |   |
| Distribution is the new des-     | Not actively supported in NIMBLE. In B2B scenarios, this        |
| tination (users are reachable    | aspect may be less influential, but it may also be that we      |
| by more than one channel)        | have not understood it yet, here.                               |
| Behaviour design is the new      | In NIMBLE subject to experimentation – at present, (Re-         |
| loyalty programme (from          | lease 2 of 8), users are not sufficiently attracted by the user |
| lock-in to opt-in)               | experience. Releases 3-4 should tell us more.                   |
| Data science is the new          | We partially agree: data science is a tool to analyze behav-    |
| business process optimisa-       | iour in value networks. However, it needs a sufficient scale    |
| tion                             | of interactions not yet reached here.                           |
| Social feedback is the new       | We agree and therefore, social feedback should be made          |
| sales commission                 | measurable in trust, reputation and ranking.                    |
| Algorithms are the new de-       | We agree. This is crucial because the algorithms not only       |
| cision makers                    | govern individual behaviour, they also define whether the       |
|                                  | playing field is level or not.                                  |
| Real-time customisation is       | We agree. The actual measures of customisation will differ      |
| the new market research          | from one platform instance to another, and should not lead to   |
|                                  | the closing-off from the rederation.                            |
| Plug and play is the new         | This may be true for pure data and digital content platforms.   |
| business development             | In the world of manufacturing, plug and play has to include     |
| The invisible hand is the        | We agree And again because the "invisit le hered" also 1        |
| new iron fist                    | we agree. And again, because the invisible hand also de-        |
|                                  | bacoma mora visibla   |
|                                  | Decome more visible!  |

The platform manifesto is a good starting point for consideration of the overall scope of functionalities that an Internet Platform like NIMBLE would have to address. We derive the following high level requirements from it:



| Platform Manifesto Thesis       | Resulting High Level Requirements for NIMBLE                        |
|---------------------------------|---|
| The ecosystem is the new        | Asset virtualisation (in the form of semantic models)               |
| warehouse                       | NIMBLE data channels (transparency over supply chains)              |
| The ecosystem is also the new   | UBL and seClass based business processes can be exe-                |
| supply chain                    | cuted partly automatically  |
| The network effect is the new   | Negotiation and business transactions must be supported             |
| driver for scale                | as core interactions.   |
| Data is the new dollar          | Information needs in a platform are high in order to reduce         |
|                                 | friction, but must be moderated in NIMBLE, by European              |
|                                 | legislation and legitimate IPR concerns of firms                    |
| Community management is         | Basic interaction mechanisms must be supported across all           |
| the new human resources         | platforms. Specialised interactions will be needed but              |
| management                      | should not "break" the basic interaction mechanisms.                |
| Liquidity management is the     | Inventories can be kept small if supply and demand are              |
| new inventory control           | balanced – the platform should provide mechanisms to                |
|                                 | achieve this balance, e.g. by tracking and tracing of goods.        |
| Curation and reputation are     | Reputation and trust measures, metrics and rankings to              |
| the new quality control         | foster good governance $\rightarrow$ see trust; see governance.     |
| User journeys are the new       | NIMBLE must provide matchmaking on the basis of rele-               |
| sales funnels (and they are of- | vant supply chain partner information, together with rele-          |
| ten non-linear vs. pipelined)   | vant product characteristics $\rightarrow$ see information needs of |
|                                 | platform customers.   |
| Distribution is the new desti-  | This aspect is particularly true for informational goods. In        |
| nation (users are reachable by  | B2B scenarios, this aspect <i>may</i> be less influential, but it   |
| more than one channel)          | may also be that <i>we have not understood it yet</i> , here.       |
| Behaviour design is the new     | At present, (Release 2 of 8), users were not attracted by           |
| loyalty programme (from         | the user experience. The overarching requirement is to              |
| lock-in to opt-in)              | achieve a convincing B2B workflow User Experience.                  |
| Data science is the new busi-   | The system must have tools to analyse user behaviour dur-           |
| ness process optimisation       | ing core interactions.  |
| Social feedback is the new      | User feedback must be supported directly, must be ana-              |
| sales commission                | lysed and should result in trust, reputation and ranking.           |
| Algorithms are the new deci-    | All algorithmic decision making should be auditable.                |
| sion makers                     | (There are likely to be conflicts of interest concerning the        |
|                                 | degree of transparency)   |
| Real-time customisation is the  | With asset and product virtualisation, end consumers can            |
| new market research             | influence actual production and design of new products              |
| Plug and play is the new busi-  | In NIMBLE, this should be called "plug and create value".           |
| ness development                | The open API and data channels are our current answer.              |
| The invisible hand is the new   | Since the "invisible hand" also decides whether the play-           |
| iron fist                       | ing field is fair to everyone, it should become more visi-          |
|                                 | $ble! \rightarrow$ see above: algorithms must be auditable.         |

From the above high-level requirements in the right-hand column, we now derive requirements for platform core services (PCS-xxx-nnn) or other requirements, e.g concerning governance (GOV-yyy-nnn). In small print, we keep the manifesto thesis that triggered the requirement, in order to trace the requirements definitions.



| PCS-ASV-01<br>The ecosystem is the new<br>warehouse                            | Users must be able to achieve asset virtualisation in order to auto-<br>mate information flows in business transactions.  |
|--|---|
| PCS-DC-01<br>The ecosystem is the new<br>warehouse                             | NIMBLE must provide data channels for informational exchange at M2M, O2O and B2B levels, for transparency over supply chains.   |
| PCS-UBL-01<br>The ecosystem is also the<br>new supply chain                    | UBL and eClass based business processes can be executed partly automatically  |
| PCS-ECL-01<br>The ecosystem is also the<br>new supply chain                    | UBL and <b>eClass</b> based business processes can be executed partly automatically   |
| PCS-NEG-01<br>The network effect is the<br>new driver for scale                | Users must be able to engage in business negotiations that lead to formal contracts.  |
| PCS-NEG-02<br>The network effect is the<br>new driver for scale                | Users must be able to close items of agreement in an iterative man-<br>ner. Closed items of agreement shall be called clauses of a contract.  |
| PCS-CON-01<br>The network effect is the<br>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<br>The network effect is the<br>new driver for scale                | Users must be able to view each element of agreement in a contract.<br>These elements of agreement shall be called <b>clauses</b> of the contract.  |
| PCS-BTX-01<br>The network effect is the<br>new driver for scale                | Users must be able to specify an execution plan for a business trans-<br>action. NIMBLE shall provide default execution plans for standard<br>business transactions.  |
| PCS-BTX-02<br>(NIMBLE T5.6: Agent supported negotiation)                       | Given a company policy, a NIMBLE agent should be able to par-<br>tially automate the negotiation and execution of standard business<br>transactions.  |
| PCS-INF-01<br>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<br>Data is the new dollar   | The platform needs to share a good proportion of behavioural data<br>with the data subjects in order to support value creation  |
| PCS-PRV-01<br>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<br>Community management is<br>the new human resources<br>management | User registration: All users must first be registered before any activ-<br>ity can be done, except for search in public catalogues (can be done<br>anonymously)   |
| PCS-BAS-02<br>Community management is<br>the new human resources<br>management | Company registration: All companies must first be registered before<br>they can become active on the platform   |
| PCS-BAS-03<br>Community management is<br>the new human resources<br>management | Catalogue publishing: A company must be able to publish a product<br>or service catalogue   |
| PCS-BAS-04<br>Community management is<br>the new human resources<br>management | <ul> <li>Entity search: a registered user from a registered company must be able to search for:</li> <li>Companies</li> <li>Products</li> <li>Services</li> <li>Users in specific roles (e.g. contacting the sales person)</li> </ul> |



| PCS-BAS-05<br>Community management is<br>the new human resources                           | Contract negotiation: a registered user from a registered company<br>must be able to engage in a contract negotiation leading to a closed<br>deal, in the case of mutual agreement.  |
|--|--|
| management   |  |
| PCS-ADV-01<br>Community management is<br>the new human resources<br>management             | Specialised interactions: when new interactions are designed then<br>they must either be defined via UBL constructs or via the NIMBLE<br>open API. Advanced services that break the basic interaction mech-<br>anisms may be disabled by the platform owner $\rightarrow$ cross-reference<br>with PM-GOV-05. |
| Liquidity management is<br>the new inventory control                                       | Measuring high quality interactions between participants $\rightarrow$ cross-reference PM-LIQ-01   |
| Curation and reputation are<br>the new quality control                                     | Reputation and trust: metrics and rankings to foster good govern-<br>ance $\rightarrow$ cross-reference trust; governance; information quality   |
| PCS-ADV-02   | NIMBLE must provide matchmaking on the basis of relevant sup-  |
| User journeys are the new<br>sales funnels (and they are<br>often non-linear vs. pipe-     | ply chain partner information, together with relevant product char-<br>acteristics and possibly, logistics options.  |
| lined) NIMBLE T5.6   |  |
| Distribution is the new des-<br>tination (users are reachable<br>by more than one channel) | This aspect is particularly true for informational goods. In manufac-<br>turing B2B scenarios, this aspect <i>may</i> be less influential, because<br>physical goods still need to be physically moved to destinations.  |
| PCS-USR-01   | Users must have a convincing B2B workflow User Experience  |
| Behaviour design is the new  | (This is at present a severe weakness of the system!)  |
| loyalty programme (from lock-in to opt-in)   | (This is at present, a severe weakness of the system?)   |
| PCS-DAT-01   | The system must have tools to analyse user behaviour during core   |
| Data science is the new  | interactions   |
| business process optimisa-<br>tion (NIMBLE Task 3.6)                                       |  |
| PCS-DAT-02   | The system must have tools to analyse company behaviour over   |
| Data science is the new<br>business process optimisa-<br>tion (NIMBLE Task 3.6)            | time   |
| PCS-DAT-03   | The system must have tools to analyse production data  |
| Data science is the new<br>business process optimisa-<br>tion (NIMBLE Task 3.6)            | The system must have tools to analyse production data  |
| PCS-USP-02   | User feedback must be sunnorted directly, must be analysed and   |
| Social feedback is the new sales commission  | should result in trust, reputation and ranking.  |
| PM-GOV-06  | All algorithmic decision making should be auditable.   |
| Algorithms are the new de-<br>cision makers  | (There are likely to be conflicts of interest concerning the degree of transparency)   |
| ADV-CEG-01   | With asset and product virtualisation end consumers can influence  |
| Real-time customisation is   | actual production and design of now products. Companies should be  |
| the new market research  | able to connect configuration tools to the NIMBLE platform   |
| PCS-API-01   | There must be a set of API calls to extend NIMRI E functionality   |
| Plug and play is the new   | without breaking core interaction mechanisms. In NIMRIE this   |
| business development   | should be called "nlug and graate value". The anan ADI and date  |
|  | shound be cance plug and create value. The open AFT and data   |
| The invisible based in the   | channels are our current answer.   |
| new iron fist  | Since the "invisible hand" also decides whether the playing field is   |
|  | tair to everyone, it should become more visible! $\rightarrow$ see above: algo-  |
|  | rithms must be auditable. Cross-reference: PM-GOV-06   |



## 4.2 Viral Growth Requirements

In order to ensure growth of the NIMBLE platform we design interactions that make the use of the platform attractive to manufacturing SMEs. Our potential market is at this stage, clearly outside of the NIMBLE platform and for any growth to occur, we need incentives for companies to join NIMBLE.

Choudary (2015, p272) reduces viral growth to four fundamental questions which should be addressed by the design of the platform and its interactions:

- 1. *Sender incentives* why will users spread the word about the platform? The underlying design question is how users can send units of value out of the platform, to other networks?
- 2. *Spreadable core value unit* what is the minimal transferable unit that can be moved to an external network?
- 3. *External network* where will the unit of value from the platform meet current non-users outside the platform?
- 4. *Recipient incentives* why will a non-user on an external network convert to a user on the platform?

At present, planned-for minimal transferable units in NIMBLE are the product/service descriptions published as company catalogues; manufacturing capabilities described in the company profile; compliance with standards and best practice (e.g. certificates of origin or PPAP level compliance) and quality and trust assessments given by customers and by the platform if it acts as an objective critic of all participants.

| PM-VG-01 | Product and service catalogue items should be accessible by public URLs<br>and indexable for search engines in order to attract outside interest to<br>NIMBLE |
|----------|---|
| PM-VG-02 | Company descriptions should be accessible by public URLs and indexa-  |
|          | ble for search engines in order to attract outside interest to NinibLE  |
| PM-VG-03 | "Units-of-value" could be <u>tenders</u> addressed to players in specific supply  |
|          | chains – in order to qualify for tender they would have to join NIMBLE  |

## 4.3 Governance Mechanisms

Based on the metrics gathered from the platform, the platform manager needs to be able to steer behaviour of groups towards some – possibly dynamic – optimum. The platform literature suggests to follow certain principles and among these are:

- Always create value for the customers you serve
- Don't use your power to change the rules in your favour
- Don't take more than a fair share in the wealth created by the platform

Good governance should minimise damage from market failures. Four types of market failure can occur

- Information asymmetry, e.g. fake branded goods
- Externalities, i.e. dynamics that are beyond the platform manager's direct control these can be positive (gain) or negative (loss)



- Monopoly power, when one side of the market becomes too dominant
- Rise in risk, increasing the uncertainty whether interactions will end badly or well

#### 4.3.1 Governance Tools and Algorithms

Tools for Governance are typically laws, norms, architecture of the platform, and the set-up of markets. In data-driven platforms, an increasing number of laws and norms can be algorithmically enforced.

Tiwana (2014, p.119) distinguishes three dimensions of platform governance:

- 1. Division of authority and responsibilities between platform owner and app developers
- 2. Control over accepting or rejecting apps (in the case of NIMBLE, kinds of businesses)
- 3. Pricing policies, i.e. how to share the value created via the platform

Tiwana also distinguishes four control mechanisms that are available for Governance:

- Gatekeeping predefined criteria who can join the platform
- Process incentives for desirable behaviour; requires reliable monitoring
- Metrics to measure performance targets; metrics must be objective
- Relational shared values between platform owner and platform constituency

| PM-GOV-01 | Gate-keeping: the registration process must include checks to ensure that<br>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 regula-<br>tors.   |
| PM-GOV-04 | Relational: the values to be shared for NIMBLE platforms are kept up-<br>to-date by an independent regulatory entity that is governed by the NIM-<br>BLE mission statement. |
| PM-GOV-05 | Gate-keeping: The platform manager must be able to switch off and re-<br>move services that break basic interaction mechanisms of the platform.                             |

This leads us to the following governance requirements:

As can be seen, the requirements for governance range from algorithmically enforceable methods to organisational measures and even to external regulatory entities.

#### 4.3.2 Applying "Lessons learned" so far, to Governance

**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. A process for this is outlined and reported in this section.

**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 JIRA for the management of software development issues, in weekly to monthly sprints.
- 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.

## 4.4 Management Metrics

Although *membership figures* can be misleading, they do give the platform owner some indication of the market that the platform is in principle, already able to reach. However, the most relevant figures are those that measure *activity on the platform*. In particular, the rate of *interaction success* will indicate whether the platform creates value for the participants. Therefore, any metrics connected with *contributing factors* to successful interactions need to be taken into consideration.

#### 4.4.1 Requirements for Metrics of the Start-up Phase

According to Parker et al (2016) platforms in the start-up phase need to focus on a high rate of high quality interactions between a growing number of participants. The relevant metrics are **Liquidity** – possibly still with a small number of participants, but with a high interaction rate; **Matching quality** – which needs excellence in product/service curation; and **Trust** with the aim of minimising risk for the participants. e.g. through reviews.

| 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)  |  |  |  |  |
|           | <ul> <li>Number of successfully agreed contracts</li> </ul>                 |  |  |  |  |
|           | <ul> <li>Number of successfully fulfilled contracts</li> </ul>              |  |  |  |  |
|           | • Number of companies not having taken part in any contracts                |  |  |  |  |
|           | • Ranking of interaction pairs according to frequency, trading vol-         |  |  |  |  |
|           | ume, 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:                      |  |  |  |  |
|           | <ul> <li>Number of successfully agreed contracts</li> </ul>                 |  |  |  |  |
|           | <ul> <li>Number of successfully fulfilled contracts</li> </ul>              |  |  |  |  |
|           | <ul> <li>Number of unsuccessful negotiations with no follow-up</li> </ul>   |  |  |  |  |
|           | <ul> <li>Number of unsuccessful negotiations vs agreed contracts</li> </ul> |  |  |  |  |
|           | Number of fulfilled contracts with quality complaints                       |  |  |  |  |

For trust measures, we refer to the set of requirements already defined elsewhere.

#### 4.4.2 Metrics for the Growth Phase

Producer-to-consumer ratio (but only for those who are active) Interaction failure  $\rightarrow$  important to realize when things go wrong "distance" between producers and consumers e.g. for feedback

| 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 interac- |  |  |
|           | tion 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. plat- |  |  |  |  |  |
|           | form growth, either in terms of participation or trading volume.           |  |  |  |  |  |

#### 4.4.3 Metrics for the Maturity Phase

When a platform matures, its ecosystem will become more stable and thus attract late-comers. At this stage, it is important that the platform mobilises the innovative power of its constituency and despite being large and possibly heterogeneous, the governance mechanisms should have a high signal-to-noise ratio in order to keep the ecosystem vibrant and immune from negative externalities.

| PM-MAT-01 | The platform manager must be able to assess participation trends on the |  |  |  |
|-----------|---|--|--|--|
|           | platform through metrics comprising the following figures:              |  |  |  |
|           | <ul> <li>Size of companies joining over time</li> </ul>                 |  |  |  |
|           | <ul> <li>Number of companies joining over time</li> </ul>               |  |  |  |
| 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               |  |  |  |



# 5 Business Needs of Platform Customers

According to a questionnaire sent out for NIMBLE's Ambassador scheme, user companies of NIMBLE would like to know the following about a potential customer / provider to start a business (first orders) relationship:

| PC-INF-01 | The platform customer should have access to the following general in-   |
|-----------|---|
|           | formation about prospective business partners:  |
|           | • complete details (name, address, sector of activity, etc.), main ac-<br>tivity, area of influence, VAT number,  |
|           | • Type of company, history and commercial references (other pro-<br>viders / other clients, reputation) the competition, habitual provid-<br>ers and company brief history. |
|           | <ul> <li>Production capacity, turnover, growth expectations.</li> </ul>   |
|           | <ul> <li>Potential consumption, purchase specifications, machinery, facili-<br/>ties, and production location</li> </ul>  |
|           | <ul> <li>Contact information / mail head buyer</li> </ul>   |
|           | <ul> <li>Ouality and safety guarantees</li> </ul>   |
|           | Troubleshooting channel   |
| PC-INF-02 | The platform customer should have access to the following information about <b>Terms and Conditions</b> of the prospective business partner:                                |
|           | • payment method,   |
|           | <ul> <li>packaging, transport,</li> </ul>   |
|           | • Incoterms,  |
|           | <ul> <li>deadlines delivery,</li> </ul>   |
|           | <ul> <li>delivery address,</li> </ul>   |
|           | • purchase volume,  |
|           | <ul> <li>special requirements if they exist,</li> </ul>   |
| PC-INF-03 | The platform customer should have access to the following information about the <b>Economic Situation</b> of the prospective business partner:                              |
|           | • Balance sheets, current profits, reputation reports,  |
|           | <ul> <li>Commercial and financial report, commercial solvency infor-<br/>mation</li> </ul>  |
|           | Solvency and risk classification  |
|           | Payment method  |
| PC-INF-04 | The platform customer should have access to the following information about the <b>Product Portfolio</b> of the prospective business partner:                               |
|           | • Type of product, style, complete portfolio of products / services.<br>Product Catalogue with technical data sheets  |
|           | • Type of components  |
|           | <ul> <li>Operative from Pre-purchase / sale, buy / sell and post-purchase / sale</li> </ul>   |
|           | • Furniture designs in AutoCAD  |
|           | Price and delivery time per product   |

So these requirements should also be added to the Platform Management's Requirements portfolio because they potentially contribute to the success of the platform.

# 6 Management Dashboards available in NIMBLE

At present, all data concerning management of the platform is implemented as analytics reports over log data, with a scalable refresh rate. In some cases, logs are checked every 10 seconds and the refresh rate can be set by the platform administrator. The reports are based on the log files of identity-service, catalogue-service and business-processes-service that are fed into the ELK Stack, with Kibana for the visualization.

There are four levels of management reporting:

- User Activity Report companies, users, transactions, etc.
- Service Health Report applications or services up/down, data space usage, etc.
- Security Dashboard unusual behaviour detection, failed logins, etc.
- Technical level log analysis programmable queries over system logs

The user activity report will be augmented by event-based reporting through microservices that will take the necessary information directly from the live databases.

#### 6.1 User Activity Report

This dashboard shows on timelines, event and accumulated counts of the events: logins, registered users & companies, submitted catalogues and business-processes (transactions). Additionally, the data is also listed in tables.





## 6.2 Service Health Report

This service is more directed at the management of service levels and may in many cases be delegated to the cloud service provider where the platform is hosted.



#### 6.3 Security Dashboard

This dashboard is similar to the User activity report, but it queries more table fields and it monitors in particular, failed logins as an indication of possible security threats. The Security dashboard can be improved by also sending the IP-address of the Login attempt in the JSON content. Furthermore, tracking of a unique IP from which the requests comes would allow us to match a location on the map to a geo-ip.





## 6.4 Log Analysis Desk

The log analysis desk is directed at technical staff who may need to audit system performance or any other platform activity

| Pie Chart, identity-service, Error and Warns for tra | ice ID  | Timeline: all serviceID stacked by levels                                   | with filtered INFO |                                       |   |                        |                        |
|--|---|---|--------------------|---------------------------------------|---|------------------------|------------------------|
|  | WWW     SINCE     SINCE     SINCE     SINCE     DEBUG      DEBUG      Understand     Inderstand     Inders | catala  |                    |                                       | ia il   | n                      |                        |
| Pie Chart, catalogue-service-srdc, Error and Warns   | s for trace ID 🧳  |   |                    |                                       |   |                        |                        |
| (  | <ul> <li>ERROR</li> <li>WARN</li> <li>65df011ed2a40724</li> <li>c027c0357e98ef97</li> <li>29f4b02d42b7414</li> <li>36919ebcf2f371c7</li> <li>4df6f4d3a7c98bac</li> </ul>  | 2018-05-31 02:00 2018-06-03 0<br>gr<br>Table ▼<br>@timestamp per 12 hours ≎ | 2018-06-07 02:00   | 2018-06-11 02:00 20<br>@timestamp per | 18-06-15 02:00 2018-06-19<br>12 hours<br>serviceID \$ | 02:00 2018-06-23 02:00 | 2018-06-27 02:00<br>√* |
|  | 674e810db4f3bd81  | 2018-06-07 12:00  | WARN               |                                       | identity-service                                      | 1                      |                        |
|  | 6c3269832f1ef8eb  | 2018-06-07 12:00  | DEBUG              |                                       | identity-service                                      | 1                      |                        |
|  | a558d6e71dc9056e  | 2018-06-08 00:00  | ERROR              |                                       | identity-service                                      | 1                      |                        |
| 0  | a5993eee02126a49  | 2018-06-08 00:00  | ERROR              |                                       | business-process-service                              | 1                      |                        |
|  |   | 2018-06-08 00:00  | ERROR              |                                       | data-channel-service                                  | 1                      |                        |
| Pie Chart, business-process-service, Error and Wa    | rns for trace ID  | 2018-06-08 00:00  | ERROR              |                                       | catalogue-service-srdc                                | 1                      |                        |
|  | 🔊 🗢 DEBUG   | 2018-06-08 00:00  | WARN               |                                       | identity-service                                      | 1                      |                        |
|  | ERROR   | 2018-06-08 00:00  | WARN               |                                       | data-channel-service                                  | 1                      |                        |
| $\bigcirc$   | WARN<br>2a437caf97dcd581  | 2018-06-08 00:00  | WARN               |                                       | catalogue-service-srdc                                | 1                      |                        |
|  | <ul> <li>3b1c467c948b23e5</li> <li>407ebae008b85706</li> <li>40c4818c248115a</li> <li>493134715efbd447</li> <li>4b643e97552b528c</li> <li>4b84c31277359bd1</li> <li>5093c2014c90cd7</li> <li>520311691e1072e0</li> <li>55c17547204d06171</li> </ul>   | 2018-06-08 12:00<br>Export: Raw 🛦 Formatted 🛦                               | DEBUG              | 1 2 3 4 512 »                         | business-process-service                              | 6                      | Page Size 10 🕈         |

In the visualisations above, we can see various log data taken from the microservices that make up the NIMBLE platform. All of these logs can be further analysed through the ELK stack (see D3.6 Data Analytics for further information) and several of the current dashboard are driven by such log analyses.

# 7 Validation of the Management Facilities of NIMBLE Release 7

In this section we validate the current functionality w.r.t. the major requirements identified for NIMBLE:

- Platform Accountability
- Security Management
- Federation Management
- Trust Management
- Information Management
- Governance Mechanisms
- Management Metrics

We use the requirements tables of the relevant sections and add a third column in which we describe the degree of conformance in Release 3.0 of the system.

## 7.1 Platform Accountability - Validation

| PM-ACC-01 | Keep a registry of users that can be (re-)connected to offi-<br>cial records if necessary (e.g. for auditing historical data<br>for fraud detection or taxation issues)   | Yes<br>Registration                        |
|-----------|---|--|
| PM-ACC-02 | Provide a list of business transaction types (negotiating, buying, supplying, paying, etc)  | Implicit, avail-<br>able from logs         |
| PM-ACC-03 | Provide a taxonomy of user roles associated with business transaction types   | Yes<br>Keycloak +<br>core services         |
| PM-ACC-04 | Keep a registry of user actions: user U <i>acting_for</i> firm F<br>in role R doing action A at time T<br>[acting_for(U,F,R,A,T)]<br>Keeping this type of information has privacy implications<br>and requires data anonymisation | Partly availa-<br>ble from logs            |
| PM-ACC-05 | Keep a record of all business transactions that happen via<br>the platform; offer different levels of aggregation / ano-<br>nymity for these, keeping to strict rules of privacy  | Yes, basic rec-<br>ords are avail-<br>able |
| PM-ACC-06 | Make visible to users, a record of the number of platform<br>transactions per user, per company (aggregates over<br>hours, day, week, month, year)  | Work in pro-<br>gress                      |
| PM-ACC-07 | Keep a record of the monetary value of the transactions per company, etc.   | yes  |
| PM-ACC-08 | Provide any user with an immediate feedback option that<br>also records the user context in which the feedback was<br>given   | Yes, available since R1.0                  |
| 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)   | Not yet imple-<br>mented                   |



## 7.2 Security Management - Validation

| PM-SEC-01          | The platform manager must be able to comply with   | Work in pro-                                  |
|--------------------|--|---|
|                    | his/her obligations as a GDPR Data Processor.  | gress   |
| PM-SEC-02          | The platform manager's account must be auditable to en-<br>sure compliance with GDPR rules and with other regula-<br>tory compliance (e.g. taxation rules)                             | Work in pro-<br>gress                         |
| PM-SEC-03          | The platform manager's account must be retrievable and<br>there must be a substitute available at all times, to ensure<br>that there is not a "single point of failure" in the system. | Work in pro-<br>gress                         |
| PM-SEC-04          | It should be possible to configure "honey pots" as a pro-<br>active security strategy.   | Not imple-<br>mented yet                      |
| PM-SEC-05<br>(NFR) | Data storage should be designed in a modular and seg-<br>mented manner to make data theft "expensive" for the at-<br>tacker (small rewards for high effort).                           | By design via<br>microservice<br>architecture |
| PM-SEC-06<br>(NFR) | The platform manager role subsumes the following sub-<br>roles: privacy management; platform security manage-<br>ment; platform operational management                                 | Work in pro-<br>gress                         |
| PM-SEC-07          | The platform's security officer should have access to a dashboard that shows the threat vectors which the platform is experiencing.  | Basic function-<br>ality available            |

Concerning the first two requirements relating to GDPR, we are designing a number of features as on-going work in WP6. For example, a user can legitimately ask to be removed from the platform if he/she is no longer working with the platform, for whatever reason. However, in order to comply with other regulations, it must be possible for NIMBLE to reconstruct who was in charge of a specific transaction at a time when the user was still active on the platform. Such information should require a specifically authorised query and that query should yield the person's encrypted ID. Depending on the circumstances (e.g. checking the identity of a person who is suspected of some wrong-doing) a further query could simply be "Was person XYZ the owner of this transaction?" and the answer would only have to be a yes or a no.

## 7.3 Federation Management - Validation

| PM-FED-01 | The NIMBLE Open API must, as a minimum require-            | Work in pro- |
|-----------|--|--------------|
| (NFR)     | ment, support search, negotiation, contracting and fulfil- | gress        |
|           | ment across platform instances of NINBLE.                  |              |

This functionality is subject to further testing, particularly in WP5 when advanced usages of the platform will be enabled. It is also subject to further development as new connectivity requirements arise. At the platform management level, we are primarily concerned with actual usage patterns of the API calls and these can be gathered from logs.



# 7.4 Trust Management - Validation

| PM-TRUST-01 | There must be an algorithm that measures an overall<br>level of trust for the platform. Can possibly be done<br>as a confidence rating for a transaction to be success-<br>ful. 100% would be the maximum.   | Done                  |
|-------------|--|-----------------------|
| PM-TRUST-02 | There should be an algorithm that measures the per-<br>ceived trust of non-users, concerning transactions<br>happening on NIMBLE.  | Work in pro-<br>gress |
| PM-TRUST-03 | There must be an algorithm to calculate the trust level between A and B, and B and A respectively.   | Done                  |
| PM-TRUST-04 | There should be an algorithm to detect trust imbal-<br>ances that go beyond individual firms and that point<br>to larger-scale discrepancies between constituencies<br>on the platform   | Work in pro-<br>gress |
| 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.  | Done                  |
| PM-TRUST-06 | There must be a measure of satisfaction for firms, for<br>getting from the state of having closed a deal, to ful-<br>filment of its terms, i.e. a measure of how well the<br>contract was honoured by both sides.  | Done                  |
| PM-TRUST-07 | There should be a measure of quality for any infor-<br>mation exchange happening inside the platform, and<br>also for any information exchange happening be-<br>tween platform and external, non-users. The platform<br>must be perceived as a constituency of highly trust-<br>worthy partners. | Done                  |

# 7.5 Information Management - Validation

| PM-INF-01 | (Info-Flow-Monitoring) Platform manager must be<br>able to monitor any B2B information flow that is<br>originally enabled by NIMBLE  | Possible via logs   |
|-----------|--|---------------------|
| PM-INF-02 | (Info-Flow-Control) Platform manager must be able<br>to halt / restart any B2B information flow that is orig-<br>inally enabled by NIMBLE.   | Work in progress    |
| PM-INF-3  | Any intervention in B2B processes at Platform level must be auditable  | Possible via logs   |
| PM-INF-4  | The platform manager must have access to a reposi-<br>tory of local edge devices that are or have been, used<br>in B2B data exchanges between companies, via<br>NIMBLE. Current connectivity must be monitor-able<br>and past connectivity must be accessible through<br>logs. | Work in<br>progress |

## 7.6 Governance Mechanisms - Validation

| PM-GOV-01 | Gate-keeping: the registration process must include<br>checks to ensure that only trustworthy entities join<br>the platform   | Manual check at present          |
|-----------|---|----------------------------------|
| PM-GOV-02 | Process: entities on the platform must have serious<br>intention to use the platform. Trial phases must be<br>possible, but must be signaled to others.                         | Separate Plat-<br>form instances |
| PM-GOV-03 | Metrics: all metrics used by the platform should be auditable by regulators.  | Work in progress                 |
| PM-GOV-04 | Relational: the values to be shared for NIMBLE plat-<br>forms are kept up-to-date by an independent regula-<br>tory entity that is governed by the NIMBLE mission<br>statement. | Work in progress                 |
| PM-GOV-05 | Gate-keeping: The platform manager must be able to<br>switch off and remove services that break basic inter-<br>action mechanisms of the platform.                              | Work in progress                 |

# 7.7 NIMBLE Platform Management Metrics - Validation

| PM-LIQ-01 | <ul> <li>The platform manager must be able to see the "Liquidity" of the platform as a metric comprising the following figures:</li> <li>Number of participants (companies)</li> <li>Number of successfully agreed contracts</li> <li>Number of successfully fulfilled contracts</li> <li>Number of companies not having taken part in any contracts</li> <li>Ranking of interaction pairs according to frequency, trading volume, satisfaction level.</li> </ul> | Available           |
|-----------|---|---------------------|
| PM-MQL-01 | <ul> <li>The platform manager must be able to assess the matching quality of the platform as a metric comprising the following figures:</li> <li>Number of successfully agreed contracts</li> <li>Number of successfully fulfilled contracts</li> <li>Number of unsuccessful negotiations with no follow-up</li> <li>Number of unsuccessful negotiations vs agreed contracts</li> <li>Number of fulfilled contracts with quality complaints</li> </ul>            | Available           |
| PM-P2C-01 | <ul> <li>The platform manager must be able to assess participation trends on the platform through metrics comprising the following figures:</li> <li>Number of products offered on the platform</li> <li>Coverage of eClass and distribution of sales over eClass items</li> </ul>  | Work in<br>progress |



|           | • Number and kind of products offered but not  |                     |
|-----------|--|---------------------|
|           | • Number and kind of products offered but not sold   |                     |
|           | Number and kind of products sought but not offered   |                     |
| PM-IAF-01 | <ul> <li>Number and kind of products sought but not offered</li> <li>The platform manager must be able to search for root causes of interaction failures through metrics comprising the following information: <ul> <li>For stopped negotiations: which side stopped the negotiation?</li> <li>For stopped negotiations: what caused stopping the negotiation?</li> <li>For unfulfilled contracts: which side complained about what?</li> <li>For unfulfilled contracts: what caused the transaction to fail?</li> </ul> </li> <li>The above must be supported by questionnaires to the parties, with "closed" questions (selectable standard options) and "open" questions for analysis by hu-</li> </ul> | Work in progress    |
| PM-IAF-02 | mans or AI techniques.<br>The platform manager must be able to assess partici-<br>pation intensity on the platform through metrics col-  |                     |
|           | <ul> <li>Number of published catalogue items, over time</li> <li>Number of initiated product or service searches, over time</li> <li>Trading volume as supplier, over time</li> <li>Trading volume as buyer, over time</li> <li>Aggregated figures can be used to derive participation intensity vs. platform growth, either in terms of participation or trading volume.</li> </ul>   | Available           |
| PM-MAT-01 | <ul> <li>The platform manager must be able to assess participation trends on the platform through metrics comprising the following figures:</li> <li>Size of companies joining over time</li> <li>Number of companies joining over time</li> </ul>   | Available           |
| PM-INN-01 | <ul> <li>The platform manager must be able to assess behaviour changes on the platform through metrics comprising the following figures</li> <li>Hot-spots: changes in transactional behaviour of groups</li> <li>Requests for changes, improvements of the platform</li> <li>Interaction types falling into disuse</li> <li>Companies leaving the platform</li> <li>Companies reducing activity on the platform</li> <li>Companies strengthening activities outside the platform</li> </ul>   | Work in<br>progress |



# 8 Conclusions

The initial validation consisted of a check of currently implemented platform management functionality. While the conceptual model distinguishes between a number of platform success factors, the current implementation is very pragmatic distinguishing only between the "health status" of services, a registry of users and companies, a dashboard with basic security level indicators, such as the number of failed logins, and a facility for directly analysing the system logs, using the ELK stack.

Further work will address the implementation of more advanced features, ranging from the list of metrics specified here, to tools that enable the platform manager to change the behaviour of platform participants. This work will partly be done as continuation of WP3 and partly as advanced services being developed in WP5.

All requirements listed in this document are also mapped and cross-referenced in the consolidated requirements repository that was issued as section 5 of D4.5 the closing deliverable of WP4 (Validation and Experimentation with the NIMBLE Platform).

# **9** References

(BalHee 2011) Ballon, Pieter and Van Heesvelde, Eric, (2011), ICT platforms and regulatory concerns in Europe, Telecommunications Policy, 35, issue 8, p. 702-714, https://EconPapers.repec.org/RePEc:eee:telpol:v:35:y:2011:i:8:p:702-714.

(Cho 2015) Choudary 2015, Platform Scale, Platform Thinking Labs Pte. Ltd., 325 pages.

(EvGaw 2016) Evans P C, Gawer A. (2016), The Rise of the Platform Enterprise – A Global Survey, 30 pages, https://www.thecge.net/app/uploads/2016/01/PDF-WEB-Platform-Survey\_01\_12.pdf

(EvSchma 2016) Evans D. S., Schmalensee R. (2016), Matchmakers - The New Economics of Multisided Platforms, Harvard Business Review Press, 260 pages.

(GawCus) 2002Annabelle Gawer and Michael A. Cusumano. 2002. Platform Leadership. Harvard Business School Press, Boston, MA, USA, 305 pages.

(LeeZhuJef 2017) Sung Une Lee, Liming Zhu, Ross Jeffery, Design Choices for Data Governance in Platform Ecosystems - A Contingency Model, https://arxiv.org/ftp/arxiv/papers/1706/1706.07560.pdf

(ParAlsCho 2016) Parker G. G., Van Alstyne M.W., Choudary S.P. (2016), Platform Revolution -How networked markets are transforming the economy and how to make them work for you, Norton Publishers, 336 pages.

(Tiw 2014) Tiwana A. (2014), Platform Ecosystems - Aligning Architecture, Governance, and Strategy, Morgan Kaufmann, 302 pages.